T.C.

POLİS AKADEMİSİ

GÜVENLİK BİLİMLERİ ENSTİTÜSÜ

GÜVENLİK STRATEJİLERİ VE YÖNETİMİ ANABİLİM DALI

DİJİTAL ÇAĞDA GÜVENLİK STRATEJİLERİ TASARIMI VE YÖNETİMİ: BİR MODEL ÖNERİSİ

DOKTORA TEZİ

Yavuz TÜRKGENCİ

Danışman

Doç. Dr. Ufuk AYHAN

Ankara – 2023

T.C.

POLİS AKADEMİSİ

GÜVENLİK BİLİMLERİ ENSTİTÜSÜ

GÜVENLİK STRATEJİLERİ VE YÖNETİMİ ANABİLİM DALI

DİJİTAL ÇAĞDA GÜVENLİK STRATEJİLERİ TASARIMI VE YÖNETİMİ: BİR MODEL ÖNERİSİ

DOKTORA TEZİ

Yavuz TÜRKGENCİ

Danışman

Doç. Dr. Ufuk AYHAN

Ankara – 2023

TELİF HAKLARI BEYANNAMESİ

GÜVENLİK BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Doktora tezi olarak sunduğum bu çalışmayı bireysel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde yollama yaparak yararlandığımı belirtir, bunu şerefimle beyan ederim.

Enstitü veya başka herhangi bir merci tarafından belli bir zamana bağlı kalmaksızın, tezimle ilgili bu beyana aykırı bir durumun tespit edilmesi durumunda, ortaya çıkan tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

Ayrıca tezde ortaya konulan, açıklanan, savunulan bütün konuların bilimsel bir çerçevede hazırlandığını, hiçbir kurumu veya kuruluşu bağlamayacağını vurgulamak isterim.

17/03/2023

Yavuz TÜRKGENCİ

ÖZET

Polis Akademisi

Güvenlik Bilimleri Enstitüsü

Güvenlik Stratejileri ve Yönetimi

Dijital Çağda Güvenlik Stratejileri Tasarımı ve Yönetimi: Bir Model Önerisi

Yavuz TÜRKGENCİ

Doktora Tezi

Tez Danışmanı: Doç. Dr. Ufuk AYHAN

2023, 241 Sayfa

Klasik güvenlik stratejisi tasarımı genellikle; nihai hedef, yöntem/konsept, güç unsurları/araç/kaynak (Ends, Ways, Means) başlıklarından oluşan bir mimari kullanılarak oluşturulmaktadır. Günümüzde, bu mimari temel bir model olarak kabul görmektedir. Bu kapsamda, durum analizi, nihai hedef, güç unsurları/araçlar/kaynaklar, yöntem/konsept, risklerin analizinden oluşan beş safhalı bir süreç kullanılarak klasik güvenlik strateji tasarımının yapılabileceği düşünülmektedir.

Ancak klasik strateji tasarım mimarisinin ve sürecinin, süratli değişim ve dönüşüm, teknolojik gelişmeler, yeni güvenlik ortamının ortaya çıkarttığı stratejik şoklar gibi nedenlerden dolayı dijital çağın ihtiyaçlarını yeteri kadar karşılayamadığı değerlendirilmektedir.

Bu tezde yapılan incelemeler neticesinde, bu problemin yalnızca bir strateji tasarım ve yönetim modeli oluşturulması ile çözülemeyeceği sonucuna varılmıştır. Bu çerçevede, beş konu üzerinde odaklanılması gerektiği kıymetlendirilmektedir. Bunlar; modelleme-prototip üretimi-deneme, periyodik değerlendirme sistemi, yeni güvenlik stratejisi modeli, strateji yönetim sistemi, dijital çağ teknolojilerinin kullanımı olarak ifade edilebilir. Her konu için tezde ayrı bir model önerisi yapılmıştır. Bu beş modelin bütüncül bir şekilde kullanılması dijital çağa uygun bir modelin oluşturulmasını sağlayabileceği düşünülmektedir.

Genel olarak nitel araştırma tekniklerinden keşfedici ve betimleyici yöntemler kullanılarak, tümden gelim tekniği ile tez konusu incelenmiştir. Tezin genelinde geçmişteki kişisel deneyimlerden ağırlıklı olarak faydalanılmıştır. Metin ve süreç analiz yöntemleriyle keşfedici bir bakış açısıyla klasik güvenlik stratejisi modeli kapsamlı bir şekilde ortaya konulmuştur. Dijital çağın ortaya çıkarttığı yeni sorunlar, sınamalar ve bunların güvenlik stratejilerinin tasarımı ve yönetimine muhtemel etkileri keşfedici bir bakış açısıyla, kişisel gözlem, durum analizi, metin analizi ve deneyimlerden faydalanılarak incelenmiştir. Dijital çağın getirdiği şartlar ve etkiler ile çağdaş teknolojilerin stratejik tasarıma ve yönetime etkileri yorumlanarak, problem sahalarına çözüm getirebilecek yeni bir model oluşturulmuştur.

Tezde, yapılan incelemeler neticesinde; klasik modelin dijital çağın ihtiyaçlarına cevap veremediği sonucuna ulaşılmış ve dijital çağ teknolojilerinin kullanımını içeren, beş konu başlığından oluşan yeni bir model önerilmiştir.

Anahtar Kelimeler: Strateji, Güvenlik, Güvenlik Stratejisi, Güvenlik Strateji Tasarımı, Dijital Çağ Teknolojileri

ABSTRACT

Turkish National Police Academy

Department of Security Strategies and Management

Design and Management of Security Strategies in the Age of Digitalization: a Model Proposal

Yavuz TÜRKGENCİ

Ph.D. Dissertation

Supervisor: Assoc. Prof. Dr. Ufuk AYHAN

2023, 241 pages

The most commonly used format of a classic security strategy is; Ends, Ways and Means structure. Today, this architecture is accepted as a basic model. In this context, it is thought that a classical security strategy design can be formulated by using a five-stage process consisting of the situation analysis, final objective, instrument of power/means/resources, concept, analysis of risks.

However, it is considered that the classical strategy design architecture and process cannot adequately meet the requirements of the digital age due to reasons such as rapid change and transformation, technological developments, and the strategic shocks caused by the new security environment.

As a result of the examinations in this thesis, it has been concluded that this problem cannot be solved only by creating a strategy design and management model. In this framework, it is appreciated that five issues should be focused on. These are; modelling-prototype production-experimentation, periodic assessment system, new security strategy model, security strategy management system and use of digital age technologies. A separate model proposal was made for each subject in the thesis. It is thought that using these five models in a holistic way can create a model suitable for the digital age.

In general, using exploratory and descriptive methods from qualitative research techniques, the thesis topic was examined with the deductive technique. Throughout the thesis, personal experiences in the past have been mainly utilized. The classical security strategy model has been comprehensively presented with an exploratory point

of view with text and process analysis methods. The new problems and challenges of the digital age and their possible effects on the design and management of security strategies are examined from an exploratory point of view, using personal observation, case studies, text analysis and experiences. By interpreting the conditions and effects of the digital age and the effects of contemporary technologies on strategic design and management, a new model has been created that can bring solutions to problem areas.

In the thesis, as a result of the examinations; It was concluded that the classical model could not meet the needs of the digital age, and a new model consisting of five topics, including the use of digital age technologies, was proposed.

Key Words: Strategy, Security, Security Strategy, Security Strategy Design, Digital Age Technologies.

İÇİNDEKİLER

Sayfa

TEZ ONAY SAYFASI …… II

TELİF HAKLARI BEYANNAMESİ ……... III

ÖZET ……... IV

ABSTRACT …… VI

İÇİNDEKİLER LİSTESİ …….. VIII

KISALTMALAR LİSTESİ ……..... XIV

TABLOLAR LİSTESİ ……... XVI

ŞEKİLLER LİSTESİ ……..…… XVII

GİRİŞ ……... 1

BİRİNCİ BÖLÜM

GÜVENLİK STRATEJİSİ TASARLAMANIN KAVRAMSAL ÇERÇEVESİ

1.1.STRATEJİ KAVRAMININ AÇIKLANMASI …… 7

1.1.1. Harbin Sevk ve İdare Seviyeleri……. 10

1.1.2. Strateji Kavramının Tanımı……... 12

1.2.TARİHİ SÜREÇTE STRATEJİ VE GÜVENLİK İLİŞKİSİNİN İNCELENMESİ…… 14

1.2.1.Tarım Çağı……. 15

1.2.2.Sanayi Çağı …… 19

1.2.3.Soğuk Savaş (Nükleer Çağ) ……. 22

1.2.4.Soğuk Savaş Sonrası …… 25

1.2.5.Terörizm ile Mücadele ve Hibrit Savaş Dönemi …… 26

1.3.GÜVENLİK YAKLAŞIMLARININ GÜVENLİK STRATEJİSİ AÇISINDAN İNCELENMESİ …… 28

1.3.1. Geleneksel Güvenlik Yaklaşımı ……. 29

1.3.1.1. Realist Güvenlik Yaklaşımı ……... 29

1.3.1.2. Neorealist Güvenlik Yaklaşımı ……. 30

1.3.1.3. İdealist Güvenlik Yaklaşımı …….. 31

1.3.1.4. Liberal Güvenlik Yaklaşımı …….. 32

1.3.2. Yeni Güvenlik Yaklaşımları ……... 32

1.3.2.1. Kopenhag Okulu …… 33

1.3.2.2. Eleştirel Yaklaşım …….. 34

1.3.2.3. İnşacı Yaklaşım …… 35

1.3.2.4. Postmodernist Yaklaşım ……..... 36

1.3.2.5. Feminist Yaklaşım ……. 37

1.3.3. Güvenlik Stratejisi Tasarımının Analiz Düzeyleri ……... 37

1.3.3.1. Uluslararası Sistem Düzeyi ……... 38

1.3.3.2. Ulus-Devlet Düzeyi …… 38

1.3.3.3. Birey Düzeyi ……... 39

1.4.GÜVENLİK STRATEJİSİ TASARIMININ İNCELENMESİ …….. 40

1.5.KLASİK STRATEJİ TASARIMI ……. 43

1.5.1.Stratejik Düşünme …… 43

1.5.2.Stratejik Düşünme Sistemi …….. 44

1.5.3.Stratejinin Özellikleri ……... 47

1.5.4. Klasik Güvenlik Stratejisi Tasarım Süreci ……... 50

1.5.4.1. Güvenlik Strateji Tasarımında Dikkat Edilmesi Gereken Genel Hususlar ……. 50

1.5.4.2. Millî Güvenlik Stratejisi …… 51

1.5.4.3. Güvenlik Stratejisi Tasarım Süreci …….. 58

1.5.4.3.1. Stratejik Durum Analizi ……. **58**

1.5.4.3.2. Nihai Stratejik Hedefin Tanımlanması ……..…. **73**

1.5.4.3.3. Millî Güç Unsurları …… **76**

1.5.4.3.4. Stratejik Konseptin Tasarımı …….……. **93**

1.5.4.3.5. Maliyet/Risklerin Değerlendirilmesi ……. **98**

1.6. SONUÇ ……. 101

İKİNCİ BÖLÜM

DİJİTAL ÇAĞIN ORTAYA ÇIKARTTIĞI ŞARTLARIN VE ETKİLERİN GÜVENLİK STRATEJİSİ TASARIMINA YANSIMALARININ İNCELENMESİ

2.1. DİJİTAL ÇAĞDA GÜVENLİK ORTAMI DURUM TESPİTİ …….. 106

2.2. DİJİTAL ÇAĞDA GÜVENLİK ORTAMININ GÜVENLİK STRATEJİSİ TASARIMINA ETKİLERİNİN ANALİZİ …….. 117

2.3. DİJİTAL ÇAĞDA GÜVENLİK STRATEJİSİ TASARIMINI ETKİLEYEN TEKNOLOJİK GELİŞMELER ……. 122

2.3.1.Büyük Veri …… 123

2.3.2. Yapay Zekâ …….. 125

2.3.3. İnternet, Sosyal Medya, Metaverse, Nesnelerin İnterneti ……... 126

2.3.4. Medya ……... 129

2.3.5. İnsansız ve Otonom Sistemler …… 129

2.3.6. Uzay Teknolojileri ……... 130

2.4. TEKNOLOJİK GELİŞMELERİN GÜVENLİK STRATEJİSİ TASARIMINA ETKİLERİ ……. 131

2.4.1. BV ve YZ'nin Güvenlik Stratejilerinin Tasarımına Etkisi …….. 132

2.4.1.1. Durum Tespitinde BV ve YZ …….. 134

2.4.1.2. Nihai Hedeflerin Belirlenmesinde BV ve YZ …… 136

***2.4.1.3. Millî Güç Unsurları, Araç ve Kaynakların Kullanımında BV ve YZ* 138**

2.4.1.4. Konsept Oluşturulmasında BV ve YZ …… 139

2.4.1.5. Risk Yönetiminde BV ve YZ ……... 140

2.4.2. İnternet, Sosyal Medya, Metaverse, Nesnelerin İnternetinin Güvenlik Stratejilerinin Tasarımına Etkisi …….. 141

2.4.2.1. Genel ……... 141

2.4.2.2. İnternet ve Diğer Uygulamaların Güvenlik Stratejilerinin Tasarımına ve Yönetimine Olan Etkisi ……... 147

2.4.3. Medyanın Güvenlik Stratejilerinin Tasarımına Etkisi …… 150

2.4.3.1. Genel …….. 150

2.4.3.2. Medyanın Güvenlik Stratejilerinin Tasarımına ve Yönetimine Olan Etkisi ……. **151**

2.4.4. Otonom Sistemleri Güvenlik Stratejilerinin Tasarımına Etkisi ... 153

2.4.4.1. Genel …… **153**

2.4.4.2. Otonom Sistemlerin Güvenlik Stratejilerinin Tasarımına ve Yönetimine Olan Etkisi …… **154**

2.4.5. Uzay Teknolojisinin Güvenlik Stratejilerinin Tasarımına Etkisi .. 155

2.4.5.1. Genel ……. **155**

2.4.5.2. Uzayın Güvenlik Stratejilerinin Tasarımına ve Yönetimine Olan Etkisi …….. **156**

2.5. DİJİTAL ÇAĞDA GÜVENLİK STRATEJİSİ TASARIMI VE YÖNETİMİNE ETKİ EDEBİLECEK FAKTÖRLERİN VE PARAMETRELERİN TESPİT EDİLMESİ ……. 157

2.5.1. Süratli Değişim …… 158

2.5.2.Belirsizlik ve Muğlaklık ……... 160

2.5.3.Yeni Aktörler …… 160

2.5.4.Siber ve Uzay Ortamları ……..... 161

2.5.5. Dijital Çağ Teknolojisi …… 163

2.5.6. Dijital Çağda Karar Verme …… 164

2.6. SONUÇ ……..... 172

ÜÇÜNCÜ BÖLÜM

DİJİTAL ÇAĞA UYGUN BİR GÜVENLİK STRATEJİSİ TASARIM MODELİ ÖNERİSİ

3.1. GÜVENLİK STRATEJİSİ TASARIM SÜRECİNE YÖNELİK MODEL ÖNERİSİ ……. 177

3.1.1. Stratejik Ortam Modeli …… 179

3.1.2. Güvenlik Stratejisi Prototipi …… 183

3.1.3. Güvenlik Stratejisi Prototipinin Denenmesi ……... 183

3.1.4. Güvenlik Stratejisi Prototipinin Değerlendirilmesi ……... 186

3.1.5. Güvenlik Stratejisi Tasarım Sürecinde Kullanılabilecek Dijital Çağ Teknolojileri ……. 187

3.2. GÜVENLİK STRATEJİSİ TASARIMI VE YÖNETİMİ MODELİ ÖNERİSİ ……... 190

3.3. GÜVENLİK STRATEJİSİNİN PERİYODİK DEĞERLENDİRİLMESİ 194

3.4. RİSK YÖNETİM MODELİ ……... 198

3.5. GÜVENLİK STRATEJİSİ YÖNETİM MODELİ ……... 204

3.5.1. GUKİ Döngüsü …….. 204

3.6. GÜVENLİK STRATEJİSİ YÖNETİMİNDE TEKNOLOJİ KULLANIMI ……... 210

3.7. SONUÇ …….. 215

SONUÇ ……. 219

KAYNAKÇA ……... 233

KISALTMALAR LİSTESİ

AB **:** Avrupa Birliği

AGİT **:** Avrupa Güvenlik ve İşbirliği Teşkilatı

GZTF **:** Güçlü-Zayıf-Tehdit-Fırsat

A2/AD **:** Erişim ve Alan Engelleme

AKKA **:** Avrupa Konvansiyonel Kuvvetler Anlaşması

BK : Birleşik Krallık

BM **:** Birleşmiş Milletler

BMGK **:** Birleşmiş Milletler Güvenlik Konseyi

BV **:** Büyük Veri

DEMI **:** Diplomatik, Ekonomik, Askeri, Bilgi

DEAŞ **:** Irak Şam İslam Devleti (Terör Örgütü)

DTÖ **:** Dünya Ticaret Örgütü

EYP **:** El Yapımı Patlayıcı

GAFAM **:** Google, Amazon, Facebook, Apple, Microsoft

GEOINT **:** Coğrafi Konum İstihbarat

İDA **:** İnsansız Deniz Aracı

İHA **:** İnsansız Hava Araçları

İKA **:** İnsansız Kara Aracı

IMINT **:** Görüntü İstihbaratı

IOT **:** Nesnelerin İnterneti

HUMINT : İnsan İstihbaratı

JFC **:** Müşterek Kuvvet Komutanlığı

KGAÖ : Kolektif Güvenlik Anlaşması Örgütü

MASINT : Yayılım İstihbaratı

MC : Milletler Cemiyeti

NAC : Kuzey Atlantik Konseyi

NATO : Kuzey Atlantik Anlaşması Örgütü

NFT : Değiştirilemez Varlık

NLP : Doğal Dil İşleme

NMS : NATO'nun Askeri Stratejisi

NMK : NATO Mukabele Kuvvetini

NWCC : NATO Temel Savaş Konsepti

PKK/YPG/PYD : Bölücü Terör Örgütü

PSO : Parçacık Sürü Optimizasyonu

R2P : Koruma Sorumluluğu

SSCB : Sovyet Sosyalist Cumhuriyetler Birliği

SHAPE : Avrupa Müttefik Kuvvetleri Yüksek Karargâhı

SIGINT : Sinyal İstihbaratı

SLBİ : Stratejik Lider Bilgi İhtiyacı

STRATCOM : Stratejik İletişim

OODA (GUKİ) : Gözlem, Uyumlandırma, Karar, İcra

OGSP : AB'nin Ortak Savunma ve Güvenlik Politikası

OSINT : Açık Kaynak İstihbaratı

TFZG : Tehdit-Fırsat-Zayıf-Güçlü

YZ : Yapay Zekâ

TABLOLAR LİSTESİ

Sayfa

Tablo 1.1: Faktör Analizi ……. 71

Tablo 3.1: Risk Tespit/Kayıt Tablosu …….. 202

Tablo 3.2: Risk Değerlendirme Tablosu …….. 205

Tablo 3.3: Değerlendirme Planı Örneği ……... 214

ŞEKİLLER LİSTESİ

Sayfa

Şekil 1.1: Klasik Güvenlik Stratejisi Yaklaşımı ……. 44

Şekil 1.2: Büyük Strateji (Örnek) …… 54

Şekil 1.3: Güvenlik Stratejisi Tasarım Süreci ……. 58

Şekil 1**.4**: Sistem Analizi ……. 68

Şekil 1.5: Beş Halka Metodu …….. 69

Şekil 1.6: Millî Güç Unsurlarının İcraya Dönüştürülmesi …….. 77

Şekil 1.7: Stratejik Konsept Hazırlanması …….. 94

Şekil 1.8: Maliyet/Risk Analizi ……... 99

Şekil 2.1: Dijital Güvenlik Ortamı …….. 105

Şekil 2.2: Büyük Verinin İstihbarat Haline Gelmesi …….. 125

Şekil 2.3: Genel Veri Bankası ……. 139

Şekil 2.4: Genel Stratejik Durum (Dashboard) ……. 141

Şekil 2.5: Karar Verme Süreci …… 168

Şekil 2.6: Kriz Yönetim Süreci …… 170

Şekil 2.7: Makine ve İnsan Hibrit Karar Verme Yöntemi ……... 172

Şekil 3.1: Dijital Çağ Güvenlik Stratejisi Tasarım Süreci ……... 179

Şekil 3.2: Stratejik Ortam Modeli …… 181

Şekil 3.3: Stratejik Seviye Oyunlama Tertibi …….. 187

Şekil 3.4: Dijital Çağ Güvenlik Stratejisi Modeli Önerisi …… 194

Şekil 3.5: Güvenlik Stratejisi Değerlendirme Modeli …….. 195

Şekil 3.6: Güvenlik Stratejisi Değerlendirme Sistemi …… 197

Şekil 3.7: Risk Yönetim Sistemi …… 199

Şekil 3.8: GUKİ Döngüsü …….. 207

Şekil 3.9: Güvenlik Stratejisi Yönetim Modeli …….. 209

Şekil 3.10: Güvenlik Stratejisi Dijital Modeli …… 211

Şekil 3.11: Durum Haritaları ve Dashboardların Değerlendirmede Kullanılması …… 212

GİRİŞ

Güvenlik Stratejisi konusunda Türkiye'de yapılan çalışmalar incelendiğinde; genel olarak, stratejinin tanımı, tarihi gelişimi, diğer ülkelerin güvenlik stratejilerinin incelenmesi gibi ağırlıklı olarak teorik konulara odaklanıldığı görülmektedir. Güvenlik stratejisinin tasarımı ve yönetimi mantığını, felsefesini açıklayan, icrayı da içeren doküman sayısı oldukça kısıtlıdır. Bu konuda güvenlik uzmanlarının başvurabileceği Türkçe doküman sayısının yeterli olmadığı değerlendirilmektedir.

Yabancı kaynaklar incelendiğinde ise teorik bilgiler olmakla birlikte, sınırlı paylaşım yapıldığı, bu nedenle güvenlik stratejilerinin pratikte tasarımına ve yönetimine ilişkin ayrıntılı bilgi bulunmadığı ifade edilebilir. Devletler güvenlik stratejilerini açıklarken yalnızca bilinmesinin uygun olacağı bölümleri açıklamakta, esas gizli bölümler açıklanmamaktadır. Bu nedenle güvenlik stratejisi tasarım mantığının anlaşılması oldukça zor olmaktadır.

Diğer taraftan başta yapay zekâ ve büyük veri olmak üzere günümüz teknolojileri güvenlik alanında gittikçe daha yaygın olarak kullanılmaya başlanmıştır. Bu teknolojilerin güvenlik stratejilerinin tasarımı ve yönetimine olan etkilerinin incelenmesi konusundaki çalışmalar oldukça yenidir, geliştirilmesine ihtiyaç duyulmaktadır. Bununla beraber dijital çağdaki değişim hızı, veri üretim miktarı nedeniyle uzun dönemli tasarlanan güvenlik stratejileri çok kısa sürede geçerliliklerini yitirmekte, uygulanamamaktadır. Uygulanmaya başlanabilse bile stratejik durumdaki gelişmelerin takibi ve bu gelişmelerle uyumlu kararların alınması mümkün olamamaktadır. Dijital çağın ortaya çıkarttığı bu ve benzeri problemlere çözüm bulunabilmesi maksadıyla gerekli araştırmaların yapılması, çözümler üretilmesi gerekmektedir.

Güvenlik stratejileri tasarımı ve yönetimi konusunda Türkiye'deki dokümantasyona katkı yapılmasına ve bu çerçevede dijital çağa uygun olarak bir model geliştirilerek uluslararası dokümantasyona katkı yapılmasının uygun olacağı değerlendirilmektedir.

Güvenlik yaklaşımları çerçevesinde birey, toplum ve devletin güvenliğini sağlamak maksadıyla güvenlik stratejileri tasarlanması ve yönetilmesi gerekmektedir. Bunun yanında güvenlik stratejisi tasarımı başta iş hayatı olmak üzere diğer alanlarda kullanılan strateji tasarımlarından önemli farklılıklar göstermektedir. Bu nedenle bu hususlar dikkate alınarak konusunda uzman ve deneyimli personelin özel olarak yetiştirilmesine ihtiyaç duyulmaktadır. Türkiye'de güvenlik strateji tasarımı ve yönetimi konusunda oldukça az kaynak ve uzman personel bulunmaktadır. Söz konusu personelin yetişmesi için güvenlik stratejisi tasarımı ve yönetimi maksadıyla kullanılan ve genel kabul görmüş klasik modelin kavramsal açıklamasının anlaşılabilir şekilde yapılması gerekmektedir. Dolayısı ile bu tez ile birinci öncelikle güvenlik stratejileri tasarımı ve yönetimi konusu kavramsal olarak ortaya konularak uzmanların yetişmesinde kullanılabilecek millî kaynakçaya katkıda bulunulması hedeflenmektedir.

İkinci öncelikli olarak; dijital çağ stratejik güvenlik ortamındaki yeni tehdit ve aktörler, çok süratle değişen stratejik güvenlik durumu, stratejik şoklar gibi hususların güvenlik stratejileri tasarımına ve yönetimine olan etkilerini incelemek; bu kapsamda güvenlik stratejileri tasarımı ve yönetimi konusunda çağımızda karşılaşılan problemleri tespit etmek ve çözüm önerilerinde bulunmak hedeflenmektedir.

Üçüncü öncelikli olarak dijital çağa uygun bir güvenlik stratejilerinin tasarımı ve yönetimi modeli oluşturulması hedeflenmektedir. Özellikle bilişim teknolojilerinde meydana gelen çığır açıcı teknolojiler insanın daha süratli düşünebilmesini, karar alabilmesini gerektirmektedir. Böyle bir ortamda, tasarlanan güvenlik stratejileri çok kısa zaman içerisinde cari durum ile uyumunu kaybederek geçersiz hale gelmektedir. Yapay zekâ ve büyük veri gibi yeni teknolojik gelişmeler güvenlik stratejilerinin süratle cari duruma uyum sağlayabilmesine ve karar vericilerin süratle durumu kavraması ve karar vermesini sağlayabilecek imkânlar sunabilmektedir. Teknolojik imkânlar kullanılarak güvenlik stratejilerinin tasarım ve yönetiminin dijital çağın şartlarına uyum sağlaması ve etkinliğinin arttırılabilmesi hedeflenmektedir. Bu çerçevede dijital çağda karşılaşılan sorunlara yönelik olarak değişik model önerileri yapılmıştır.

Tez çalışmasının literatüre katkı sağlayabildiği gibi çağımız teknolojileri kullanılarak güvenlik stratejilerinin çağın ihtiyaçlarına ve şartlarına uygun bir şekilde tasarlanmasını ve yönetilmesini sağlayabileceği düşünülmektedir. Söz konusu

teknolojiler ve çağımızın özellikleri dikkate alınılarak bir strateji tasarlama modelinin ortaya konulması birçok açıdan Türkiye'nin güvenlik stratejilerinin tasarımı ve yönetimine katkıda bulunabilecektir.

Türkiye'nin jeopolitik konumu, devam eden ve gelecekte karşılaşılması muhtemel güvenlik sorunları göz önüne alındığında iç ve dış güvenliğe yönelik millî ve yerli, etkin güvenlik stratejilerinin tasarlanması ve yönetilmesi hayati önemi haizdir.

Tezin güvenlik stratejileri tasarımı ve yönetimi konusundaki çalışmalara katkı sağlayabileceği; tasarım ve yönetim konusunda çağımızın özelliklerinin ve sorunlarının ortaya konulması ile gerçekçi ve uygulanabilir çözümlerin, modellerin üretilmesine yardımcı olabileceği değerlendirilmektedir. Ayrıca tezin güvenlik stratejisi tasarımı ve yönetimi konusundaki çalışmalarda faydalanılabilecek bir kaynak olabileceği düşünülmektedir.

Bunun yanında güvenlik stratejileri uzmanlarımızın yerli ve millî bakış açılarıyla başta yapay zekâ ve büyük veri olmak üzere teknolojik imkânları da kullanarak, güvenlik ortamını değerlendirmeleri ve uygulanabilir, dijital çağa uygun güvenlik stratejileri tasarlayabilmelerine yardımcı olunabilecektir.

Klasik güvenlik stratejisi tasarımı genel olarak; nihai hedef, yöntem veya konsept, araç/kaynak (Ends, Ways, Means) olarak tanımlanabilecek başlıklar altında bir süreç takip edilerek oluşturulabilmektedir. Bu süreç aynı zamanda strateji tasarımında kullanılan temel bir model olarak kabul görmektedir. Dolayısı ile temel strateji tasarım modeli, insanın kavrama, değerlendirme, karar verme gibi temel düşünme yeteneklerine uygun olarak inşa edilmiş bir gerçeklik olarak görülebilir. Bu gerçeklik temelinde stratejik tasarımın ve yönetimin dijital çağın şartlarına göre incelenmesi, karşılaşılan sorunların ortaya konulması; yapay zekâ ve büyük veri gibi teknolojikler kullanılarak daha uygun bir modelin ortaya konulması hedeflenmektedir. Bu hususlar dikkate alınarak belirlenen tez sorusu ve hipotezi aşağıda sunulmuştur.

Tezin Sorusu: Klasik güvenlik stratejisi tasarımı ve yönetimi modeli dijital çağın şartlarına cevap verebilmekte midir? Klasik model dijital çağa uygun hale nasıl getirilebilir?

Tezin Hipotezi: Dijital Çağda ortaya çıkan teknolojiler ve bu teknolojilerin güvenlik ortamı ve insan hayatı üzerine etkileri düşünüldüğünde; klasik güvenlik

stratejisi tasarım ve yönetim modelinin çok süratli ve sürekli değişime, stratejik şoklara uyum sağlayabilecek; aynı zamanda yapay zekâ ve büyük veri gibi teknolojik gelişmeleri kullanabilecek bir yapıya dönüştürülmesi gerekmektedir.

Bu çerçevede genel olarak nitel araştırma tekniklerinden keşfedici ve betimleyici yöntemler kullanılarak tümden gelim tekniği ile tez konusu incelenmeye çalışılmıştır. Öncelikle yukarıda belirtilen genel güvenlik stratejisi tasarım modeli, metin ve süreç analiz yöntemleriyle keşfedici bir bakış açısıyla incelenerek model daha kapsamlı bir şekilde ortaya konulmuş ve kavramsal konulara açıklık getirilmeye gayret edilmiştir. Müteakiben dijital çağın ortaya çıkarttığı yeni sorunlar ve sınamalar keşfedici bir bakış açısıyla, kişisel gözlem, durum analizi, metin analizi ve deneyimlerden faydalanılarak incelenmiştir. Tespit edilen sorun alanları ve sınamaların güvenlik stratejilerinin tasarımı ve yönetimine muhtemel etkileri durum analizi ve kişisel deneyimler kullanılarak betimleyici bir yaklaşımla tespit edilmiştir.

Takiben günümüzde yapay zekâ, büyük veri gibi yıkıcı teknolojilerin keşfedici bir yöntemle incelenmesi ve betimleyici bir teknik ile güvenlik strateji tasarımına muhtemel etkileri incelenmiştir. Bu maksatla kişisel gözlem, metin analizi, mevcut yapay zekâ ve büyük veri programlarının güvenlik stratejilerine uygulanma şekillerinin (ARSUS, Hyperion, textfli gibi) incelenmesi gibi metotlar kullanılmıştır. Klasik tasarım modelinin süreç analizinden elde edilen sonuçlar, dijital çağın getirdiği şartlar ve etkiler ile çağdaş teknolojilerin stratejik tasarıma ve yönetime etkileri ile beraber yorumlanarak yeni bir model oluşturulması üzerinde çalışılmıştır.

Kişisel deneyimler, kişisel gözlem konusu çerçevesinde, içeriden/dışarıdan araştırmacı konseptinin (concept of insider/outsider researcher) incelenmesi tezde kullanılan metodolojinin daha iyi anlaşılmasına yardımcı olabilir. Eğer bir araştırmacı üzerinde çalışılan grubun bir üyesi ise içeriden bir araştırmacı olarak nitelendirilmektedir. Araştırmacının grubun üyesi olmaması durumunda ise dışarıdan bir araştırmacı olarak nitelendirilmektedir[1]. Bu çalışmada etkin sonuçlar alınabilmesi için güvenlik, strateji ve teknoloji (mühendislik) konularında yeterli bilgiye sahip olunması gerektiği düşünülmektedir. Çalışmayı yürütenin bahse konu üç alandaki geçmiş deneyimlerinin ve süreç içerisinde biriken örtük bilgisinin içeriden bir araştırmacı olarak teze katkısı olduğu değerlendirilmektedir. Ancak içeriden bir

[1] Bukamal, H. (2022). Deconstructing insider–outsider researcher positionality. British Journal of Special Education, C. 49, S. 3, 327-349.

araştırmacı olmanın iki önemli dezavantajı bulunmaktadır. Bunlar önyargının oluşması ve tarafsızlığın yitirilmesidir. Tez konusunun bir grubun incelenmesi gibi önyargı oluşmasına ve tarafsızlığın yitirilmesine neden olacak bir içerikte olmaması bu dezavantajların minimum seviyede kalmasını sağladığı ifade edilebilir. Buna ilave olarak başta iş dünyası olmak üzere diğer alanlarda strateji konusundaki çalışmaların dikkate alınması ve incelenmiş olması yine bu dezavantajların asgari seviyede kalmasına yardımcı olduğu belirtilebilir.

Diğer taraftan içeriden bir araştırmacı bakış açısıyla tarihi süreçte güvenlik ve stratejinin gelişiminin incelenmesinin, sonuçlar ortaya konulmasının, NATO ve AGİT gibi uluslararası güvenlik örgütlerinden örnekler verilmiş olmasının kavramların daha iyi anlaşılmasına yardımcı olduğu kıymetlendirilmektedir.

Tez üç ana bölümden oluşmaktadır. Birinci bölümde klasik stratejinin tanımına ve tasarım süreci üzerine odaklanılmıştır. Güvenlik stratejileri tasarımı ve yönetimi hem kavramsal hem de uygulama düzeyinde anlaşılır hale getirilmeye çalışılmıştır. Ayrıca strateji olgusunun kavramsal özellikleri de ele alınmıştır. Klasik güvenlik stratejisi tasarım ve yönetim modeli kapsamlı bir şekilde açıklanmıştır.

İkinci bölümde güvenlik ortamındaki ve teknoloji alanındaki gelişmelerin güvenlik stratejisi tasarımı ve yönetimine olan etkileri incelenmiştir. İnceleme sonucunda ortaya çıkan faktörlerin güvenlik stratejisi tasarımına olan etkileri anlaşılmaya çalışılmıştır. Elde edilen bilgiler ile klasik güvenlik stratejisi tasarım ve yönetim modelinin niçin dijital çağ ihtiyaçlarına cevap veremediği sorusu cevaplandırılmaya çalışılmıştır.

Üçüncü bölümde ise elde edilen verilerden dijital çağa uygun, çağın ihtiyaçlarına cevap verebilen; belirsizliklere, çok süratli değişen, stratejik şokları içeren stratejik güvenlik ortamına uyum sağlayabilecek, esnek bir güvenlik stratejisi tasarım ve yönetim modeli ortaya konulmaya çalışılmıştır.

BİRİNCİ BÖLÜM

GÜVENLİK STRATEJİSİ TASARLAMANIN KAVRAMSAL ÇERÇEVESİ

Güvenlik stratejisi tasarlamanın kavramsal çerçevesinin oluşturulabilmesi maksadıyla hem güvenliğin hem de strateji konusunun kavramsal çerçevesinin incelenmesi gerekmektedir. Her iki konunun da herkes tarafından kabul edilmiş bir tanımının olmaması ve tarihi süreçte her iki konunun da değişime uğramış olması kavramsal çerçevenin çizilmesini zorlaştırmaktadır. Bunun yanında strateji tasarlanmasının hem sanat hem de bilimsel yönünün bulunması, ancak göreceli olan sanat yönünün daha ağır basması yine kavramsal çerçevenin çizilmesini zorlaştıran faktörler arasında sayılabilir. Strateji kavramının; oyun kurma, düşünme sistemi oluşturma, taktik seviyede bir faaliyeti açıklamak için kullanılması, bazen de strateji kavramının gizemli, etkileyici, prestij kazandırıcı bir şekilde algıyı yönlendirmesinden de istifade edilmesi strateji tasarımının anlaşılmasını önemli ölçüde olumsuz etkileyebilmektedir.

Diğer taraftan güvenlik stratejisi çalışmalarında genellikle güvenlik yaklaşımlarının incelenmesi üzerinde ağırlıklı olarak durulmaktadır. Ancak gerçek hayatta güvenliğin sağlanabilmesi maksadıyla teorilere, yani yaklaşımlara hâkim olunması yeterli olmamakta, bu yaklaşımlardaki temel düşünceleri de dikkate alan güvenlik stratejisi tasarlanması gerekmektedir. Güvenlik yaklaşımları tasarlanan stratejiye değişik şekillerde katkıda bulunmaktadır. Buna karşın güvenlik yaklaşımlarının strateji tasarlanmasıyla olan ilgisi konusunda literatürde yeterli bilgi ve örnek bulunmamaktadır. Bu nedenle, müteakip maddelerde strateji ve güvenlik kavramlarının üzerinde ayrı ayrı durularak, tarihi süreçteki ve günümüzdeki örnekler güvenlik stratejisi tasarımı mantığının anlaşılabilmesi düşüncesiyle incelenmiş; güvenlik yaklaşımlarının güvenlik stratejisi tasarımına olan etkileri, ilişkisi değerlendirilmiştir. Bu alt yapı üzerine klasik güvenlik stratejisi tasarımı süreç analizi yöntemi ile önce keşfedici bir yaklaşımla incelenmiş ve betimlenmiştir. Bu yöntemle güvenlik stratejisi tasarımının kavramsal çerçevesi müteakip bölümlerde yapılacak incelemelere temel oluşturacak şekilde ortaya konulmaya çalışılmıştır.

1.1.STRATEJİ KAVRAMININ AÇIKLANMASI

Tarihi süreçte strateji kavramının kullanımı incelendiğinde; strateji kavramının genel olarak savaşın yönetimi anlamında ağırlıklı olarak askeri olarak kullanıldığı görülmektedir. Günümüzde "stratejik çalışmalar" olarak adlandırılan disiplin esas itibar ile bu konu ile yani savaşın askeri yöntemler ile yönetimi üzerine yoğunlaşmaktadır.

Strateji konusunda çalışma yapan çevreler genellikle üç düşünüre ağırlıklı olarak atıfta bulunurlar. Bunlar Thucydides, Sun Tzu, Carl von Clausewitz'dir. Bu düşünürler strateji kavramından daha ziyade tarihi süreçleri, gelişmeleri ortaya koyarak analizler yapmışlardır. Bu analizler bugün strateji konusunda yapılan çalışmalara önemli girdiler oluşturmaktadır. Thucydides özetle; savaşların niye çıktığını, niçin gerilimin tırmandığını, niçin savaşın sonlandırılmasının zor olduğunu ortaya koymaya çalışmıştır[2]. Thucydides "Peloponez Savaşı" adlı eseri ile başta "mahkûm ikilemi" olmak üzere uluslararası ilişkiler yaklaşımlarına önemli katkıları olmuştur. Bu eserle Thucydides'in realizmin ilk kaynaklarından birisini ortaya koyduğunu ifade etmek yanlış olmayacaktır. Bu çerçevede Thucydides "güçlünün yapabileceğini yapacağı, güçsüz olanların ise bunu kabullenmek zorunda olduğu" fikrini ileri sürmek suretiyle stratejik düşüncenin özünü güç kavramı ile ilişkilendirmiştir. Benzer bir yaklaşımı Machiavelli'nin strateji anlayışını yansıttığı "Prens" ve "Savaş Sanatı" adlı eserlerinde de görmek mümkündür. Ayrıca Thucydides söz konusu eserinde şehir devletleri ve Pers krallığı arasındaki ittifak ilişkileri, güç dengesi kurma gayretleri, diplomatik süreçler, savaşın politik hedeflere yönelmesi, savunma planlaması kapsamında güç oluşturulması (uzun gemilerin savaş için, yuvarlak gemilerin kargo için kullanılması)[3], deniz (Atina) ve kara (Sparta) gücü arasındaki strateji/taktik savaşları gibi konuları ele alarak günümüz güvenlik stratejileri çalışmalarına önemli katkılar sunmaktadır.

Sun Tzu ise "Savaş Sanatı" isimli eseri ile bir liderin nasıl davranması ve savaşı sevk ve idare etmesi gerektiğini açıklamaya çalışmıştır[4]. Sun Tzu genel olarak dolaylı tutum, istihbarat, aldatma, psikolojik harp gibi günümüz savaşlarının sevk ve idaresine yönelik önemli düşünceler ortaya koymuştur. Bu yöntemler kullanılarak "savaşmadan savaşın kazanılmasını" ön plana çıkartmıştır. Başta Çin olmak üzere Asya'daki

[2]Thucydides, *Peloponnesian War*, Çev. Martin Hammond, Oxford World's Classics, 2009.
[3]Thucydides, *Peloponnesian War*, Çev. Martin Hammond, Oxford World's Classics, 2009, s. 546.
[4]Finney, K. Nathan, *On Strategy: A Primer,* 2020, s. 26.

aktörlerin günümüzde hâlâ bu strateji/taktikleri kullandıkları görülmektedir. Çin'in mümkün olduğu kadar çatışmadan kaçınması bu anlamda iyi bir örnek olarak değerlendirilebilir.

Clausewitz "Savaş Üzerine"[5] isimli eserinde ise Sun Tzu'nun aksine savaşta dolaylı tutum yerine direkt yaklaşımı ön planda tutmuştur[6].Günümüzde strateji oluşturmada kullanılan; ağırlık merkezi, savaşın belirsizlik ortamı (fog of war), savaşın planlandığı gibi icra edilemeyeceği (friction), savaşın politik hedefin ele geçirilmesine odaklanması gerektiği, savaşın başlı başına bir olay olmadığı, politikanın bir devamı olduğu gibi konular bu eserde ortaya konulmaktadır. Sun Tzu'nun aksine Clausewitz rakip ordunun etkisiz hale getirilmesi gerektiğini ifade etmektedir. Diğer önemli bir konu ise klasik strateji oluşumunda kullanılan; hedef, konsept, kaynak (güç unsuru) üçlüsünün ortaya çıkışı da yine Clausewitz'in "Savaş Üzerine" adlı eseriyledir. Clausewitz eserinde; "Tek bir muharebede[7] silahlı kuvvetlerin kullanımına taktik denilirken; savaşın amacını gerçekleştirmek için bu muharebelerin kullanılması düşüncesini ise strateji" olarak tanımlamaktadır.

Strateji konusunda çalışacak uzmanların bu üç düşünürün eserlerini okuması ve düşünme sistemlerini kavraması başarılı olmalarında önemli bir yer tutacaktır. Bunun yanında üç düşünürün de savaşın doğasının yani temel kuram ve kurallarının değişmeyeceği, karakterinin veya yöntemlerinin değişebileceğine yönelik tespitleri bugün için de strateji konusunda çalışma yapan çevreler tarafından geçerliliğini koruduğu düşünülmektedir.

Tarihi süreç içerisindeki gelişiminden de görüleceği üzere strateji kavramı milletlerin kaderlerini belirleyen en önemli olgulardan birisi olan savaşların sevk ve idaresi çerçevesinde askeri alanda ortaya çıkmıştır. İkinci Dünya Savaşı'nın sonuna kadar sadece askeri alanda kullanılan "strateji" kavramı, ilke ve yöntemleri savaş sırasında uygulanan bazı bilimsel yöntemlerden elde edilen başarılı çalışmalar neticesinde bilimsel alana taşınmış; Soğuk Savaş döneminde bilimsel anlayışın yaygınlaşması ile birlikte, strateji kavramının bilimsel yönü gelişmeye başlamıştır.

[5]Clausewitz, Carl, On War, 1832.
[6]Finney, K. Nathan, On Strategy: A Primer, 2020, s. 29.
[7] Türk Dil Kurumu Sözlüğü (sozluk.gov.tr), Savaşta yapılan çarpışmalardan her biri, 23 Mart 2023. Özetle savaş ve harp kavramlarının genel olarak aynı anlamı verdiği, muharebe kavramının ise savaşların içerisindeki bir çarpışmayı ifade ettiği görülmektedir.

Strateji kavramı yukarıda vurgulandığı gibi başlangıçta orduların sevk ve idaresi anlamında kullanılmış olmasına rağmen 1960'lardan sonra iş hayatında da kullanılmaya başlanmıştır[8]. Bu çerçevede Richard Rumelt (Good Strategy Bad Strategy), Michael Porter (Competitive Strategy) gibi düşünürlerin önemli eserleri bulunmaktadır. İş insanları strateji oluşturma konusunu başlangıçta askerlerden almış olmalarına rağmen, günümüzde strateji oluşturma, plan hazırlama, stratejik yönetim modellerinin oluşturulması gibi konularda önemli bir aşama kaydetmişlerdir. Bununla beraber 1990'lı yıllardan itibaren kamu yönetimi alanında da kullanılmaya başlanan strateji kavramı günümüzde güç oluşturma, politika, felsefe, tarih, işletme vb. pek çok farklı disiplinle ilişkili bir şekilde; savunma planlamasından kamu yönetimine, spordan pazarlamaya kadar birçok alanda kullanılmaktadır. Hatta askerlerin bazı alanlarda başta iş hayatında kullanılan modeller olmak üzere diğer disiplinlerdeki yaklaşımları esas almaya başladığı da görülmektedir. Herkesin stratejiye ihtiyacı vardır. Ancak strateji kavramının her kullanımı aynı anlamı ifade ettiğini söylemek pek mümkün değildir. Strateji kavramının kullanıldığı disiplinlere göre farklılıkların olduğu görülmektedir.

Strateji kavramının kullanımı incelendiğinde çok farklı ve değişik sonuçlar ile karşılaşılmaktadır. Strateji kavramının bazen oyun kurma, bazen düşünme sistemi oluşturma, bazen de taktik seviyede bir faaliyeti açıklamak gibi maksatlar ile kullanıldığı görülmektedir. Bazen de strateji kavramının gizemli, etkileyici, prestij kazandırıcı bir şekilde algıyı yönlendirmesinden istifade edildiğine şahit olunmaktadır.

Daha önce belirtildiği gibi strateji kavramının günümüzde tanımı konusunda bir uzlaşı mevcut değildir. Genel kabul gören bir tanımın olmaması strateji kavramının ve kuramının anlaşılmasını zorlaştıran önemli faktörlerden birisidir. Tarihi süreçte strateji kavramının sürekli değişmesi kavramın anlaşılabilir şekilde kullanılmasını engelleyen bir sebep olarak karşımıza çıkmaktadır. İnsan beyninin genel olarak taktik olarak, yani bugünü ve basit düşünmeyi tercih etmesi strateji kavramının anlaşılmasını zorlaştıran önemli faktörler arasında sayılabilir. İnsanoğlu için uzun vadeli ve geniş kapsamlı düşünmek kolay elde edilen bir yetenek olarak görülmemektedir. Bunun yanında strateji oluşturmanın sanat yönünün daha ağır basması hususu da dikkate alındığında strateji kavramının anlaşılmasının niçin zor olduğu daha iyi anlaşılabilecektir. Belirtilen hususlar dikkate alındığında başlangıç olarak strateji kavramının harbin sevk

[8]Grattan, F. Robert, The Strategy Process; A Military-Business Comparison, 2002, s. 10.

ve idare seviyesindeki yerinin incelenmesi kavramın daha iyi anlaşılmasına yardımcı olabilecektir.

1.1.1. Harbin Sevk ve İdare Seviyeleri

Günümüzde harbin sevk ve idaresinde dört seviyenin kullanıldığı genel kabul gören bir yaklaşımdır. Bunlar; politik, stratejik, operatif ve taktik seviyelerdir. Politik seviye bilindiği gibi hükümet seviyesinde verilen kararlardan oluşmaktadır. Bu kararlardan bazıları; savaş ilan edilmesi, kimin düşman, kimin müttefik olacağı, millî menfaatler, tehdit ve risklerin tespit edilmesi gibi kararlardır. Bu kararlar seçimle işbaşına gelmiş bir hükümetin olduğu bir durumda, milletin iradesini yansıtacak şekilde verildiği kabul edilen kararlar olarak kabul edilebilir. Harbin başında bu hususların yer aldığı bir politik direktifin hükümet tarafından yayımlanmasını müteakip askeri stratejinin oluşturulmasına başlanır. Tarihi örnekler incelendiğinde strateji kavramının genel olarak verilen politik hedeflere ulaşmak için muharebelerin birbirleriyle uyumlu şekilde kullanılmasını içerdiği ifade edilebilir. Bu çerçevede strateji kavramının yalnızca askeri yöntemlerin kullanılmasını içerdiği tespit edilebilir. Ancak günümüzde strateji kavramının daha ziyade politik seviye ile müteakip seviyeler arasında bir köprü anlamında kullanıldığı görülmektedir. Daha önce, barış zamanında hazırlanan stratejiler varsa yeni gelişen durum çerçevesinde gözden geçirilerek güncellenebilir. Yine bu çerçevede her bir harekât alanına yönelik olarak operatif planlama (tasarım) yapılabilir. Operatif planlamada her bir muharebenin verilen stratejik hedeflere yönelik olarak icra edilebilmesi maksadıyla planlama yapılmaktadır. Anlaşılacağı üzere daha önce tarihi süreçte strateji olarak kullanılan kavram yerini kısmen de olsa operatif seviyeye bırakmıştır. Bu kavramın anlaşılmasını ve etkin olarak kullanılmasını olumsuz etkilemiştir. Taktik seviyede ise her bir muharebenin icrasına yönelik planlama yapılmaktadır. Unutulmaması gereken önemli bir husus bu süreç veya seviyeler içerisinde bulunulan duruma göre yeniden gözden geçirilebilir, şartlara uygun hale getirilebilir. Bu anlamda tarihi süreçte görüldüğü gibi bazen operatif planlama atlanabilir, direkt olarak stratejiden taktik planlamaya veya icraya geçiş sağlanabilir.

Millî güvenlik açısından konu incelendiğinde; barış zamanında politik direktif yerine Millî Güvenlik Siyaset Belgesi hazırlanabilir. Bu belge esas alınılarak Millî Güvenlik Stratejisi hazırlanır. Millî Güvenlik Siyaset Belgesi ile Millî Güvenlik

Strateji Belgesinin birleştirildiği ortak bir doküman da oluşturulabilir. Millî Savunma Stratejisi hazırlanabilir. Buraya kadar güvenlik anlamında verilen kararların ağırlıklı olarak politik seviyede olduğu ifade edilebilir. Bu dokümanlar esas alınarak Millî Savunma Stratejisi ile uyumlu Askeri Strateji hazırlanır. Politikadan stratejiye geçiş burada başlar. Askeri Stratejinin esas görevi Millî Savunma Stratejisinde verilen esaslar veya görevler doğrultusunda askeri-politik seviyede yapılması gerekenleri ortaya koymaktır. Bir anlamda politik olarak verilen direktifin askeri dile çevrilmesidir. Yani strateji politik seviyeden operatif veya askeri profesyonel seviyeye bir köprü olarak değerlendirilebilir. Aynı husus güvenlik konusunda etkin olan iç güvenlik, diplomasi gibi alanlarda da geçerlidir. Hatta benzer mantığın, felsefenin iş hayatında da geçerli olduğunu ifade etmek yanlış olmayacaktır. Askeri Stratejinin oluşturulmasını müteakip operatif seviye olarak nitelendirebileceğimiz her bir harekât alanına yönelik ağırlıklı olarak askeri hususların yer aldığı bir operatif seviye plan hazırlanır. Bu planda stratejik seviyede belirlenen hedeflerin taktik seviyedeki faaliyetler ile birleştirilmesi yani köprü kurulması gerçekleştirilir. Taktik seviye planlama ise yalnızca bir muharebe veya faaliyete ait bir planlamadır.

Yukarıda belirtilen dört seviyede üretilen dokümanların birbirleri ile uyumlu olması çok önemlidir. Taktik seviyede icra edilecek faaliyetlerin stratejik seviyede belirlenen hedeflere ulaşmayı sağlayacak şekilde belirlenmesi topyekûn savaşın kazanılmasını sağlayacaktır. Taktik seviye ile stratejik seviyenin uyumlu olmaması muharebelerin veya faaliyetlerin boşa icra edilmiş olmasına, kaynak ve emek sarfına neden olabilecektir. Günümüzde taktik seviyede meydana gelen olayların strateji ve hatta politik sonuçlarının olabileceği de göz önünde bulundurulmalıdır. İlave olarak günümüzde artık harbin sevk ve idaresi yalnızca askeri yöntemler ile yapılmamaktadır. İleriki bölümlerde bu hususa yönelik güvenlik paradigmasının değişimi konusunda inceleme yapılacaktır.

Konunun daha iyi anlaşılabilmesi maksadıyla uluslararası bir örnek üzerinde inceleme yapılabilir. En önemli güvenlik örgütlerinden birisi olan Kuzey Atlantik Anlaşması Örgütü'nde (North Atlantic Treaty Organization, NATO) bu seviyelerin oldukça iyi bir şekilde, kendi yapısına uygun olarak ortaya konulduğu görülmektedir. Kuzey Atlantik Konseyi (North Atlantic Council, NAC) NATO'nun politik karar verici organıdır. Ülkelerin güvenlik konusundaki politik iradeleri bu konseyin kararlarına yansımaktadır. Belçika'nın Mons kentinde konuşlu stratejik veya askeri

politik seviye karargâh olan Avrupa Müttefik Kuvvetleri Yüksek Karargâhı (Supreme Headquarters Allied Powers Europe, SHAPE) ise NATO'nun Genelkurmay Başkanlığı gibi çalışmaktadır. Yani NAC tarafından verilen politik kararların askeri stratejik seviyeye tercümesi ve stratejinin hazırlanması bu karargâhta yapılmaktadır. Müşterek Kuvvet Komutanlığı (Joint Force Command, JFC) ise operatif seviye planlama yapmaktadır. Daha aşağı seviyedeki kara, deniz ve hava komutanlıkları ile daha aşağıdaki birliklerde taktik seviye planlamalar ve icralar yapılmaktadır. Ancak, NATO'nun bu yapılanmayı kendi ihtiyaçları, içinde bulunulan şartlara göre değiştirdiği ve şartlar değiştikçe gözden geçirdiği, şartlarla uyumlu hale getirdiği unutulmamalıdır.

Bu incelenen dört seviye değişik alanlara uyarlanabilir. Örneğin bankacılıkta yönetim kurulu tarafından alınan politik kararların, bankanın merkezi teşkilatı tarafından stratejiye dönüştürülmesi ve stratejik planlama yapılması, bölge temsilcilikleri tarafından operatif planlama yapılması, şubeler tarafından ise taktik seviye bir planlamanın yapılması bu çerçevede dikkate alınabilir. Unutulmaması gereken konu bankacılık, satış pazarlama, sağlık gibi değişik alanların kendi şartlarının olduğu ve bu şartlara uygun seviyelerin belirlenmesi gerektiğidir.

1.1.2. Strateji Kavramının Tanımı

Strateji kavramının tarihi süreçte değişik stratejistler tarafından nasıl ortaya konulduğunun incelenmesi kavramın anlaşılmasına yardımcı olabilmektedir. Bu anlamda ilk olarak Clausewitz'in strateji üzerine çalışmaları günümüzde bu konudaki çalışmalara önemli bir referans oluşturmuştur. Clausewitz harbi "irademizin hasmımıza zorla kabul ettirilebilmesi maksadıyla şiddetin kullanılması" olarak tanımlamaktadır[9]. Diğer önemli bir tanım ise "harbin politikanın diğer araçlarla devam ettirilmesi" şeklinde verilmektedir[10]. Bu çerçevede strateji ise "muharebelerin harbin hedefine ulaşmak maksadıyla araç olarak kullanılması" şeklinde tanımlanmaktadır[11]. Bu tanımlar birleştirildiğinde; strateji kavramının savaşın kazanılması için bir savaş planı olarak algılandığı sonucuna varılabilir. Clausewitz'in yaklaşımının stratejinin

[9]Clausewitz Carl, *On War*, 1832, s. 44.
[10]Clausewitz Carl, *On War*, 1832, s. 70.
[11]Clausewitz Carl, *On War*, 1832, s. 257.

yalnızca muharebelerin kullanımı çerçevesinde ele alındığı dar bir çerçeveye sıkıştırıldığı tartışılmaktadır.

Prusyalı General Helmuth Karl Bernhard von Moltke (1800-1891) stratejiyi askeri bir bakış açısından "Generallerin emrine verilen araçların savaşın amacına erişmek üzere pratik düzeyde uygulanmasıdır." şeklinde ifade etmektedir[12]. Bu tanımda hükümet tarafından harbin genel olarak yönetildiği, bu çerçevede Genelkurmay Başkanlığının emrine kuvvetler ve kaynaklar tahsis ettiği, bu kuvvetlerin ve kaynakların emredilen hedeflere ulaşılmasında başarıyla kullanılmasının ise komutanın sorumluluğunda olduğu ön plana çıkmaktadır.

Liddell Hart ise bu tanımları birleştirerek stratejiyi "askeri araçların politik nihai hedeflere ulaşılması için tahsis edilmesi (dağıtılması) ve kullanılması sanatı" olarak tanımlamaktadır[13].

Strateji kavramı Türk Dil Kurumu sözlüğünde; "Bir ulusun veya uluslar topluluğunun, barış ve savaşta benimsenen politikalara destek vermek amacıyla politik, ekonomik, psikolojik ve askerî güçleri bir arada kullanma bilimi ve sanatı, sevkülceyş"[14] olarak tanımlanmaktadır.

ABD Müşterek Doktrini Dokümanına göre strateji; "Millî güç unsurlarının koordineli ve bütüncül bir yaklaşımla harekât alanı, milli ve uluslararası seviyede kullanılması için oluşturulan düşünce veya düşüncelerdir." şeklinde tanımlamak mümkündür[15].

Buraya kadar verilen tanımlar incelendiğinde stratejinin; bir yol haritası, politik seviye ile taktik seviye (operatif seviye) arasında bir köprü, mevcut durum ile ulaşılması istenen nihai hedef (vizyon) için planlama, eldeki kaynaklar ile nihai hedefe ulaşılması için yapılan çalışma gibi değişik tanımları ortaya çıkmaktadır. Stratejinin başta iş hayatı olmak üzere değişik meslek gruplarında kullanıldığından hareketle, her bir tanımın işaret ettiği yöntem söz konusu meslek grubunun özelliklerine ve amaca uygun olarak kullanılması mümkündür. Güvenlik stratejisinin tasarlanmasında ise güvenlik yaklaşımlarından faydalanılabilmektedir.

[12]Hart, Liddell, The classic book on military strategy; *Strategy*, 1991, s.320.
[13]Hart, Liddell, The classic book on military strategy; *Strategy*, 1991, s.321.
[14] Türk Dil Kurumu Sözlüğü, 2005, s.1811.
[15] Joint Doctrine 1-18, Strategy, s I-1.

1.2. TARİHİ SÜREÇTE STRATEJİ VE GÜVENLİK İLİŞKİSİNİN İNCELENMESİ

İnsanlar tarihin bütün dönemlerinde güvenliğe ihtiyaç duymuş ve önem vermek zorunda kalmıştır. Bu nedenledir ki askerlik ve polislik dünyanın en eski mesleklerindendir. Bu çerçevede tarihi süreçte güvenlik konusunda önemli çalışmalar yapılmış olmasına rağmen, çalışmaları ve buna bağlı olarak güvenlik stratejisi tasarlanması konuları akademik olarak oldukça yenidir. Güvenlik çalışmaları önce Uluslararası İlişkilerin bir bölümü olarak çalışılmış, özellikle İkinci Dünya Savaşı'nı takiben ayrı bir çalışma alanı olarak ortaya çıkmıştır. Bu nedenle oldukça yeni bir akademik çalışma alanı olarak değerlendirilmektedir.

Güvenlik çalışmaları önce pratikte ortaya çıkmış, müteakiben yaklaşımlar üretilmeye başlanmıştır. Güvenlik tarihin eski çağlarında, önce bireyin fiziki güvenlik ihtiyacı olarak ortaya çıkmış, toplum halinde yaşamanın bir gereği olarak şehir devletlerinin oluşması ve bireyin güvenliğinin şehir devletleri tarafından sağlanması şeklinde süreç devam etmiştir. Roma İmparatorluğu döneminde sağlanabilen güvenlik Ortaçağda derebeyleri tarafından sağlanmaya başlanmıştır. Vestfalya Anlaşması (1648)[16] ile beraber egemenlik ve toprak kavramlarının devletin temel unsurları olarak uluslararası sistemde kabul edilmesiyle beraber güvenlik kavramı daha belirgin olarak ortaya çıkmaya başlamış, Soğuk Savaş döneminde ise önemli bir yere sahip olmuştur. Bu çerçevede devletlerin yanında ittifaklar tarafından ülkelerin sınırlarının ve egemenliklerinin güvenlik stratejileri oluşturularak korunması ön plana çıkmıştır.

Dar anlamda güvenlik, özellikle Soğuk Savaş dönemi dâhil ağırlıklı olarak askeri tedbirler kullanılarak devlet, ülke ve/veya milletin güvenliğinin sağlanması olarak benimsenmiş, politika ve diplomasi gibi yöntemler, araçlar buna ilave edilmiştir. Günümüzde ise yaşamın her alanında değişik şekillerde ve seviyelerde olsa dahi güvenlik önem kazanmıştır. Bu nedenle güvenlik probleminin anlaşılması ve çözümler üretilebilmesi için yaklaşımlar, yöntemler, stratejiler ortaya konulmuştur. Bununla beraber İkinci Dünya Savaşı öncesi savaş çalışmaları, savunma, askeri strateji ve jeopolitik çalışmalar ağırlıklı olarak devletin veya devletlerin güvenliğini, uluslararası güvenlik sisteminin anlaşılmasına ve yönlendirilmesine odaklanan güvenlik

[16]Arı, Tayyar, Uluslararası İlişkiler ve Dış Politika, 2013, s.39.

çalışmaları olarak karşımıza çıkmaktadır. İkinci Dünya Savaşı'ndan sonra stratejik çalışmalar ve barış çalışmaları ortaya çıkmaya başlamıştır. Bu dönemde stratejik çalışmalar caydırıcılığın sağlanması, silahların kontrolü gibi nükleer silahların kullanılmasının engellenmesi üzerinde yoğunlaşmaktadır. Barış çalışmaları ise özetle ekonomi, çevre gibi barış ortamının sağlanması için gerekli olan diğer alanlara odaklanmıştır. Savaş veya çatışma olmaması anlamındaki geleneksel güvenlik anlayışı yapısal şiddetin olmamasını da içerecek şekilde pozitif barış konsepti olarak tanımlanmaya başlamıştır. Dolayısı ile bir toplumda barışın olması için iyi kurallar, iyi komşuluk, insan haklarına saygı, yolsuzlukların engellenmesi, iş güvenliğinin sağlanması, kaynakların adaletli dağıtılması gibi diğer şartların da olması gerektiğine odaklanan bir güvenlik anlayışı kabul görmeye başlamıştır. Çağdaş güvenlik çalışmaları birey, devlet, uluslararası sistemi de içeren daha geniş bir analiz düzlemi üzerinde yoğunlaşmıştır.

Güvenliğin değişik algılama ve tanımlarının bulunmasının temel nedenlerinden birisi toplumların veya devletlerin güvenlik ihtiyaçlarının farklı olması olarak gösterilmektedir. Ortak görüş olarak güvenliğin tanımı ise "tehdit veya risklerin olmaması, korku içerisinde yaşamamak" olarak özetlenebilir. Tarihi süreçte güvenlik derinlemesine aktör çeşitliliği artarak; genişliğine ise ilave alanları içerecek şekilde genişlemiştir.

Teknolojinin getirdiği yenilikler, keşif ve icatlar, insanların bilgi seviyesinin artması, yeryüzünün şartlarının değişmesi gibi faktörler nedeniyle tarihi süreçte strateji ve güvenlik ilişkisi evrime uğramıştır. Bu evrim Tarım Çağı ve Sanayi Çağı ile başlayan değişik dönemler halinde incelenebilir. Müteakip maddelerde değişik dönemlerdeki strateji ve güvenlik ilişkisi incelenmeye çalışılacaktır. Dijital Çağ ise müteakip bölümlerde ayrı olarak incelenecektir.

1.2.1.Tarım Çağı

Güvenlik olgusunun temel yapısını ve evrimini anlamakta modern devlet anlayışının ortaya çıkışı önem taşımaktadır. Ortaçağ'da toprak esaslı devlet yapısının benimsenmesi ve monarşiden milli devlet anlayışına geçiş güvenlik kavramının anlaşılmasında iki önemli dönemi yansıtmaktadır. Ortaçağda devletin iki temel unsuru kilise ve siyasi yapı olduğu bilinmektedir. Bu çerçevede iki kılıç kuramı ağırlıklı

olarak kullanılmıştır. Bu dönemde daha ziyade Papa'nın kontrolünde imparatorluklara, prensliklere, derebeyliklere toplulukları yönetmek için statü verilmiştir. Topraklar kralın veya onun yetki verdiği prenslerin, kısacası soyluların elinde bulunmaktadır. Bu dönemde ağırlıklı olarak tarım toplumunun egemen olduğu, güvenlik yapılarının tarım toplumuna göre tasarlandığı görülmektedir.[17] Tarım toplumunda güvenlik anlayışı; krallığın güvenliği, köylülerin tarımda rahat çalışmaları ve yeni topraklar ele geçirerek daha da güçlenmek, zenginleşmek olarak özetlenebilir. Bu çerçevede güvenlik stratejileri ağırlıklı olarak orduların hazırlanması ve düşmana üstün gelecek şekilde kullanılmasına odaklanmıştır. Doğal olarak ordular ve güvenlik stratejileri de kaynak ihtiyacını karşılayacak şekilde tarım toplumunun yapısına ve teknolojiye göre şekillendirilmiştir.

Bunun yanında tehdit ve risklerin belirlenmesinde dinin de egemen olması neticesinde birçok din savaşının yaşandığı bilinmektedir. Karşı dinin veya mezhebin bir tehdit veya risk olarak algılanması güvenlik stratejisi tasarımında önemli bir yere sahip olmuştur. Hatta bazen din konusu güvenliğin temel parametresini teşkil etmiştir. Haçlı seferleri bunun en güzel örneklerinden birisini oluşturmaktadır.

Niccolo Machiavelli (1469–1527) tarafından 1513 yılında yazılmış, 1532'de yayımlanmış "Prens" isimli kitap bu dönemin yönetim ve güvenlik sisteminin anlaşılması için önemli bir eserdir. Eserde özet olarak hükümdarın iktidarını nasıl güçlendirip idame ettirebileceğine yönelik önemli tespitler yer almaktadır.[18] Dönemin güvenlik anlayışı kralın veya prensin hükümranlığını idame ettirebilmesidir. Yani esas olan toprağın sahibi olan kralın elindeki toprakları muhafaza edebilmesi, tebaasına hükmetmesi, hükümranlığını genişletebilmesi, olarak özetlenebilir. Machiavelli krala uygulayabileceği güvenlik stratejisinin temellerini verirken, güvenliği sağlamada kullanabileceği iyi bir ordunun da nasıl oluşturulabileceği konusunda tavsiyelerde bulunmakta, bir anlamda savunma politikasını açıklamaktadır. Thukidides'den (Thucydides, MÖ 471-400) sonra realist güvenlik yaklaşımının ve güvenlik stratejisi oluşturulmasının temellerinin atılmasında önemli etkisinin olduğu ifade edilebilir. Benzer anlamda Fransa'nın dönem itibarı ile benimsediği "tek kral, tek iman, tek kanun" prensibi de güvenlik anlayışının ve stratejilerinin dayandığı parametrelerin

[17] Özpolat, Haşim, "Tanrının Siyasetinden Siyasetin Tanrısına Egemenlik Kuramının Dönüşümü", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,* C. 23, S. 2, İstanbul 2017.
[18]Machiavelli, Niccolo, *The Prince (1513).* Hertfordshire: Wordsworth Editions, 1993.

anlaşılmasına yardımcı olabilir. Fransa için güvenlik stratejisinin temeli; tanrıdan yetkisini alan ve Katolik inancını benimsemiş kralın koyduğu kanunlara dayanarak bir devlet yapısı ve bu yapının güvenliğinin sağlanmasıdır.[19]

Ortaçağ anlayışında modern devlet anlayışına geçiş güvenlik kavramının gelişiminde etkin rol oynamıştır. Vestfalya Anlaşması 30 yıl süren din savaşlarını müteakip devletlerin sınırlarının ve bu sınırlar içerisinde egemenliklerinin tanınması açısından önem kazanmaktadır. Egemen modern devletin ilk adımlarının atılmasının yanında uluslararası güvenlik sistemi ve güvenlik stratejisi tasarımı ihtiyacı yavaş yavaş ortaya çıkmaya başlamıştır.

Thomas Hobbes (1588-1679) tarafından yazılmış olan ve 1651'de yayınlanan, din ve dünya devletinin içeriğini ortaya koyan Leviathan[20] bu dönemin devlet ve güvenlik anlayışını yansıtan önemli bir eserdir. Hobbes insanların doğa durumda birbirlerinin güvenliğini olumsuz etkilediklerini, bu nedenle güçlü bir düzen kurucuya ihtiyaçları olduğunu açıklamaktadır. Bu düzen kurucuya Leviathan adını vermektedir. İnsanlar egemenliklerini Leviathan'a devrederek güvenli bir ortam yaratılmasını sağlamaktadırlar. İnsanlar özgürlüklerinden vazgeçerken güvenliklerinin Leviathan tarafından sağlanmasını kabul etmektedirler. Leviatan'ın bir elinde kılıç, diğer elinde ise dini kontrol eden bir asa bulunmaktadır. Dolayısı ile Leviatan, Vestfalya Anlaşması sonrasında egemenliği ve sınırları belirlenmiş olan krallıkların veya devletlerin toplumlarının ulus haline gelmesinde önemli bir yer tutmaktadır. Leviatan'ın gücü ve orduyu temsil eden kılıçla savunmayı ve iç güvenliği sağlarken; kiliseyi yönlendirerek huzurlu bir toplum yaratarak iç güvenliğe de önemli katkı yaptığı düşülmektedir. Bu anlamda Leviatan konsepti günümüzdeki iç ve dış güvenlikten oluşan millî güvenlik stratejisinin ilk uygulaması olarak düşünülebilir. Yine realist bir güvenlik yaklaşımıyla hazırlanmış bir eserdir. Kitabın diğer önemli bir katkısı mülk konusudur. Güvenliğin olmadığı bir toplumda mülk edinmek anlamsız olacaktır. Doğa durumunda olan bir toplumda bireylerin elde ettikleri mülk daha güçlü bir birey veya bireyler tarafından gasp edilecektir. Bireylerin Leviatan ile yaptıkları sözleşme neticesinde iç güvenlik sağlanabilecek, kişiler mülk edinmek için emek harcayabilecek, hatta mülklerini çocuklarına miras olarak bırakabileceklerdir. Kişiler özgürlüklerinden

[19]Özdemir, Hakan, ve Bakan, Selahaddin (2016). Ulus devletin oluşumu ve sorunları açısından Almanya ile Fransa'nın karşılaştırılması. *Bitlis Eren Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, C. 5, S.3, s.19-58.
[20]Hobbes, Thomas, *Leviathan*, 1651.

vazgeçmişlerdir. Ancak dışarıya karşı ve içeride güvenlikleri sağlanmış, mülkün temeli olan adalet sağlanmış olacaktır. Leviatan sayesinde güvenlikleri sağlanmış bireyler mülk edinmek için emek harcayabilecek, ülkenin ileri gitmesine katkı sağlayacaktır. Mülk edinebilme sayesinde tüccarlar, yani burjuva yeni bir sınıf olarak ortaya çıkmıştır. Sanayi devriminin güvenlik yaklaşımlarının ve buna bağlı olarak stratejilerinin temelleri atılmaya başlamıştır.[21]

Klasik liberalizmin önemli düşünürlerinden olan John Locke (1632-1704) "Toplum sözleşmesi" teorisinin ikinci önemli düşünürüdür. Locke, Hobbes'in doğa durumuna katılmamakta; doğa kanunu olduğuna, bunu da insanların aklı sayesinde keşfedebildiğini ileri sürmektedir[22]. Dolayısı ile bireylerin özgürlükleri ile güvenlikleri arasında bir tercih yapmaları gerektiğinde Hobess güvenlik konusuna daha fazla ağırlık verirken Locke bireyin özgürlüğüne daha fazla ağırlık vermiştir. Bu nedenle bireyin mülk edinmesi konusunu daha ağırlıklı gündeme getirmiş, Hobbes ise devlet güvenliğine öncelik vermiştir. Her iki düşünürün güvenlik konusundaki yaklaşımları yaşadıkları deneyimle direkt ilgilidir. Hobbes otuz yıl süren din savaşını ve İngiltere'deki iç savaşı yaşadığı için devlet gibi bir otoriteye bireylerin egemenliklerini teslim ederek huzurun sağlanabileceğini, bunun karşıtı olan doğa durumunun ise kötü sonuçlarının olacağı için tercih edilmeyeceğini ileri sürmektedir. Protestan olan Locke ise İngiltere'deki Katolik baskısının sonuçlarını yaşamış, dolayısı ile insanların özgür olmasını ve kilisenin etkinliğinin sınırlandırmasını ileri sürmektedir. Hobbes güvenlik stratejisi anlayışında devlet güvenliğine öncelik verirken, Locke birey güvenliğine önem vermektedir. Devlet güvenliğine önem veren stratejinin birey güvenliğini tehlikeye atabileceği, bireylerin güvenliklerinin kendi devletleri tarafından olumsuz etkilenebileceği veya başarısız/zayıf devletlerin kendi vatandaşlarına ihtiyaç duyulan güvenliği sağlayamayacağı konusu da göz önünde tutulması gerekmektedir. Her iki düşünürün fikirleri bir araya getirildiğinde birey ve devletin güvenliğinin birbirleri ile bağlantılı olduğu, bu anlamda güvenlik stratejilerinin nihai hedefi güvenliğin birey ve/veya devlet düzeyinde olabileceği sonucuna varılabilir. Her iki düşünürün ortaya koyduğu güvenlik stratejisi yaklaşımları sanayi çağının güvenlik stratejisi yaklaşımlarına önemli bir temel oluşturmuştur.

[21]Hobbes, Thomas, *Leviathan*, 2016, s.200.
[22] Locke, John, *Hoşgörü Üzerine Bir Mektup*, Ankara Liberte Yayınları, 2017.

1.2.2.Sanayi Çağı

Fransız İhtilali ulus düşüncesini ortaya koyarak güvenlik konusunda önemli bir dönüm noktası oluşturmuştur. İhtilal ile birlikte "tek kral, tek iman, tek kanun" yerine "tek kral, tek millet, tek kanun" düşüncesi benimsenmiştir.[23] Dolayısı ile devletlerin ulus inşa süreçleri başlamıştır. Bu maksatla "eşitlik, kardeşlik, özgürlük" temaları benimsenmiş ve hiyerarşik yapı yerine eşit vatandaşlık ortaya konularak, vatandaşların ulus olarak devlete sadakatinin sağlanması amaçlanmıştır. Vestfalya Anlaşması ile egemenlik ve ülkenin sınırları belirlenirken; Fransız İhtilali ile ulus tanımı bu iki parametre ile birleşerek ulus-devletin tarih sahnesindeki yerini almasını sağlamıştır. Bu nedenle devletler artık yalnızca dini veya monarşik anlayışla halkı yönetemeyecek, değerleri, çıkarları ve halkın kimliğini de hesaba katarak yönetmek zorunda kalacaktır. Bu çerçevede Hobbes'un devletin mutlak egemenliği sorgulanmaya başlamış, eğer hükümet halkın çıkarlarına hizmet etmez ise devrilebileceği ortaya çıkmıştır. Devlet vatandaş ilişkisi bu anlamda önem kazanmıştır. Tarım çağının gereği olarak ortaya çıkan toprağa dayalı devlet, dışarıdan gelen tehditlere karşı ülkeyi savunurken veya yeni topraklar zapt ederken, aynı zamanda kralın tacına rakip çıkabilecek, kamu düzenini bozabilecek iç tehditlere karşı da güvenlik stratejisi geliştirmek durumunda kalmıştır. Bu nedenle askeri imkân ve kabiliyetin geliştirilmesi dış ve iç tehdide karşı güvenlik stratejisinin temelini oluşturmuştur. Ulusun ve halk desteğinin önem kazanmasıyla birlikte güç ve halkın kontrolü yanında kamu düzenin önemli unsurlarından olan meşruiyet ve toplumsal uyum da önem kazanmıştır. Dolayısı ile halkın kendi arasındaki uyumu ve hükümete desteği güvenlik stratejilerinin önemli parametreleri haline gelmiştir. Halkın bir kısmının uyum içerisinde olmaması ayrılıkçı düşüncelerin ortaya çıkmasına veya şiddete varacak şekilde iç güvenliğin olumsuz etkilenmesine neden olabilecektir. Ayrıca diğer aktörler tarafından ayrılıkçı hareketlerin teşvik edilebilmesi için verimli bir ortam oluşabilecektir. Güvenlik stratejisi tasarımı artık askeri tedbirlerin ötesinde diğer araçların da dikkate alınmasını gerektirmektedir.

Napolyon, Fransa için idari ve hukuki bakımdan önemli teşkilatlar kurmuş (vali atanması gibi), Yurttaşlar Yasası gibi düzenlemeler yapmıştır. Yasalarda eşitlik,

[23] Özdemir, Hakan, ve Bakan, Selahaddin (2016). Ulus devletin oluşumu ve sorunları açısından Almanya ile Fransa'nın karşılaştırılması. *Bitlis Eren Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, C. 5, S.3, s.19-58.

özgürlük ve mülkiyet vaatleri ön plana çıktığı ifade edilebilir.[24] Güvenlik stratejisi açısından bakıldığında Napolyon'un yeni düzenlemeleri ile Hobbes'un ve Locke'un toplum sözleşmesi kavramını vatandaşların devlete olan bağlılığını artıracak şekilde pekiştirdiği, bunun sonucu olarak orduyu güçlendirdiği, iç cepheyi sağlamlaştırarak dış cephede önemli savaşlar icra ettiği görülmektedir.

Buna ilave olarak toplum sözleşmesi konusunda üç düşünürden birisi olan Jean-Jacques Rousseau'nun (1712-1789) toplum sözleşmesi alanında yaptığı çalışmaların bu dönemde önemli sonuçları olmuştur.[25] Bu çerçevede başta mülk olmak üzere diğer iki düşünüre ilave olarak orta sınıfın oluşmasına yardımcı olacak düzenlemeler konusundaki düşünceleri vatandaşların devlete bağlılığını artırıcı, iç cephenin ve dolayısı ile dış cephede icra edilen faaliyetleri önemli ölçüde destekleyici mahiyettedir. Bu düzenlemelerin devlet güvenliğinin iç ve dış cephe olarak nasıl etkin hale getirilebileceğinin iyi bir örneğini teşkil etmektedir. Bu hususlar Napolyon'un liderlik özellikleri ile birleştiğinde tarihte önemli bir yer edinen Fransa gibi bir ülke ortaya çıkmıştır. Fransa'nın icra ettiği savaşların temel stratejisi artık Katolik mezhebinin yayılması değil, ihtilal ile ortaya çıkan milliyetçiliği esas alan, sanayi çağının güç kazanmaya yönelik düşüncesine dayanmaktadır.

Vestfalya Anlaşması'nın dönem itibari ile din savaşlarının nispeten engellenmesine neden olduğu ifade edilebilir. Buna karşın güvenlik stratejilerinin geliştirilmesinin ana nedeni olan savaşların asıl nedenlerini sanayi çağının temel gereksinimi olan hammadde ele geçirmek, ekonomik ilişkiler, jeopolitik kaygılar gibi hususlar oluşturmuştur. Sonuç olarak sömürgecilik sanayi çağının önemli bir sonucu olarak tarih sahnesindeki yerini almıştır. Devletler sömürgelerine kendi üstün medeniyetlerini götürme görüntüsü altında sömürgecilik faaliyetlerini meşrulaştırmaya, halkların direncini kırmaya yönelik stratejiler geliştirmişlerdir. Gelişmiş devletler uluslarının refah ve huzurlarını sağlamayı esas aldıkları güvenlik stratejilerinde sömürgecilik, köle ticareti gibi yeni yaklaşımlar sergilemeye başlamışlardır. Doğal olarak bu yaklaşımların veya stratejilerin sanayileşmiş ülkelerin

[24]https://www.geeksforgeeks.org , Changes Introduced By Napoleon in the Administrative System, 23 Mart 2023.

[25]Laskar, Manzoor Elahi, *Summary of Social Contract Theory by Hobbes, Locke and Rousseau*, SSRN, 2013.

güvenliğini olumlu etkilemesi öngörülürken, sömürge olarak hedeflenen ülkeler için günümüzde de hâlâ hissedilen güvenlik açısından olumsuz sonuçlara neden olmuştur.

Diğer taraftan Napolyon'un bozduğu Avrupa düzeni 1815 Viyana Anlaşması'yla bir güçler dengesi oluşturacak şekilde "Avrupa Uyumu" adı altında yeniden oluşturulmuştur. Ancak 1871 yılında Alman birliğinin sağlanması, Almanya'nın bu güçler dengesini bozucu ve başta Fas olmak üzere, Fransa ve İngiltere'nin sömürgelerine yönelik tutumu; Balkanlardaki Alman ve Rus menfaatleri Birinci Dünya Savaşı'nın önemli sebeplerini oluşturmuştur. Viyana Anlaşması (1864)[26] ile neorealist ve inşacı güvenlik yaklaşımı yerine yeniden klasik realist güvenlik stratejilerinin benimsenmesi savaşın çıkmasına neden olmuştur. Birinci Dünya Savaşı sonrasında yapılan barış anlaşmalarının Almanya'yı tatmin etmemesi (1919-1939, Versay Düzeni) ve aşırı milliyetçilik akımının etkin olması neticesinde İkinci Dünya Savaşı yaşanmıştır. Birinci Dünya Savaşı sonunda imparatorluklar, İkinci Dünya Savaşı sonucunda ise sömürgecilik ortadan kalkmıştır.

Her iki dünya savaşı da sanayi devriminin güvenlik stratejilerinin bir ürünü olarak görülebilir. Sanayi devriminin güvenlik anlayışında devletin ayakta kalması için üretimin artması, bunun için yeterli hammaddenin ve pazarın elde bulundurulması gerekmektedir. Diğer ülkelerin sanayi ve hammadde açısından kuvvetli olması bahse konu ülke için önemli bir tehdit ve risk olarak algılanmıştır. İkinci Dünya Savaşı sonrasında ise nükleer silah kullanılması savaşların öldürücülüğünü ve yıkıcılığını artırdığından dolayı sıcak çatışmaların, topyekûn savaşların yerine Vietnam ve Kore'de olduğu gibi sınırlı savaşların yaşandığı Soğuk Savaş dönemine girilmiştir.

Tarım çağından farklı olarak sanayi çağında buharlı makinelerin keşfedilmesiyle insanın kas gücünün yerini makinelerin alması, güvenlik stratejilerinin temel yapısını teşkil eden; Millî menfaatler, konsept ve kaynaklar, buna bağlı olarak da strateji, yöntem veya konseptlerin değişmesine neden olmuştur. Millî menfaatler belirlenirken hammaddenin elde edilmesi çerçevesinde sömürgeciliğin esas alınması düşünülmüştür. Kara ve deniz kuvvetlerinin yanında hava kuvvetlerinin sahneye çıkmasıyla savaş stratejileri, güvenlik stratejileri önemli ölçüde değişmiştir. Artık

[26]Avusturya ve Prusya 16 Ocak 1864'de Danimarka'ya savaş açarak bir kısım topraklarını işgal etmişlerdir. Savaşın sonucunda 30 Ekim 1864'de Viyana Antlaşması imzalanmıştır. Alman milliyetçiliğinin zaferi olarak görülen bu savaş ve antlaşma yeniden milliyetçiliğin ve realizmin Avrupa'da ortaya çıkmasına neden olmuştur. (Lesaffer, Randall, Oxford Public International Law, https://opil.ouplaw.com, 23 Mart 2023

stratejiler üç boyut dikkate alınarak hazırlanmak zorunda kalınmıştır. Sanayi devriminde meydana gelen teknolojik gelişmeler çerçevesinde kara muharebelerinde makineli tüfek, demir yolları, kimyasal silahlar, tank gibi yeni silahlar karada icra edilen savaşların; buharlı gemilerin, yeni navigasyon tekniklerinin kullanılmaya başlanması deniz stratejilerinde önemli değişikliğe neden olmuştur. Bu gelişmeler millî güvenlik stratejilerinin geliştirilmesinde önemli değişikliğe neden olurken, aynı şekilde savunma ve kuvvet planlamalarını da temelden değiştirmiştir. Buna karşın dijital çağ başlamasına rağmen hâlâ aynı savaş stratejilerinin, millî güvenlik stratejisi yaklaşımlarının ve orduların kuvvet yapılarının devam ettiği durumlarla çok sık karşılaşılmaktadır.

1.2.3.Soğuk Savaş (Nükleer Çağ)

Sanayi çağının en önemli olgularından birisi olan Soğuk Savaş NATO müttefikleri ile Sovyet Sosyalist Cumhuriyetler Birliği (SSCB) ve uydu ülkeleri arasında 1946-1991 yılları arasında meydana gelmiştir. Soğuk Savaşın temel özelliği sıcak çatışmaya gitmeden iki grup ülkenin hasım tarafı zayıflatırken kendilerini güçlendirmeye çalıştıkları bir kriz/gerginlik durumu olmasıdır. Bu nedenle güvenlik stratejilerinde özellikle caydırıcılık, propaganda ve diplomatik boyutlar ağır basmış, nükleer silahların yıkıcı etkisi de göz önüne alınarak büyük çaplı bir çatışma çıkmamıştır.

Soğuk Savaş dönemi boyunca iki kutuplu bir dünya düzeni oluşmuştur. Soğuk Savaşın askeri açıdan belirleyici özelliği her iki taraf için de düşman durumu, uygulanacak stratejiler, taktikler, tehdit durumu, kullanılabilecek silahlar, muhtemel harekât alanları gibi konuların belli olmasıdır. Diğer bir ifadeyle belirsizlik hemen hemen yok denecek kadar azdır. Güvenlik stratejilerinin tasarlanmasında kullanılan kuvvet, zaman, mekânın biliniyor olması strateji tasarımcılarının işlerinin nispeten daha kolay olmasına neden olmuştur. Ancak nükleer silahların kullanılma olasılığı ve yıkıcılığı, ülkelerin birbirlerinin halklarını örtülü ve gizli operasyonlar ile etkileyerek iç karışıklık çıkarma gibi yeni stratejiler, güvenlik stratejileri tasarımını daha karmaşık hale getirmiştir.

Diğer önemli bir konu ise eskiden askeri ağırlıklı olarak üzerinde çalışılan güvenlik anlayışının yerine daha geniş bir bakış açısının hâkim olmasıdır. Aslında Soğuk Savaş devam ederken, 1970'li yıllardan itibaren savaşın yıkıcı boyutlarının

görülmesi üzerine "yumuşama" (detente) dönemi başlamış ve bunun neticesinde geleneksel güvenlik yaklaşımlarının yanında yeni güvenlik yaklaşımları üzerinde çalışmalar başlamıştır.

NATO'nun bu dönemde izlediği stratejiler güvenlik stratejisi tasarımı konusunda önemli bilgiler vermektedir. Bu nedenle yalnızca örnek teşkil etmesi maksadıyla NATO'nun stratejilerinin ve icraatlarının incelenmesi, güvenlik stratejisi tasarımcılarının strateji kavramını daha iyi anlayabilmelerini sağlayabilecektir. NATO Soğuk Savaş döneminde 12 ülke tarafından 4 Nisan 1949 tarihinde SSCB'ye karşı kurulmuş bir ittifaktır[27]. İttifaka, Türkiye ve Yunanistan 1952 yılında, Almanya 1955 yılında, İspanya 1982 yılında, Çek Cumhuriyeti, Polonya, Macaristan 1999 yılında, Bulgaristan, Romanya, Estonya, Letonya, Litvanya, Slovakya, Slovenya 2004 yılında, Arnavutluk ve Hırvatistan 2009 yılında, Karadağ 2009 yılında tam üye olmuşlardır. Bunun yanında Akdeniz Diyalogu(7), Körfez işbirliği inisiyatifi(4), Ortak üye (21) gibi İttifakla değişik düzeylerde ilişkisi bulunan ülkeler bulunmaktadır. İttifakın temel prensibi 5. Madde olarak bilinen, bir üyeye yapılan saldırının bütün üyelere yapılmış olarak kabul edilmesidir. Güvenlik stratejisi tasarımının yanında, İttifakın daimi sivil ve askeri karar mekanizmalarını, komuta ve kuvvet yapılarını içeren, karar verilen stratejilerin uygulanmasını sağlayan bir teşkilatlanmasının bulunması ayrıca önem taşımaktadır. Burada dikkat edilmesi gereken konu İttifakın yeni oluşan güvenlik ortamını süratle değerlendirerek sonuçlar çıkarması, çıkarılan sonuçlar çerçevesinde hâkim konumunu devam ettirebilecek yeni bir teşkilatlanmaya ve ilave üyelerin İttifaka dâhil edilmesine karar vermesidir. NATO'nun genişlemesi dikkatli incelendiğinde sistematik bir güvenlik stratejisinin yansıması olduğu görülebilecektir.

NATO'nun tarihin en başarılı savunma örgütlerinden birisi olmasının nedenleri arasında; değişen güvenlik ortamına süratle uyum sağlayabilmesi, yani güvenlik stratejilerini çağa uyarlayabilmesi sayılabilir. İttifak bugüne kadar 7 stratejik konsept, yani güvenlik stratejisi yayımlayarak değişen güvenlik ortamına ayak uydurabilmiş, birlik ve beraberliğini muhafaza edebilmiştir. Başlangıçta Soğuk Savaş döneminde savunma ağırlıklı bir örgüt olan NATO, Soğuk Savaş döneminin sonrasında yakın çevresindeki krizlere müdahale ederek bölgesel, Afganistan'a müdahale ederek

[27]ABD, Belçika, Danimarka, Fransa, Hollanda, İngiltere, İtalya, İzlanda, Kanada, Lüksemburg, Norveç, Portekiz.

küresel bir örgüt olmuştur. İngiltere'de yapılan zirvede (2019) ise Çin konusunda aldığı kararla yeni bir tehdit değerlendirme sürecine girmiştir.

İttifak başlangıçta realist bir güvenlik politikası izlemiş, SSCB'nin saldırgan tutumuna gücünü ve kabiliyetlerini arttırarak cevap vermiştir. Bu şekilde güç dengesini ve dolayısı ile caydırıcılığı başarıyla sağlayabilmiştir. Bu dönemde güvenliğin askeri temelli olarak sağlanması esas alınmış, Marşal Planı gibi ekonomik tedbirler yine askeri temelli güvenliğin sağlanması maksadıyla kullanılmıştır. İttifakın askeri temelli güvenlik anlayışı üye ülkelerin güvenlik stratejilerinin de askeri tabanlı olmasına neden olması sonucunu doğurmuştur.

Avrupa güvenlik mimarisinin diğer önemli bir ayağı Avrupa Güvenlik ve İşbirliği Teşkilatıdır (AGİT). Soğuk Savaş döneminde başlatılan AGİT süreci, 1975 yılından Soğuk Savaş bitimine kadar Doğu-Batı ilişkilerinin önemli bir platformu olmuştur. Doğu Blokunun Berlin Duvarının yıkılması ile dağılmaya başlaması nedeniyle 1989'dan itibaren AGİT farklı bir niteliğe bürünmüştür. Bu çerçevede daha kurumsal bir yapı oluşturularak etkinliği artırılmaya çalışılmıştır.

Bu süreçle birlikte güvenliğin diğer alanlara da yansıması, antlaşmalar yapılarak bir uzlaşıya gidilmesi ve tarafların birbirlerine olan güveninin arttırılması gündeme gelmiştir. Bu çerçevede başta Avrupa Konvansiyonel Kuvvetler Anlaşması (AKKA) olmak üzere bir dizi anlaşma müzakere edilmeye başlanmıştır. Yapılan bu anlaşmalar Avrupa Güvenlik Mimarisinin temelini oluşturmuştur. Yukarıda belirtilen hususlar dikkate alındığında Soğuk Savaş dönemi başında realist bir güvenlik anlayışından neorealist, hatta idealist bir küresel güvenlik anlayışına geçilmeye çalışıldığı ifade edilebilir.

SSCB'nin yenilgisi konusunda birçok neden sayılabilir. Bunlardan en önemlilerinden birisi SSCB'nin Soğuk Savaş döneminde ağırlıklı olarak yalnızca askeri yöntemlerin kullanıldığı bir güvenlik stratejisi benimsemesidir. Özetle mevcut kaynakların askeri güç unsurunun muhafaza edilmesi ve geliştirilmesi üzerine harcanması neticesinde kaynaklar tükenmiş ve yenilgi gerçekleşmiştir. Ayrıca SSCB'nin güvenlik stratejilerini zamanın şartlarına uygun olarak gözden geçirip yenileyememesinin de başarısızlıkta önemli etkisinin olduğu ifade edilebilir.

1.2.4.Soğuk Savaş Sonrası

Diğer taraftan İttifak 1989 yılında Soğuk Savaştan galibiyetle çıkmasıyla tekrar bir uyum (adaptasyon) sürecine girmiştir. Ortak düşmanın, tehdidin ortadan kalkması İttifakın dağılmasını dahi gündeme getirmiştir. Bu süreçte İttifak özellikle Balkanlarda ve Doğu Avrupa'daki krizlerin kontrol edilmesi üzerine strateji oluşturulmuştur. Soğuk Savaş döneminde çatışmaya girmeyen İttifak başta Kosova ve Bosna olmak üzere Balkanlardaki krizlere müdahale etmek zorunda kalmıştır. Bu dönemde 5. Madde, yani top yekûn savunma esas güvenlik anlayışı olarak kalmaya devam ederken, krizlerin problemsiz olarak sonlandırılması üzerine yoğunlaşan bir güvenlik stratejisi benimsenmiştir. Doğu Avrupa ve Balkan ülkelerinin İttifaka kabul edilmesi Rusya'ya karşı caydırıcılığın yanında ülkeler arasındaki çatışma olasılığını azaltarak bölgenin istikrarlı hale gelmesine önemli katkılarda bulunmuştur. Rusya ile etkin bir diyalog başlatılması için gerekli mekanizmaların kurulması bu sürecin başarıya ulaşmasına önemli katkı sağlamıştır.

İttifak AB ile de uyum içerisinde olması gerektiğini kavramış ve bir iş bölümüne gidilmiştir. Bu çerçevede NATO'nun askeri olarak müdahale ettiği krizlerin istikrar safhası için, AB'nin lider olmasını esas alan bir iş bölümüne gidildiği ifade edilebilir. Ancak özellikle Fransa'nın liderliğinde AB'nin otonom harekât icra edebilme kabiliyetini kazanması yönünde yoğun çaba harcanmaya devam edilmektedir. Bu çerçevede AB'nin ABD'den bağımsız bir güvenlik stratejisi tasarlayıp icra edilebilmesi üzerinde çalıştığı ifade edilebilir.

Buna karşın Rusya NATO'nun ve AB'nin Doğu Avrupa'ya doğru genişlemesinde rahatsızlığını daha fazla gündeme getirmeye başlamıştır. Bu çerçevede Rusya güvenlik stratejisini "yakın çevre stratejisi" üzerine oturtmuştur. Bu maksatla Rusya Kolektif Güvenlik Anlaşması Örgütünü (KGAÖ); Kazakistan, Kırgızistan, Tacikistan, Ermenistan ve Özbekistan'ın katılımı ile 2002 yılında kurmuştur. Rusya'nın 2008 yılında Gürcistan'a müdahalesi söz konusu stratejinin uygulanmasının diğer bir örneğidir.

Çin ise ABD'nin ana karasına yaklaşmasını engellemek maksadıyla "Erişim ve Alan Engelleme" (Anti-Access/Area Denial, A2/AD) stratejisini icra etmeye başlamıştır. Ayrıca Tayvan konusunda baskılarını artırmış ve silahlı kuvvetlerinin gücünü arttırmak için tedbirler almıştır.

1.2.5.Terörizm ile Mücadele ve Hibrit Savaş Dönemi

NATO'nun dikkati 11 Eylül 2001 tarihinden sonra terörizme doğru kaymıştır. Bu çerçevede terörizm nedeniyle "önleyici saldırı" stratejisi ön plana çıkmıştır. Bu strateji ile İHA'lar kullanılarak başta Afganistan olmak üzere bazı ülkelerde saldırılar gerçekleştirilmiştir. Bu saldırıların uluslararası hukuka uygun olup olmadığı konusundaki tartışmalar devam etmektedir.

Gündeme gelen diğer önemli bir konsept ise "Responsibility to Protect, R2P" (koruma sorumluluğu) olmuştur. Özellikle iç savaş veya başarısız devletlerde acı çeken halkın korunmasına yönelik herhangi bir otorite bulunmamasından dolayı dışarıdan başka bir aktörün müdahale etmesi ve halkın korunması anlamına gelmektedir. Bu durumda devletlerin egemenlikleri ikinci plana atılmış olmakta ve yine uluslararası hukuk ihlal edilmiş olmasından dolayı tartışmalı bir durum olarak karşımıza çıkmaktadır. NATO'nun Kosova'ya (1999) müdahalesi bu çerçevede değerlendirilebilir.

Diğer taraftan AB'nin "Doğu Avrupa Ortaklığı Stratejisi" çerçevesinde tamamı eski SSCB üyesi ülkeler olan Gürcistan, Ermenistan, Azerbaycan, Moldavya, Ukrayna ve Belarus gibi ülkeleri AB üyeliğine hazırlayacak adımları atmaya başlaması Rusya'yı iyice rahatsız etmeye başlamıştır.

Bunun yanında Genelkurmay Başkanı Valeriy Gerasimov Rus Savaş Bilimleri Akademisi'nde 2013 yılında yaptığı konuşmada Rus Silahlı Kuvvetlerinin karşı karşıya olduğu zorlukları ifade ederek "asimetrik savaş" ifadesini ve Rus güçlerinin Ukrayna'daki operasyonlarının temelini oluşturan "hibrit savaş" terimini ortaya koymuştur. Gerasimov bu stratejiyi; Afgan ve Çeçen Savaşları, ABD'nin Panama'daki operasyonları, NATO'nun Balkanlar ve Afganistan'daki operasyonları, Çöl Fırtınası Harekâtı, Irak'a Özgürlük Operasyonu ve Gürcistan ile savaştan alınan dersler ve Uluslararası Hukuka Uygunluk prensibi değerlendirilerek hazırladığını ifade etmektedir. Söz konusu stratejinin en önemli özelliklerinden birisi askeri ve askeri olmayan güç unsurlarının bir arada kullanılmasını kapsamasıdır.

Rusya'nın uyguladığı stratejinin en önemli özelliği belirsizlik ihtiva etmesidir. Belirsizlik ortamının yaratılmasıyla hedef/rakip ülkelerin zamanında karar vermesi engellenecek ve durum üstünlüğü ele geçirilecektir. Rusya'nın Ukrayna'da uyguladığı

“hibrit harekât” stratejisinin özü de belirsizlik yaratılarak karar vermenin engellenmesi olarak ifade edilebilir. Rusya’nın Kırım çerçevesinde 2014 yılında Ukrayna’ya müdahalesi uluslararası güvenlik açısından önemli sonuçlar meydana getirmiştir. 2022 yılında meydana gelen Rusya-Ukrayna Savaşı ise küresel ve bölgesel açıdan çok daha önemli sonuçlar ortaya çıkarmıştır. Bir sonraki bölümde bu konu incelenmeye çalışılacaktır.

Rusya’nın 2008’de Gürcistan’a müdahalesinden sonra Ukrayna krizinin, tek kutuplu dünyadan çok kutuplu dünyaya geçişin başlangıcını oluşturduğu ifade edilebilir. Buna ilave olarak Rusya’nın Suriye’ye müdahale ederek sıcak denizlere inme hayalini gerçekleştirmesi ve Ortadoğu’ya tekrar döndüğünü göstermesi bu iddiayı teyit eder mahiyette değerlendirilebilir.

Suriye Krizi Arap Ayaklanmalarının bir sonucu olarak ortaya çıkmıştır. Arap Ayaklanmaları başlangıçta diktatörlükle yöneltilen Arap ülkelerinin demokrasiye geçişleri için önemli bir olay olarak değerlendirilmiştir. Ancak Mısır’da Müslüman Kardeşlerin iktidara gelmesi, Libya’da ABD Büyükelçisinin öldürülmesi, DEAŞ terör örgütünün ortaya çıkması hesapları değiştirmiştir. Suriye’nin daveti üzerine Rusya bölgeye gelmiş, yine ABD Suriye’ye asker göndermek durumunda kalmıştır. Ukrayna krizi ile birlikte Suriye’ye müdahalesi Rusya’ya önemli bir durum üstünlüğü sağlamış olarak görülmektedir.

Bu arada Çin 2013 yılında resmi olarak “tek yol tek kuşak” projesini veya stratejisini hayata geçirerek küresel güvenliği etkileyebilecek bir yaklaşım içerisine girmiştir. Bunun yanında Çin jeopolitik açıdan başta güney Çin Denizi olmak üzere konuşlandığı bölgenin kontrolünü tamamen ele geçirmek için önemli hamleler yapmaya devam etmektedir. Çin’in bu hamleleri ile beraber, ekonomik ve teknolojik olarak ortaya koyduğu stratejiler Soğuk Savaşı müteakip güvenlik alanında önemli tartışmaların başlamasına neden olmuştur. Çin’in bu hamleleri çok kutuplu dünyaya geçişin önemli emarelerini vermektedir. Brüksel’deki NATO zirvesinde (2021) Çin’in bir tehdit olabileceği konusundaki yorumlar bu düşünceleri teyit eder mahiyettedir.

Gelinen aşamada 2019’dan itibaren NATO bir kez daha güvenlik stratejisini yeni gelişen küresel güvenlik durumuna adapte edecek çalışmalara başlamıştır. Bu anlamda iki doküman üzerinde ağırlıklı olarak durulmaktadır. Bunlardan birincisi NATO’nun Askeri Stratejisi (NATO Military Strategy, NMS), ikincisi ise NATO Temel Savaş Konsepti (NATO War fighting Capstone Concept, NWCC) olarak karşımıza

çıkmaktadır. Bu dokümanlar ile NATO'nun kriz yönetimi ve terörizmden tekrar klasik savaş stratejisine yöneldiği görülmektedir. Bu dokümanlardan NMS ile Rusya'nın ve terörizmin tehdit olarak algılandığı, bu tehditlere yönelik nasıl mukabele edileceği ortaya konulmaktadır. NWCC ile ise gelecek 20 yıl içerisinde geleceğin muharebe sahası çerçevesinde ihtiyaç duyulacak imkân kabiliyetlerin ve sistemlerinin tedariki esas alınmıştır.

Günümüzde yaşamakta olduğumuz Dijital Çağda güvenlik stratejilerinin tasarımına ilişkin önemli değişikler yaşanmaktadır. Yukarıda örnekler verilerek incelenmeye çalışılan, bir kısmı içerisinde bulunduğumuz zamanı da içeren tarihsel süreçte güvenlik stratejilerinin gelişimi konusu müteakip bölümlerde Dijital Çağ güvenlik ortamının ve bu ortama bağlı olarak güvenlik stratejilerinin tasarlanması konusunda önemli bir alt yapı oluşturacaktır. Sonuçta Dijital Çağ insanlık tarihinin yeni bir dönemidir. Bu dönemin insan yaşamının her alanında olduğu gibi güvenlik stratejilerinin tasarımına da önemli girdilerinin olması doğaldır. Bu etkilerin ve girdilerin tespit edilmesi güvenlik stratejilerinin çağa uygun, mevcut tehditlere cevap verecek şekilde tasarlanmasına yardımcı olabilecektir.

1.3.GÜVENLİK YAKLAŞIMLARININ GÜVENLİK STRATEJİSİ AÇISINDAN İNCELENMESİ

Güvenlik stratejisi tasarımı kavramının daha iyi anlaşılabilmesi maksadıyla güvenlik yaklaşımlarının veya teorilerinin güvenlik stratejisi tasarımı açısından incelenmesi faydalı olacaktır. Sonuçta teorinin icrası strateji ile mümkün olabilmektedir. Müteakip maddelerde güvenlik yaklaşımları çok özet olarak incelenmektedir. Her yaklaşımın sonunda yaklaşımın güvenlik stratejisi tasarımı çerçevesinde kısa bir değerlendirmesi yapılmıştır. Bu değerlendirmeden amaç güvenlik tasarımı konusunda bir fikir vererek müteakip maddelerde incelenecek güvenlik stratejisi tasarım süreci için bir alt yapı oluşturabilmenin yanında yaklaşım (teori) ile strateji tasarımının ilişkilendirilmesine yardımcı olabilmektir. Bu çalışmada yapılan bu değerlendirmelerin güvenlik stratejisi tasarımında faydalanılması ve değişik çalışmalarda kullanılması önerilmektedir.

Güvenlik yaklaşımlarını geleneksel ve yeni (çağdaş) güvenlik yaklaşımları[28] olarak ikiye ayırmak mümkündür.

1.3.1. Geleneksel Güvenlik Yaklaşımı[29]

Bilindiği gibi Vestfalya Sistemi ulus devletin ve geleneksel güvenlik stratejisi tasarımının temeli olarak görülmektedir. Geleneksel güvenlik yaklaşımına göre devletin güvenliğini tehdit eden en önemli tehdit yine devletlerden gelmektedir. Devletlerin sahip oldukları askeri güçler veya kapasiteler tehdit olma özelliklerini belirleyen en önemli husus olarak görülmektedir. Bu çerçevede realist yaklaşımın geleneksel güvenlik yaklaşımlarının temelini oluşturduğunu ifade etmek yanlış olmayacaktır.

1.3.1.1. Realist Güvenlik Yaklaşımı

Realist yaklaşımda uluslararası sistemin anarşik bir yapıya sahip olduğu, bu nedenle sistemin temel aktörü olan devletin ancak güçlü olarak ve gücünü muhafaza ederek bu sistemde güvenliğinin sağlanabileceği kabul edilmektedir. Bu nedenle devlet gücünü arttırmak ve çıkarlarının peşinde koşmak zorundadır. Uluslararası sistemin temel aktörü olan devletin güvenliği her şeyden önemli ve güvenliğin sağlanması için askeri güç en önemli unsurdur. Devletlerin güç ve çıkar peşinde koştuğu, düzen kurucu hâkim bir otoritenin bulunmadığı anarşik sistemde yeteri kadar güçlü olmayan devletlerin güç dengelemesi için ittifaklar kurmaları veya güçlü olan diğer bir devletin koruması altına girmeleri doğal bir sonuç olarak karşımıza çıkmaktadır. İki devlet arasındaki güç dengesinin bozulması güvenlik açısından olumsuz sonuçlar doğurabilecektir. Yine devletlerarasındaki sorunların çözümünde güç temel faktördür. Thucydides, Niccolo Machiavelli, Thomas Hobbes, Edward H.Carr[30], Hans J.Morgenthau[31] gibi yazarlar realizmin önemli düşünürleridir.

[28] Sandıklı, Atilla ve Emeklier, Bilgehan, Güvenlik Yaklaşımlarında Değişim ve Dönüşüm, 2011, s. 4-5.
[29]Haser, Demet, *Uluslararası İlişkilerde Güvenlik Kavramı: Soğuk Savaş Sonrası Dönem Güvenlik*, 2018, s. 12.
[30] Carr, Edward H. *The Twenty Years Crisis*, 1939.
[31] Morgenthau, Hans J., *Politics Among Nations*, 1955.

Realist yaklaşım esas alınarak bir güvenlik stratejisi tasarımı yapılacağı zaman stratejinin mantıksal yapısı, hedeflerin, konseptlerin ve güç unsurlarının ağırlıklı olarak askeri güç çerçevesinde hazırlanmasının esas almasını gerektirecektir. Millî hak ve menfaatlerin gerçekleşmesine en önemli tehdit hedef ülkenin askeri olarak gerçekleştirdiği faaliyetler veya askeri kapasitesi olarak tespit edilecektir. Bu nedenle hedef ülkenin askeri gücünün etkisiz hale getirilmesi veya ittifak haline girilerek bir güç dengesinin oluşturulması gerekmektedir. Soğuk Savaş döneminde başta ABD ve SSCB olmak üzere realist güvenlik yaklaşımı benimsemiş, askeri güç kapasitesi artırılırken ittifaklar kurulmuştur. Buna karşın aktörlerin eğilimlerinin tespit edilmesinde askeri güç kapasitesini artırmaları, ittifak arayışına girmeleri realist bir güvenlik yaklaşımı benimsediğinin önemli ipuçlarını verebilecektir. Bu tespitten sonra hedef ülkenin uygulayacağı hal tarzlarının realist yaklaşım kalıbı çerçevesinde daha kolay tahmin edilmesi strateji tasarımcısının işini kolaylaştırabilecektir.

1.3.1.2.Neorealist Güvenlik Yaklaşımı

Realizmin güvenlik alanındaki gelişmeleri yeterince açıklayamaması karşısında neorealist güvenlik yaklaşımı gündeme gelmiştir. Neorealist yaklaşımın temelinde uluslararası sistemin anarşik yapısının temel nedenlerinden birisinin toplumlarda olduğu gibi güvenliğin sağlanması maksadıyla egemenliğin devredileceği bir yapının veya aktörün olmaması olduğu ifade edilebilir. Bu nedenle de devletler kendi güvenliklerini sağlamak maksadıyla güç artırımına gitmekte, uluslararası sistemin devletler için güvenli bir yapıya kavuşması için bir otorite veya yapı kurulamamaktadır. Dolayısı ile neorealist düşünce uluslararası sistemin yapısının devletlerin güç artırmasına ihtiyaç olmayacak bir hale getirildiği takdirde barışın ve istikrarın da sağlanabileceğini öngörmektedir.

Kenneth N. Waltz'a[32] göre uluslararası sistemin en istikrarlı olduğu dönem Soğuk Savaş ortamındaki çift kutuplu yapıdır. Buna karşın günümüzde şahit olduğumuz çok kutuplu güvenlik sistemi belirsiz bir ortama neden olduğu için daha az güvenlidir. Kutup oluşturan birden fazla aktör uluslararası güvenlik sisteminin anarşik yapısının daha da artmasına neden olmaktadır.

[32] Waltz, N Kenneth, Theory of International Politics, 1979, s.121

Neorealist bir yaklaşımla güvenlik stratejisi tasarlanması durumunda uluslararası sistemin anarşik yapısının kontrol altına alınması, devletlerin karşılıklı güvenlerinin artırılması, bu nedenle bir güvenlik sistemi oluşturulması düşünülebilir. Bu anlamda AGİT iyi bir örnek teşkil etmektedir. AKKA, Viyana Belgesi, Açık Semalar Anlaşması gibi bir dizi anlaşmalar ve AGİT platformunun kurulması Avrupa'da güvenli bir ortam oluşturulmasında önemli katkıları olmuştur. Bu çerçevede güvenlik stratejisi tasarımında diğer ülkelerin askeri güç kapasitelerinin ve niyetlerinin takip edilmesi, antlaşmalardan doğan sorumlulukların yerine getirilmesi gibi hedefler, konseptler ve millî güç unsurlarının esas alınması gerekebilecektir. Yani sadece askeri değil başta diplomasi olmak üzere diğer güç unsurlarının ve bunların gerektirdiği konseptlerin kullanılması gerekebilecektir.

1.3.1.3. İdealist Güvenlik Yaklaşımı

İdealizm 20. yüzyılda uluslararası güvenliğin ve barışın sağlanması maksadıyla ortaya çıkmıştır. İdealizme göre devletlerarası işbirliği ve uluslararası sistemin anarşik yapısını engelleyen bir yapının kurulmasıyla uluslararası düzen sağlanabilecek ve çatışmaların sebepleri ortadan kalkabilecektir. Sonuç olarak savaşa neden olan sebeplerin devletlerin işbirliği ile beraber hareket etmesiyle ortadan kalkacağı üzerine kurulu olan idealizm, liberalizm ile benzer düşünceleri benimsemektedir. Bu kapsamda Birinci Dünya Savaşının hemen sonrasında 10 Ocak 1920 tarihinde Milletler Cemiyeti (MC) kurulmuştur. Ancak bilindiği gibi İkinci Dünya Savaşı'nı engelleyememiştir. Yeni bir devlet olan ABD'nin uluslararası sistemde kendisine yer oluşturmak maksadıyla idealizmi ortaya atmış olduğu tartışmaları devam etmektedir. İdealizmin başarılı olamayışının sebeplerinden birisi sömürgeci devletlerin "manda yönetimi" gibi kendi millî menfaatlerini gerçekleştirmek maksadıyla ortaya attıkları konseptler ile Milletler Cemiyetini kullanma eğilimleri olarak ifade edilebilir.

İdealizm esas alınarak hazırlanan bir güvenlik stratejisi tasarımında ülkelerin çatışmalarını engelleyecek, merkezi otorite veya MC/BM gibi bir teşkilatın kurulması, bu teşkilata işlerlik kazandırılmasına yönelik eylemleri esas alan bir stratejik yaklaşım sergilenmesi gerekmektedir. Ayrıca ülkeler arası işbirliğini geliştirici faaliyet alanlarının yaratılması ve desteklenmesinin hedeflenmesi gerekmektedir. Bunun yanında bütün ülkelerin kabul edebileceği ticaret dâhil küresel bir düzen ve adaletli bir yapılanmaya ihtiyaç olduğu bugün ortaya çıkan sorunlardan anlaşılmaktadır. Ancak

bu yaklaşımda ABD, Rusya ve Çin gibi ülkeler ile bölgesel güç olan veya gelişmekte olan devletlerin güvenlik stratejisi tasarımı farklı olabilecektir. Söz konusu ülkelerin geçmişte olduğu gibi bu ortamı küresel hâkimiyetlerini pekiştirmek maksadıyla kullanma potansiyelleri de bulunmaktadır.

1.3.1.4. Liberal Güvenlik Yaklaşımı

Liberalizm Birinci Dünya Savaşı sonrasında, idealizme benzer bir şekilde çatışmaların engellenmesi maksadıyla daha belirgin olarak ortaya çıkmaya başlamıştır. Liberalizm uluslararası sistemde barışı ve işbirliğini ön plana çıkarmaktadır. Liberallere göre yalnızca askeri anlamda güvenlik değil, sağlık, ekonomi, çevre, göçler gibi konular da güvenlik için önemlidir. İdealizmde olduğu gibi liberalizme göre de demokrasi ile savaşlar önlenebilecektir. Liberalizmde demokratik yönetimlerin ve demokrasi düşüncesinin artmasının uluslararası sistemde barışın sağlanmasını gerçekleştirebileceği düşüncesi hâkimdir. Liberal yaklaşıma göre devletlerarası işbirliği önemlidir. Ağırlıklı olarak devletlerarası ekonomik ilişkiler ve uluslararası çerçevede kurulan örgütler işbirliğini geliştirerek karşılıklı bağımlılığı arttıracaktır. Bu sayede uluslararası sistemin anarşik yapısı azalabilecektir. Böyle bir sistemde bütün aktörler kazanan olabilecektir.

Liberal bir güvenlik stratejisi tasarımında ülkelerin liberalizmi benimsemeleri ve bu çerçevede çatışmadan uzak durmaları hedeflenebilecektir. Bu çerçevede demokratik yapıların teşvik edilmesi, uluslararası kuruluşlar ve küresel ticaret sayesinde ülkelerin birbirlerine bağımlılıklarının artması sayesinde çatışmaların engellenmesine yönelik bir stratejik mantık benimsenebilir. Bu anlamda AB, DTÖ (Dünya Ticaret Örgütü), G-7, G-20, AGİT gibi uluslararası yapıların desteklenmesine yönelik stratejiler önem kazanabilecektir. Ancak idealizmde olduğu gibi bu yaklaşımın özellikle büyük güçler veya geçmişte sömürgecilikten fayda sağlayan devletler tarafından istismara açık olduğu unutulmamalıdır.

1.3.2. Yeni Güvenlik yaklaşımları

Nükleer silahların yıkıcı etkisinin büyüklüğü Soğuk Savaş döneminde tarafları görüşmeye ve bir uzlaşıya ulaşarak barışın sağlanmasına yönlendirmiştir. Bu çerçevede askeri güç unsurunu esas alan geleneksel güvenlik yaklaşımlarının üzerinde

tekrar düşünülmesi gerektiği 1970'li yıllarla birlikte gündeme gelmeye başlamıştır. Soğuk Savaş döneminin sona ermesi ve küreselleşmenin daha da hızlanmasıyla yeni yaklaşımların gündeme gelmesi daha da hızlanmıştır. Ayrıca tehdidin niteliğinin değişmesi ve yeni tehdit türlerinin ortaya çıkması sonucunda yeni güvenlik yaklaşımları üretmek zorunlu olmuştur. Bu yaklaşımların genel olarak realist güvenlik düşünceyi eleştirmeye yönelik olduğu görülmektedir. Müteakip maddelerde bu yaklaşımlardan bazıları özet olarak incelenmiştir.

1.3.2.1 Kopenhag Okulu

Yeni güvenlik yaklaşımlarına en önemli katkılardan birisini Kopenhag Okulunun yaptığı ifade edilebilir. Bilindiği gibi Kopenhag Okulu'nun en önemli isimleri olan Barry Buzan[33], Ole Weaver ve Jaap de Wilde[34] tarafından geliştirilen düşünceler Okulun güvenlik çalışmalarına dört önemli katkısı olmuştur. Bunlar güvenlikleştirme kavramı, sektörel güvenlik analizi, bölgesel güvenlik ve analiz düzeylerinin belirlenmesidir.

Özet olarak güvenlikleştirmenin millî hak ve menfaatlere yönelik bir tehdidin olduğunu ve bir güvenlik sorunu olarak ele alınması gerektiğini ortaya koyan bir süreç olduğu ifade edilebilir. Doğal olarak bunun tam tersi olarak da güvenlik dışılaştırma yani tehdit olma özelliğinin ortadan kalktığını ortaya koyan bir süreç de bulunmaktadır.

Sektörel güvenlik düşüncesiyle askeri anlamdaki güvenlik anlayışı eleştirilmekte, beş farklı güvenlik sektörünü analize dâhil ederek güvenliğin genişletilmesi gerektiği ortaya konulmaktadır. Bu sektörler: Askeri Güvenlik, Politik Güvenlik, Toplumsal Güvenlik, Ekonomik Güvenlik, Çevresel Güvenlik olarak belirtilmektedir. Her bir sektörün güvenlik çerçevesinden tanımlaması da yapılmıştır.

Bölgesel güvenlik olarak ise özetle her bölgenin kendisine has dinamiklerinin, ilişkilerinin, özelliklerinin olduğu, bu çerçevede coğrafi olarak güvenlik sisteminin oluşturulabileceği ifade edilmektedir.[35]

[33]Buzan, Barry, *People, states & fear: an agenda for international security studies in the post-cold war era.* 2008
[34] Buzan, Barry, Weaver, Ole ve Wilde, Jaap de, *Security: A New Framework for Analysis*, 1998.
[35] Buzan, Bary and Waver, Ole, *Regions and Powers the Structure of International Security*, 2003, s.40

En son olarak ise yalnızca devletler düzeyinde değil birey, devlet ve uluslararası sistem olmak üzere üç düzeyde güvenlik analizi yapılması gerektiği ortaya konulmuştur.

Kopenhag Okulu ile güvenlik stratejisi tasarımı askeri sektör yanında diğer sektörlerin de eklenmesi ile daha belirgin olarak çok boyutlu hale gelmiştir. Tasarımcıların artık yalnızca askeri boyutu değil diğer sektörleri de dikkate almaları gerektiği daha açık bir şekilde tanımlanabilmiştir. Sektörel güvenlik düşüncesi ile belirlenecek stratejik hedeflerin ve kullanılabilecek güç unsurlarının tanımı yapılabilmiştir. Konsept bağlamında ise stratejik hedeflere ulaşmak maksadıyla yalnızca askeri güç unsuru değil diğer güç unsurlarının uygun bir şekilde kullanılmasının dikkate alınması gerektiği düşüncesi ortaya çıkmaya başlamıştır. Güvenlikleştirme ile ise millî menfaatlere yönelik tehdidin ortaya konulması ve başta halk olmak üzere bütün paydaşlar tarafında kabul edilmesinin sağlanması süreci tanımlanmıştır. Analiz düzeyi yaklaşımı ile güvenliğin daha gerçekçi bir şekilde sağlanabilmesi maksadıyla, yalnızca devlet değil millî güvenlik stratejilerinde bireylerin güvenlikleri, özgürlüklerinin de dikkate alınması, uluslararası güvenlik sisteminin dinamiklerinin hesaba katılması gerektiği ortaya konulmuştur.

1.3.2.2. Eleştirel Yaklaşım

Eleştirel yaklaşım özet olarak insanların eleştiri yoluyla özgürleşmesini savunmaktadır. Eleştiri sayesinde daha iyi bir toplum veya yapı oluşturulabileceği bunun da insanların özgürleşmesine hizmet edebileceği savunulmaktadır. Bu çerçevede bireylerin özgürlüğünün kısıtlamasının bir güvenlik sorunu olduğu, özgürleşen bireyin güvenliğinin sağlanmış olduğu ortaya atılmaktadır. Bu çerçevede devletlerin yalnızca dış güvenliğe değil aynı zamanda bireylerin güvenliğine, dolayısı ile iç güvenliğe de önem vermesi gerektiği belirtilmektedir. Realizmin devlet temelli güvenlik anlayışı ile bireyin güvenliği ikinci planda kalmıştır. Bireylerin yaşadığı güvenlik sorununun kaynağı olarak kendi iradeleri dışında maruz kaldıkları ekonomik, kültürel, toplumsal baskılar gibi konular görülmektedir.

Robert W.Cox eleştirel yaklaşıma en büyük katkı yapan düşünürler arasındadır. Cox 1981 yılında yayımladığı "Sosyal Kuvvetler, Devletler ve Dünya Düzenleri: Uluslararası İlişkiler Yaklaşımının Ötesinde" isimli makalesinde yaklaşımları; problem çözücü ve eleştirel olarak ikiye ayırmıştır. Makalede özet olarak; problem

çözücü yaklaşımların mevcut sistemdeki problemlerin çözümünü, dolayısı ile mevcut sistemin devamını esas aldığı, bu nedenle mevcut sistemin değişemeyeceği belirtilmekte; ancak eleştirel yaklaşım sayesinde alternatif bir düzenin kurulmasına rehberlik edebileceği belirtilmektedir. Ayrıca herhangi bir sistem üzerinde çalışılırken fikirlerin, somut kabiliyetlerin ve kurumların; sosyal kuvvetler, devlet şekilleri ve dünya düzenlerinin ise uluslararası ilişkiler çerçevesinde değişiklik yaratılabilmesi için dikkate alınması gerektiği vurgulanmaktadır.[36]

Bu yaklaşımı esas alan bir strateji tasarımcısı bireyin özgürlüğünü esas alan bir toplumsal yapı ortaya koymayı, bu yapıya olabilecek tehditlerin etkisiz hale getirilmesini esas almayı düşünmesi gerekmektedir. Eleştirel yaklaşım esas alındığında devlet güvenliği nihai hedef değil bireyin özgürleşmesi için kullanılabilecek araçlardan birisidir. Meseleye iç güvenliği esas alan bir güvenlik tasarımı perspektifinden bakıldığında bireyin özgürlük-güvenlik dengesinin kurulduğu, teröristlerin bireyin güvenliğine bir tehdit oluşturmadığı bir kamu düzeninin kurulması önemli bir hedef olabilecektir. Bu hedef ile uyumlu olarak kolluk kuvvetlerinin kullanımı ve başta ekonomi olmak üzere diğer millî güç unsurları ile kolluk kuvvetlerinin faaliyetlerinin desteklenmesi göz önüne alınabilir.

Diğer taraftan Cox'un yaklaşımının güvenlik stratejisi tasarımında üzerinde çalışılan sistemin daha kapsamlı olarak incelenmesinde, istenilen sonuçların ortaya çıkarılabilmesinde faydalı olabileceği kıymetlendirilmektedir.

1.3.2.3.İnşacı Yaklaşım

İnşacılar realist yaklaşımın savunduğu çatışmaya dayalı ulusal güvenlik ve millî menfaat etrafında biçimlenen güvenlik anlayışını kabul etmezler. İnşacı yaklaşıma göre devletlerin millî menfaatleri sosyal yapılar tarafından oluşturulmaktadır. Dolayısıyla inşacı fikirler, normlar, kültürler, kimlikler gibi unsurlardan oluşan sosyal yapıyla güvenliği ilişkilendirmeye çalışmaktadır. Devletlerin güvenlik çerçevesinde davranışlarını sosyal yapılarının belirlediğini savunmaktadır. Bu çerçevede bir devletin diğer bir devleti tehdit olarak tanımlamasındaki en önemli etken söz konusu devletin sosyal yapısı veya kendini ve dolayısı ile ötekiyi nasıl tanımladığıdır. Daha kapsamlı olarak bakıldığında kimliklerin oluşturduğu sosyal yapıları çerçevesinde

[36]Cox, Robert W., *Social Forces, States and World Orders: Beyond International Relations Theory*, 1981.

devletlerarasındaki güven ilişkisi diğer devletlerin tehdit, yani öteki olarak algılanmasında önemli bir unsur olarak karşımıza çıkmaktadır. Bu yaklaşımda devletlerin sosyal yapıları, kimlikleri esas alınarak öteki veya tehdit inşa edilmektedir. En önemli yazarlardan bazıları Nicholas Onuf[37], Alexander Wendt[38] olarak sıralanabilir.

İnşacı yaklaşımı esas alan bir güvenlik tasarımında millî menfaatlerin belirlenmesi kimlik veya sosyal yapı esas alınarak yapılabilecek, bu çerçevede millî menfaatlere yönelik tehditlerin de belirlenmesi aynı yöntemle olabilecektir. Bu mantık yapısında millî menfaatlere tehdit olabilecek devletler güçleri ile değil sosyal yapıları veya kimlikleri ile değerlendirilebilecek, eğer öteki olarak belirlenmiş bir devlet ise tehdit olarak nitelendirilebilecektir. Örnek olarak dini yaklaşımların esas alındığı bir durum verilebilir. Bu durumda başka bir dine mensup olan bir devlet dini nedenlerden dolayı öteki ve sonuç olarak tehdit olarak nitelendirilebilecektir.

1.3.2.4. Postmodernist Yaklaşım

Postmodernizm genel olarak eleştirel yaklaşıma benzer bir yaklaşım sergilemektedir. Modern devletin, yani ulus devletin gerekli olmadığını, yaratılmış bir gerçeklik olduğunu savunmaktadır. Postmodernist yaklaşıma göre ulus devletin yükseltildiği konum sorgulanmalıdır.

Diğer taraftan bu yaklaşım uluslararası güvenlik sisteminde sadece devletin değil, bireylerin, kültürel ve dini grupların da güvenliğinin dikkate alınması gerektiğine vurgu yapmaktadırlar. Ayrıca devletlerin güvenliğe yönelik endişe yarattığı savunulmaktadır. Bu çerçevede devletlerin halklarının, egemenliklerinin ve sınırlarının güvenliğini sağlamak maksadıyla güvenlikleştirmeye başvurdukları, bazen de olmayan tehdit ve tehlike algısı yarattıkları düşünülmektedir. Bu yaklaşımın en önemli yazarlarından bazıları Friedrich Nietzsche[39], Martin Heidegger[40] olarak belirtilebilir.

Postmodernist bir yaklaşımı esas alan bir güvenlik stratejisi hazırlanması kolay değildir. Bunun temel nedenlerinden birisi postmodernistlerin bir model ortaya koymakta yeterli olmaması, yalnızca ağırlıklı olarak ulus devletin eleştirilmesinin esas

[37]Onuf , Nicholas Word of Our Making: Rules and Rules in Social Theory and International Relations, Columnia University of South Caroline Press, 1989
[38] Wendt, Alexander Social Theory of International Politics,Cambridge University, 2003
[39] Nietzsche, Friedrich, *Thus Spoke Zarathustra (1883-1885)*
[40] Heidegger, Martin, *Being and Time*, 2010.

alınması olarak gösterilebilir. Tehdit olarak yalnızca modern devlet yapısının alınması sağlıklı sonuçlar vermeyebilecektir. Ancak yapılacak stratejik durum tespiti veya analizlerde kısmen de olsa postmodern yaklaşımdan faydalanılması düşünülebilir.

1.3.2.5. Feminist Yaklaşım

Feminist yaklaşımın temelini Postmodern ve Eleştirel yaklaşımlar gibi genel olarak modernitenin ve realizmin güvenlik kavramının eleştirisi oluşturmaktadır. Bununla beraber feminist yaklaşımlarını düşüncelerini cinsiyet üzerinden şekillendirmektedir. Feminist yaklaşım modernite ve realizmin oluşturduğu olguların erkek egemen bir düşünce ile yaratıldığını savunmaktadır. Buna karşın feminist bir yaklaşım sergilenerek erkek egemen güvenlik sisteminin ortaya çıkarttığı şiddet ortamı, ayrımcılık gibi sorunların engellenmesini gündeme getirilmektedir. Feminist güvenlik yaklaşımının en önemli yazarlarından birisi J.Ann Tickner[41] olarak ifade edilebilir.

Feminist yaklaşım esas alınarak hazırlanacak bir güvenlik stratejisinde şiddetin ikinci planda olması gerektiği yukarıdaki açıklamalardan ortaya çıkmaktadır. Bu yaklaşım gerek hedeflerin seçimini, gerek konsepti ve millî güç unsurlarının seçimini direkt olarak etkileyebilecektir.

1.3.3. Güvenlik Stratejisi Tasarımının Analiz Düzeyleri

Strateji daha önce belirtildiği gibi yalnızca askeri olarak değil birçok alanda kullanılmaktadır. Örneğin iş hayatında stratejinin tasarımı ve kullanımı askeri alandakine oldukça benzerdir. Liddell Hart stratejiyi "askeri araçların politik nihai hedeflere ulaşılması için tahsis edilmesi (dağıtılması) ve kullanılması sanatı" olarak tanımlamaktadır[42]. Bu cümleden "askeri" kelimesinin çıkarılması ile tanımın iş hayatında da kullanılabileceği görülmektedir. Güvenlik stratejisi tasarımı diğer alanlarda üretilen stratejiler ile önemli benzerlikler gösterse de kimin güvenliğinin sağlanacağı, bu çerçevede tehdidin ne olduğu, tehdidin bertaraf edilmesi için hangi hedeflere ulaşılmasının gerektiği, kullanılacak kaynak ve araçların neler olabileceği gibi kendine özgün kararları içermektedir. Bu çerçevede güvenlik yaklaşımları dikkate

[41] Tickner, J.Ann Introducing Feminist Perspectives into Peace and Word Security Courses, 1995 ve Feminist Responses to International Security Studies, 2004

[42] Hart, Liddell, The classic book on military strategy; *Strategy* 2. Baskı, Mart 1991, s. 321.

alınarak üç düzeyde analiz yapılabilir. Bunlar uluslararası sistem, ulus-devlet ve bireysel düzeylerdir[43].

1.3.3.1. Uluslararası Sistem Düzeyi

Uluslararası sistemin özellikleri ulus-devletlerin ve hatta diğer aktörlerin davranışlarını doğrudan etkilemektedir. Sistemin kendisi aktörleri belirli şekillerde davranmaları için yönlendirmektedir. Realizm kapsamında ortaya çıkan "güç dengesi" buna iyi bir örnek teşkil etmektedir. Bu çerçevede soğuk savaş döneminde SSCB'ye karşı güç dengesinin oluşması maksadıyla NATO kurulmuştur. Uluslararası sistemdeki kuvvet dağılımı ve aktörlerin davranışları bu analiz düzeyinde yapılan incelemeler ile ortaya çıkmaktadır.

Realizmde açıklandığı gibi sistem anarşiktir. Aktörler rekabet halindedir ve farklılıklarını güç kullanarak çözme eğilimindedir. Aktörler kendi kendilerine yeterli olmak durumundadır. Dolayısı ile aktörler diğer aktörlere göre güçlerini geliştirmek durumundadırlar. Ulus-devlet yapısındaki bireylerin haklarını koruyan, adaleti sağlayan hükümet benzeri bir sistem olmadığı için aktörler kendi başlarının çarelerine bakmak durumunda kalmaktadırlar. Almanya'nın İkinci Dünya Savaşı öncesi davranışları ve buna karşın diğer devletlerin tepkileri güvenlik yaklaşımları kullanılarak sistem düzeyinde anlamlandırılabilecek gelişmeler olarak görülebilir. Günümüzde Çin'in davranışlarının Almanya'nın geçmiş süreçteki, uluslararası sistem düzeyindeki davranışları esas alınılarak inceleme yapıldığı çalışmalara rastlanmaktadır.

1.3.3.2. Ulus-devlet Düzeyi

Günümüzde bu seviye aktör düzeyi değerlendirme olarak adlandırılmaktadır. Bu düzeyde özellikle ulus-devletlerin ülke içindeki durumları dikkate alınarak davranış kalıpları değerlendirilmeye çalışılmaktadır. Bu çerçevede ulus-devletlerin verdikleri kararlar uluslararası sistemde barış, savaş veya işbirliğinin ortaya çıkmasına neden olmaktadır. Devletlerin politik sistemleri, kültürleri güvenliğe yönelik karar vermelerinde etkin olmaktadır. Demokratik devletlerin otoriter devletlere göre daha

[43]Nye, S. Joseph ve Welch D., *Küresel Çatışmayı ve İşbirliğini Anlamak*, 2017, s. 75.

barışçıl davranış sergiledikleri bilinmektedir. Demokratik sistemlerin daha barışçıl olduklarından hareketle, demokratik devletlerin sayısının artırılması barış ve uluslararası sistemin korunması için olumlu olacağı sonucuna varılabilir. İkinci Dünya Savaşı'nda "güç dengesinin" oluşmuş olması savaşı engelleyememiş; Almanya, Japonya, İtalya gibi otoriter rejimler karakterleri gereği savaşı başlatmışlardır.

1.3.3.3. Birey Düzeyi

Bu seviyede liderlerin rolünün analiz edilmesi önemlidir. Liderlerin savaş ve barışa karar vermeleri dikkate alınabilir. Liderlerin davranışlarının devletlerin davranışlarını etkileyen önemli bir faktör olduğu bilinmektedir. Devletlerin davranışlarının anlamlandırılmasında; ülkedeki en önemli karar vericilerin kimler olduğu, bu liderlerin motivasyonları ve algılamaları, neyi başarmaya çalıştıklarının tespiti önemli parametreler olarak karşımıza çıkmaktadır. Bunun yanında karar verme mekanizmaları da göz önüne alınmalıdır.

Ayrıca eleştirel yaklaşımın esas aldığı bireyin özürleşmesinin güvenliğin temeli olduğu düşüncesi bu analiz düzeyinde dikkate alınması gereken önemli bir konudur. Bu çerçevede güvenlik stratejisi tasarımında özgürlük-güvenlik dengesinin iyi bir şekilde ayarlanması birçok açıdan tasarımın başarıya ulaşmasını sağlarken bireylerin ülkelerine bağlılığını da artıracağı değerlendirilmektedir.

Bu analiz düzeyleri dikkate alınarak güvenlik konusunda değişik yaklaşımlar ve modeller üretilmiştir. Stratejik tasarımda bu yaklaşımların dikkate alınması önemlidir. Ancak esas olan gerçek durumun analiz edilmesidir. Yaklaşımlar ve analiz düzeyleri kullanılarak uluslararası siyasi sistem açıklanmaya çalışılabilir. Analiz yapılırken her üç düzeyin de analiz edilerek stratejik bir değerlendirme ve teklifler yapılabilir. Önemli olan devletlerin değişik durumlarda sergileyebileceği davranışların sebeplerinin ortaya konulması ve millî menfaatlere zarar verecek davranışların engellenmesi veya millî menfaatlerle uyumlu olanların teşvik edilmesinin sağlanmasıdır.

1.4. GÜVENLİK STRATEJİSİ TASARIMININ İNCELENMESİ

İlgili aktör tarafından yapılan güvenlik tanımlaması çerçevesinde hedeflenen güvenlik durumuna ulaşmak ve bu durumu muhafaza edebilmek maksadıyla bir güvenlik stratejisi geliştirilmesi gerekmektedir. Bu çerçevede Avrupa'da bir devlet ile Ortadoğu veya Asya'daki bir devletin güvenlik tanımlaması aynı olmayabilecektir. Polonya gibi ülkeler doğudan gelen tehdidin engellenmesini güvenlik tanımlaması kapsamına alırken, Çin yeraltı kaynaklarına ulaşımını esas alan bir güvenlik tanımlaması yapabilecektir. Diğer taraftan güvenlik stratejisi geliştirilmesi diğer alanlardaki stratejiler ile benzerlik göstermesine rağmen önemli farklılıklar arz etmektedir. Bu çerçevede güvenlik stratejileri genellikle tehdidin ortadan kaldırılmasına odaklanırken, iş hayatında stratejiler genellikle piyasada üstünlük kurmak, para kazanmak, iş geliştirmek gibi hedeflere yönelebilmektedir.

Güvenlik stratejisi geliştirmek yerine dijital çağda tasarlamak kelimesinin kullanılması çok daha isabetli bir sonuç verebilmektedir. Strateji geliştirmek hem bir sanat hem de bir bilim olarak kabul edilmekle birlikte, dijital çağda gelişen teknolojik kabiliyetler çerçevesinde bilim yanının güçlenmeye başladığı ifade edilebilir. Bu nedenle bir mühendisin bir arabayı, silahı tasarlaması gibi mümkün olduğu kadar bilimsel yöntemler kullanarak, uygun bir güvenlik stratejisi tasarlanmasının dikkate alınması gerekmektedir. Bu nedenle strateji geliştirilmesi yerine tasarlanması çok daha uygun bir kavram olabilecektir. Tasarım kavramı ile beraber tabii ki güvenlik stratejisi geliştirme sürecinin de mühendislerin tasarım yöntemlerinin bazı özelliklerini yansıtacak şekilde değiştirilmesi gerekmektedir. Tasarım konusu daha detaylı incelenecektir.

Güvenlik stratejisi tanımı yapılması gerekirse; menfaatlere ulaşılması veya tehditlerin bertaraf edilebilmesi için stratejik tasarımcı tarafından tanımlanması gereken hedefler, millî güç unsurları veya kaynaklar ve bunların kullanım konsepti olarak ifade edilebilir. Bu cümledeki tasarımcı tarafından tanımlanması gereken konusu stratejinin sanatsal özelliğini yansıtan unsurdur. Stratejist genellikle boş bir kâğıt parçasıyla tasarıma başlar ve tasarım sürecinde aşağıda bazıları ifade edilmiş olan birçok soruya cevap vermek durumunda kalır. Bu çalışmada cevap verilmesi gereken bazı sorular aşağıda önerilmektedir.

- Hükümet veya politik irade tarafından ortaya konulan hedefler nelerdir?
- Politik direktif olmaması durumunda stratejik hedefler nasıl belirlenebilecektir?
- Mevcut stratejik durumda önemli stratejik faktörler nelerdir?
- Stratejik durum gelecekte nasıl şekillenecektir? Hangi senaryolar önem kazanmaktadır?
- Stratejik problem tanımı nasıldır?
- Hangi faraziyeler makul ve mantıklı olarak kabul edilebilir?
- Millî menfaatler nelerdir? Hangi menfaat hangi öncelik ve öneme sahiptir?
- Millî menfaatleri tehdit eden aktörler nelerdir? Tehdit gerçek midir?
- Tehdidin bertaraf edilmesi için hangi hedefin seçilmesi gerekir?
- Millî güç unsurları bu tehdidi bertaraf etme imkân ve kabiliyetine sahip midir?
- Millî güç unsurlarından geliştirilmesi gereken var mıdır?
- Millî güç unsurlarından hangileri, ne zaman, hangi hedefe tahsis edilebilir?
- Tasarlanan stratejinin riskleri nelerdir? Öncelikleri nasıldır? Nasıl yönetilebilir?

Görüldüğü gibi tasarımın başlangıcında bilinmeyen oldukça fazla husus bulunmaktadır. Stratejist, sürekli değişen, belirsiz, karmaşık ve muğlâk bir ortamda, kendi belirlediği nihai hedefe uygun olarak stratejik ortamı şekillendirmek için bir düşünme sistematiği ortaya koymak zorundadır. Politik direktifin bulunmadığı durumlar ile oldukça sık karşılaşılmaktadır. Bu durumda güvenlik stratejisi tasarımında millî menfaatlerden yola çıkarak bir mantık çerçevesinde stratejik hedeflerin belirlenmesi ve politik seviye ile diğer paydaşlar tarafından tasdik edilmesi en uygun yol olabilecektir. Dar anlamda bir plan olarak nitelendirilen strateji, bu düşünme sistematiği ile daha geniş anlamda bir hipoteze[44]benzetilebilir. Tasarlanan strateji hipotezin icraya dökülebilmesi için yapılacak planlamaya ışık tutmalı, bir çatı görevi görmelidir. Bu nedenle hem bilimsel hem de sanatsal yönünün olduğu ifade edilebilir. Strateji tasarlanırken menfaatlerin veya tehditlerin ortaya konulması birçok parametreye ve hatta liderin özelliğine göre değişir. Bazı liderlerin Kopenhag Okulunda belirtildiği gibi tehdit olarak belirledikleri veya güvenlikleştirdikleri olgular başka bir lider tarafından farklı yorumlanabilir. Bu nedenle stratejinin bir hipotez olarak algılanması tasarımda kolaylık sağlayabilecektir.

[44]Hipotez bir probleme karşı çözüm yollarını doğru ya da yanlış bir şekilde ortaya koyan varsayımlar olarak tanımlanabilmektedir.

Strateji gerçek anlamda politika ile icra, yani operatif seviye veya taktik seviye arasında bir köprü olarak kabul edilebilir. Bu nedenle tasarımcı hem politik seviye, hem de operasyonel veya icraya yönelik bilgiye sahip olmalıdır. Bu şekilde nihai hedefe (ends) ulaşmak maksadıyla eldeki güç unsurlarının (means) gerçekçi bir şekilde kullanılması sağlanabilir. Strateji tasarımı bu sayede operasyonların veya faaliyetlerin belirlenen hedeflere yönlendirilmesi için bir direktif, bir yol haritası şeklini almaktadır.

Belirli bir hedef ve bu hedeflere ulaşmak için ortaya konulmuş bir stratejik tasarım olmadığı takdirde söz konusu organizasyonda bir kaos ortamı, fırsatların değerlendirilememesi, farklı birimlerin veya yapıların birbirlerinin faaliyetlerini olumsuz etkilemesi, gayretlerin boşa gitmesi gibi sorunlarla karşılaşılabilecektir. Aslında yazılı olmasa da her organizasyonun bir stratejisinin var olduğu kabul edilebilir. Ancak bu strateji genellikle organizasyonun tamamını değil bireyleri, alt birimleri parça parça kapsayan genel istikametin belirlenmesine ve gayretlerin bir hedefe yönlenmesini sağlayamayan bir stratejidir. Organizasyonların genel istikametleri belirleyememeleri veya açık olarak ortaya koyamamaları personelin moralini ve dolayısı ile performansını olumsuz etkileyebilecektir. Bu aynı zamanda liderlerin otoritelerinin olumsuz etkilenmesine neden olabilecektir.

Diğer taraftan strateji tasarımı gelecekte ulaşılması hedeflenen durum ile mevcut durum arasında bir köprü olarak da görülebilir. Gelecekte ulaşılması hedeflenen durum vizyon, hayal veya millî menfaatler ışığında oluşturulan nihai durum olarak algılanabilir. Mevcut durumdan gelecekte ulaşmayı hedeflediğimiz duruma ulaşmak için kullanacağımız yöntem strateji olarak ifade edilebilir. Bu kapsamda hem mevcut durumun doğru olarak tespit edilmesi hem de gelecekte ulaşılması hedeflenen durumun belirlenmesi bilimsel yöntemlerin yanında sağduyu ve stratejinin sanatsal yönünü oluşturmaktadır.

1.5.KLASİK STRATEJİ TASARIMI

1.5.1.Stratejik Düşünme

Stratejik düşünmenin ve buna bağlı olarak stratejik tasarımın birçok tanımı ve algılaması bulunmakla birlikte genel olarak literatürde üç ana eleman üzerine oturmaktadır. Arthur F. Lykke Jr tarafından 1989 yılında ortaya konulan, denklem olarak da ifade edilen yaklaşım, klasik güvenlik strateji tasarımının temeli olarak kabul edilebilir. Strateji = Hedef + Konsept + Kaynak. Kaynaklar burada millî güç unsurları olarak da ifade edilebilir.[45]

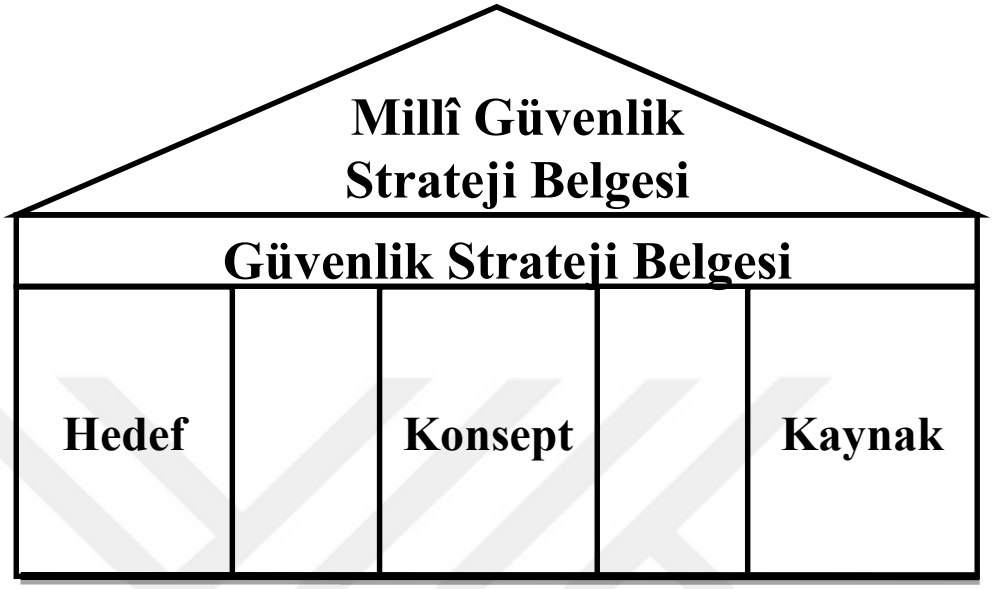
Bu yaklaşım esas alınarak Şekil 1.1'de ana hatlarıyla klasik anlamda bir güvenlik stratejisi yaklaşımı gösterilmektedir. Müteakiben açıklanacağı gibi Millî Güvenlik Strateji Belgesi bir çatı dokümandır. Bu çatı doküman esas alınarak herhangi bir güvenlik strateji belgesi hazırlanabilir. Klasik anlamda güvenlik strateji belgesi üçayak üzerine oturmaktadır.

Bu genel yaklaşım klasik strateji yaklaşımı olarak herhangi bir stratejinin tasarımda bir başlangıç noktası olarak kullanılabilir. Stratejinin tasarım amacı ve özelliklerine göre ilave başlıklar eklenebilir. Bu stratejik düşünme sistemi başta iş hayatı, spor olmak üzere birçok alanda kullanılmaktadır. Eğer amaç bir askeri strateji tasarlamak ise bu denklemde hedefler askeri hedefler olabilecek, askeri kuvveti kullanma yöntemi, yani konsept olacak, kaynaklar (güç unsurları) ise insan kaynağı, silah, teçhizat, lojistik, askeri kuvvet gibi görevin başarılması için kullanılacak askeri ağırlıklı kaynaklar olabilecektir. Aslında bu yaklaşım stratejik, operatif ve taktik seviyeler için de uygulanabilir. Ancak her bir seviye için başta faraziyeler, zamanlama, kullanılan kuvvetlerin seviyesi, harekât alanının genişliği gibi farklılıklara tasarımda dikkat edilmesi gerekmektedir.

Yukarıdaki klasik strateji yaklaşımı esas alınarak stratejinin tasarlanması ve uygulanması stratejik olarak düşünmeyi gerektirmektedir. Stratejik düşünme genel olarak bir sistematik üzerine oturtulabilir. Stratejik düşünme sistemi müteakip bölümde açıklanmaya çalışılmıştır.

[45] Lykke, Arthur F. Jr., Defining Military Strategy, *Military Review*, C. 69, S. 5, 1989.

Şekil 1.1: Klasik Güvenlik Stratejisi Yaklaşımı



1.5.2.Stratejik Düşünme Sistemi

Klasik anlamda etkin bir strateji tasarlanabilmesi birçok sorunun sorulmasını, analizlerin yapılmasını ve karar vericiler tarafından zamanında kararların verilmesini gerektiren karmaşık bir işlemi gerektirmektedir. Bu işlemlerin sağlıklı olarak yapılabilmesi, özün kaybedilmemesi, amaca istenildiği şekilde ulaşılabilmesi maksadıyla stratejik düşünmenin bir sistematiğe veya mantığa oturtulması gerekmektedir. Stratejistlerin kritik ve analitik düşünme sistemini bilmesi ve kullanması bu mantığın oluşturulmasını kolaylaştırırken tasarımın etkinliğini de artırabilecektir.

Başarılı bir stratejik tasarımın stratejik bir mantık üzerine oturtulması gerekmektedir. Stratejik mantık; karmaşık, doğrusal olmayan, çok boyutlu, genellikle kişilere göre farklılıklar arz eden tartışmalı bir konudur. Değişik stratejik mantık yaklaşımları bulunmaktadır. ABD Millî Savunma Üniversitesi tarafından ortaya konulan stratejik mantık yaklaşımının genel olarak klasik güvenlik tasarımında esas alındığı ifade edilebilir. Söz konusu yaklaşım özet olarak: stratejik durum analizi,

hedefin belirlenmesi, kaynakların belirlenmesi, konseptin formüle edilmesi, risk/maliyetin değerlendirilmesi şeklinde ifade edilmektedir[46]. Bununla beraber Güvenlik stratejisi tasarımında elde edilen deneyimler konuya daha geniş bir bakış açısıyla bakılmasını gerektirebilmektedir. Bu anlamda politik alandaki gelişmeler, stratejinin oluşturulma amacı, millî hak ve menfaatler, stratejinin başarısının değerlendirilmesi gibi konuların dikkate alınmasının gerektiği değerlendirilmektedir.

Bu çerçevede söz konusu sistem incelenmiş ve aşağıdaki gibi daha anlaşılır ve kullanışlı bir hale getirilmeye çalışılmıştır. Ayrıca güvenlik stratejisi çalışmalarda kullanılması önerilmektedir. Bu sistem**;**

- Politik direktifin incelenmesini,
- Amaca göre stratejik çerçevenin incelenmesini,
- Problemin tanımlanmasını,
- Millî menfaatlerin veya hakların belirlenmesini (gözden geçirilmesini),
- Millî menfaatlere veya haklara tehdit oluşturan hedeflerin/aktörlerin veya bunların gerçekleştirilmesi için beliren fırsatların ortaya konulmasını,
- Tehdidin etkisiz hale getirilmesi veya fırsatın değerlendirilebilmesi için ulaşılması gereken nihai hedefin ve stratejik alt hedeflerin tespit edilmesini,
- Bu maksatla kullanılacak (millî) güç unsurlarının/kaynakların/araçların belirlenmesini,
- Millî güç unsurlarından/kaynaklardan/araçlardan geliştirilmesi gerekenlerin gözden geçirilmesini,
- Belirlenen hedeflere ulaşılmakta kullanılacak konseptin oluşturulmasını,
- Risklerin hesaplanmasını,
- Stratejinin değerlendirilebilmesi için yöntemin belirlenmesini içerebilir.

Yukarıda belirtilen elemanlardan da faydalanılarak çeşitli mantık modelleri oluşturulabilir. Bu anlamda özet olarak diğer bir stratejik mantık yapısı ise mevcut durumun belirlenmesini, ulaşılmak istenen nihai durumun belirlenmesini, mevcut durumun istenen nihai duruma dönüştürülebilmesi maksadıyla izlenecek konseptin belirlenmesini içerebilir. Yine aynı mantık çerçevesinde mevcut durumdan istenen duruma ulaşmada karşılaşılması muhtemel veya karşılaşılan problemlerin belirlenmesi, bu problemlerin çözümlerinin ortaya konulması karşımıza diğer bir

[46]Heffington, Steven; Oler, Adam; Tretler, David, *A National Security Strategy Primer*, 2019.

stratejik mantık örneği olarak çıkmaktadır. Başka bir stratejik mantık ise herhangi bir coğrafyada veya fonksiyon alanında takip edilen stratejinin sadece bozulmasını esas alan bir mantık anlayışı olabilir. Bu stratejik yaklaşımı genel olarak Rusya Federasyonu'nun yaklaşımlarında görmek mümkündür. Buna örnek olarak Rusya'nın Suriye veya Libya'daki yaklaşımları verilebilir. Rusya'nın bu bölgelere sonradan müdahil olarak diğer aktörlerin stratejik tasarımlarını bozduğu ifade edilebilir. Stratejik felç mantığı ile formüle edilen bir stratejide ise ağırlıklı olarak rakipten çok daha hızlı stratejik kararlar vererek rakibin karar mekanizmasının hızlı olan tarafın karar mekanizmasına tabi kalmasını sağlayarak durum üstünlüğünün sağlamasını esas alan bir mantık izlenebilir. Bu örneklerden başka stratejik mantık çeşitleri de bulunmaktadır. Hangi stratejik mantığın kullanılacağı stratejik tasarımın sanat yönünü oluşturan özelliklerden birisidir.

Tasarımda kullanılan stratejik mantık sisteminin bütün elemanlarının birbirleriyle ilişkisinin dikkate alınması ve sistem bütünlüğü içerisinde incelenmesi uygun olacaktır. Stratejist her aşamada önemli tespitler, kabuller yapmak, gerekirse faraziyeler üretmek, bunları yaparken de sistemin diğer elemanlarıyla uyum içerisinde olmasına dikkat etmek zorundadır. Örneğin millî menfaatler ve millî menfaatlere muhtemel tehditler veya fırsatlar uygun belirlenmeli, seçilen nihai hedef millî güç unsurlarının imkân kabiliyetleri dâhilinde olmalı, oluşan risk iyi tespit edilip yönetilmesi için tedbirler düşünülmelidir.

Strateji tasarımı bir plan değildir. Planlar da genellikle strateji hazırlanması prensiplerinde; nihai hedef+konsept+güç unsurları esas alınarak hazırlanır. Ancak stratejist tasarımı yaparken birçok bilinmeyeni bilinir hale getirerek planlamanın yapılacağı zemini oluşturur. Stratejilerin belirlediği zemin çerçevesi esas alınarak planlar daha deterministik ve lineer (gelecekte beklenen gelişmeler olabilen, doğrusal, rastgelelik bulunmayan) bir yapı oluşturabilir. Stratejinin üç temel faktörü; kuvvet, zaman ve mekândır. Stratejist planlamalar için politik direktif çerçevesinde bunlara karar vermek zorundadır. Örnek olarak; hangi aktöre karşı nerede mücadele edilecektir? Ne zaman mücadele başlayacaktır? Hangi güç unsurları kullanılacaktır? Bu ve benzeri sorulara cevap verilmeden daha alt planlar geliştirilemez. Daha da ileriye gidersek önce stratejinin hazırlanması, sonra stratejik seviye planın hazırlanması oldukça sık karşılaşılan bir yöntem olarak karşımıza çıkmaktadır. Bu anlamda politik direktif çerçevesinde önce askeri strateji hazırlanabilir, stratejik seviye

tarafından bu stratejinin icraata konulabilmesi için stratejik bir plan hazırlanarak strateji uygulamaya sokulabilir. Strateji ile stratejik planın ayrı anlamlar ifade ettiği göz önünde bulundurulmalı, birbirleri ile karıştırılmamalıdır. Aynı husus iş hayatı, sağlık, kamu yönetimi gibi alanlar için de geçerlidir.

1.5.3.Stratejinin Özellikleri

Uzun Süreli Olması: Stratejinin en fazla bilinen özelliklerinden birisi uzun vadeli olmasıdır. Tasarımcı uzun vadeye bakarak karar vericilerin acil olandan daha ziyade önemli olana odaklanmasını sağlar. Bu önemli problemlerle karşılaşmadan zamanı iyi kullanarak çözüme kavuşturmak, sorunlar karşımıza çıkmadan, hatta problem haline gelmeden çözüme kavuşturmak veya ortamı şekillendirerek sorunları çözmek proaktif yaklaşımın temelini oluşturmaktadır. Bunun aksini yapmak yalnızca cari konulara odaklanmak kartopunun çığa dönüşmesine benzer bir sonuç yaratabilecektir. Zamanında uzun vadeli olarak çalışma yapılmaması, sorunların çığ gibi birikmesine ve içinden çıkılmaz hale dönüşmesine neden olabilecektir. Geleceği tahmin etmenin en iyi yolu uzun vadeli düşünerek şekillendirmektir. Bu nedenle uzun vadeli tasarımların yapılması gerekmektedir. Genellikle beş yıldan otuz yıla kadar değişen bir zaman aralığında stratejilerin tasarlandığı görülmektedir. Klasik anlamda Güvenlik Stratejilerinde icra edilen faaliyetin, etkinin sonucunun alınması aylar, hatta yıllar almaktadır. Bu nedenle stratejik sabır önem kazanmaktadır. Bir devletin stratejik seviyede aldığı tedbirlerin diğer devletin veya sistemin davranışlarını değiştirmesinin sonucunun alınması için devamlılık ve istikrar gerekmektedir. Stratejilerin ancak uzun vadeli planlanmasıyla proaktif yaklaşımlar sergilenebilir.

Kapsamlı Yaklaşım Gerektirmesi: Gerek mevcut durumun değerlendirilmesi gerek konseptlerin ortaya konulmasında kapsamlı yaklaşım esas alınmalıdır. Strateji artık sadece askeri güç unsurları ile değil ekonomik, politik, diplomatik güç unsurlarından oluşan millî güç unsurları gibi birbirleri ile koordineli olarak kullanılmasıyla tasarlanabilmektedir. Herhangi bir güç unsurunun nihai hedefe etkisinin veya diğer bir güç unsurunun kullanılmasına olan olumlu veya olumsuz etkisi hesaba katılmalıdır. Stratejik durumun izlenmesinde de bu husus dikkate alınarak izlenecek hususlar dikkatlice seçilmelidir. Özetle tek ağaca odaklanıp ormanın gözden kaçırılmaması gerekir.

Güç Unsurlarının Kullanımının Hassasiyeti: Politik düşünme ile stratejik düşünmeyi ayıran en önemli özelliklerden birisi politikanın enstrümanları ile stratejinin enstrümanlarının farklı olmasıdır. Politikacı genellikle verdiği beyanatın, basın açıklamasının yeterli olduğunu düşünürken; stratejist beyanatlar neticesinde istenen sonuca ulaşılamayacağını, millî güç unsurlarının koordineli bir şekilde kullanılması gerektiğini bilmelidir. Stratejist güç unsurlarını kullanarak politikayı operasyona veya gerçek, somut faaliyetlere dönüştürerek başarıya ulaşması gerektiğini bilmelidir. Bu nedenle millî güç unsurlarının kabiliyetlerine hâkim olunması, hangi hedefin veya amacın gerçekleştirilmesinde ne gibi katkılarının olabileceğinin, kuvvetli, zayıf taraflarının iyi tespit edilmesi gerekmektedir. Bunun yanında millî güç unsurlarının oluşturulması, etkinliğinin artırılması ve idame ettirilmesi için de gayret sarf edilmelidir. Savunma Planlama Sistemi buna iyi bir örnek olarak verilebilir. Bir ordunun mevcut operasyonlar, muhtemel savaş senaryoları, geleceğin muharebe sahası ve teknolojik gelişmeler çerçevesinde savunma planlaması ile askeri güç unsurunun etkin şekilde muharebeye hazır olmasını sağlaması iyi bir örnek teşkil edebilir.

Amaca Odaklanılması: Strateji tasarımında iki amaç önem kazanmaktadır. Birinci amaç stratejinin hazırlanma amacı, ikincisi ise stratejinin icrası ile ulaşılması beklenen amaçtır. Örnek olarak strateji hazırlama amacı iç güvenliğin sağlanması, bir bölgenin istikrara kavuşması, millî güç unsurlarından birisinin geliştirilmesi gibi olabilir. Bunlardan iç güvenlik stratejisi için terör örgütünün etkisiz hale getirilmesi, istikrarın sağlanması için uluslararası yardımların ulaştırılması gibi amaçlar ortaya konulabilir. Birinci amaç stratejinin formatını dikte ettirirken, ikinci amaç stratejinin mantığını dikte ettirebilecektir. Stratejinin icrası maksadıyla ortaya konulan bir kutup yıldızı gibi gerek strateji tasarımında gerek ise icra esnasında her zaman göz önünde tutulmalıdır. Amacın uygulanabilir olması için devletin (aktörün) yeteri kadar güçlü olması ve gerekli millî güç unsurlarına sahip olması gelmektedir.

Uyum: Nihai hedef, konsept, kaynak(güç unsuru), uyumunun yanında; bütün millî güç unsurlarının koordineli, organize, bütüncül bir şekilde azami verimin ve etkinliğin sağlanacak şekilde yönlendirilmesi önem arz etmektedir. Bunun yanında stratejiyi tasarlayanın, icracılar olan değişik kurum ve kuruluşlarla da uyumlu olması gerekmektedir. Bazen kurumlar içerisinde icrayı olumsuz etkileyebilecek atalet oluşabilmektedir. Ayrıca bu kurum ve kuruluşların her birinin kendi gündemleri ve

önceliklerinin olması stratejinin arzu edilen düzeyde uygulanmasını etkileyebilecektir. Stratejik ortamın oldukça karmaşık olduğu dikkate alındığında millî güç unsurlarının birbirlerinin etkisini olumsuz etkilemeyecek şekilde, bir hedef üzerine sıklet merkezi oluştururken diğer bir hedefin olumsuz etkilenmesinin engellenmesi için ilave tedbirler alınması gerekebilecektir.

Rakibin/Düşmanın Hesaba Katılması: Strateji tasarımında dikkate alınması gereken en önemli konulardan birisi düşmanın veya rakibin de bir stratejisinin olduğu, bu nedenle tasarıma karşı bir direnç oluşacağı ve stratejinin öngörüldüğü şekilde uygulanamayabileceğidir. Askeri anlamda düşman imkân ve kabiliyetleri ile hal tarzları sürekli dikkate alınan önemli bir faktördür. Ancak iş hayatında veya dış ilişkilere yönelik bir strateji tasarımında düşman yerine rakipler, hatta tarafsızlar bulunmaktadır. Stratejinin kapsadığı uzun bir vade boyunca her bir rakibin veya tarafsızın uygulayacağı stratejik hal tarzlarının belirlenmesi oldukça zordur. Ayrıca dost tarafın veya tarafların da hal tarzlarının takip edilmesi ve tarihte şahit olunduğu şekilde, düşman konumuna geçmeleri sorunu daha karmaşık hale getirebilecektir. Bu durumda bu aktörlerin de kendi menfaatleri, hedefleri olacağı stratejik tasarımın beklendiği şekilde uygulanmasına engel olacağı, etkileyebileceği akılda tutulmalıdır. Aslında bir strateji nadiren tasarlandığı şekilde icra edilebilecektir. Burada esas olan tasarımda bunun dikkate alınması ve gerekli uyarlamaların zamanında yapılması için tasarımda zemin oluşturulabilmesidir. Strateji tasarımı bir düşünme sistemi olarak algılanmalı; bu düşünme sisteminin süreç içerisinde stratejik durumun izlenmesi, değerlendirilmesi, kararların verilmesi için bir satranç tahtası oluşturduğu göz önüne alınmalıdır.

Değerlendirme Yapılmasının Zorluğu: Taktik seviyede yapılan bir icraatın değerlendirilmesi nispeten daha kolaydır. Bunun temel nedenlerinden bazıları olayların ve sonuçlarının gözlemlenmesinin daha kolay olması; zaman, mekân, kuvvet anlamında dar çerçevede olması gibi hususlar verilebilir. Ancak stratejik anlamda birçok olayın gelişimi gözden uzak olarak gerçekleşebilecek, sonuçlar gözle değerlendirilemeyecektir. Bunun yanında zaman, mekân, kuvvet açısından da çok daha geniş, karmaşık bir süreç izlenebilecektir. Bu nedenle strateji tasarımının daha başlangıcında değerlendirmenin nasıl yapılacağı düşünülmesi gerekmektedir.

Stratejik Yönetimin Yerinde Görmeden Yapılmasının Zorluğu: Liderler taktik seviyede genellikle görerek, bizzat nezaret ederek planın icrasını sağlarlar. Stratejik seviyede bu neredeyse mümkün değildir. Dolayısı ile liderler tahayyül ederek sevk ve idare etmek zorunda kalırlar. Bu çerçevede hem rakibin yaklaşımlarını hem de dost unsurların yaklaşımlarının tahayyül edilmesi gerekmektedir. Liderlerin stratejik olarak gelişen durumu anlamaları ve karar vermeleri de oldukça zor olmaktadır. Liderlerin bilgi seviyesi, tecrübesi gibi liderlik özellikleri icrayı kolaylaştırıcı etki yaratırken, tasarımda bu sorun akılda tutularak gerekli ilave tedbirlerin alınması düşülmelidir.

1.5.4. Klasik Güvenlik Stratejisi Tasarım Süreci

Güvenlik stratejisi hazırlanması diğer alanlardaki stratejilerden bazı farklılıklar arz etmektedir. Örneğin güvenlik strateji hazırlanmasında en önemli hususlardan birisi riskin ve tehdidin iyi belirlenmesi ve etkisiz hale getirilmesidir. Buna karşın bir basketbol antrenörünün stratejik hedefi ise diğer takımlar ile rekabet ederek galip gelmektir. Bunun yanında iş hayatında; şirket stratejisi, sektör stratejisi, rekabet stratejisi gibi değişik strateji çeşitleri ile karşılaşmak mümkündür. Belirtilen stratejilerin formatları ve mantıklarının tasarlanma amaçlarına uygun bir yapıda olmaları gerekmektedir.

1.5.4.1. Güvenlik Strateji Tasarımda Dikkat Edilmesi Gereken Genel Hususlar

Deneyimler neticesinde elde edilen aşağıdaki sonuçların güvenlik stratejisi tasarımında kullanılması önerilmektedir.

- İnsan beyni taktik, yani kısa vadeli düşünmeye odaklanmıştır. Bunun bilincinde olunarak stratejik düşünme sisteminin göz ardı edilmemesi gerekmektedir.
- Öngörü stratejik tasarımın temelidir. Mühim olan bugünden yarını görmek değil, geleceği görmek, belirlenen nihai hedefe ulaşmak için oyun kurabilmektir.
- Uygulanan stratejinin sonuçlarını görmek oldukça zordur. Ancak eğitilmiş, deneyim kazanmış uzmanlar stratejinin sonuçlarını önceden tespit edip gerekli düzeltmeleri yapabilirler.
- Stratejik düşünme sisteminin elemanları arasında bir uyum olmalıdır. Bu çerçevede nihai hedef ile millî güç unsurları veya konsept arasında uyum olmalıdır.

- Strateji tasarımı uygulama göz önünde tutularak yapılmalıdır. Uygulanamayan strateji bir hikâye anlatımından öteye gidemez.
- Basitlik strateji tasarımında en büyük güçtür. Basit, anlaşılır tasarım koordinasyonu ve uygulamayı kolaylaştıracaktır.
- Stratejik tasarım çok iyi olabilir. Ancak icracı makamlar tarafından icraya uyarlanamıyorsa hayal kırıklığı yaratabilir.
- Stratejik tasarımın planlandığı şekilde icra edilmesi oldukça nadirdir. Bu bilinçle stratejist stratejik durumu sürekli takip etmeli, riskleri önceden tespit edebilmeli ve gerekli teklifleri, düzeltmeleri ön alarak yapabilmelidir.
- Strateji uygulanmaya başlar başlamaz bazı sınamalarla karşılaşılacak, beklenen sonuçlar alınamayabilecektir. Bu tasarımın hatalı olduğu anlamına gelmemelidir. Strateji tasarımı sevk ve idarenin yapılabilmesi için bir satranç tahtası ve düşünme sistemi üzerine oturtulmuş bir hipotez olarak görülmelidir.
- Rakibin veya düşmanın da bir stratejisi olduğu unutulmamalıdır. Tasarlanan stratejinin gerek rakip, gerek ise diğer aktörler ve doğal nedenler ile dirençle karşılaşabileceği dikkate alınmalıdır.
- Strateji tasarımı her konu veya fonksiyon için aynı olmayabilir. Konunun özelliğine göre stratejik düşünme sistemi ve tasarı gözden geçirilmeli, uygulama esas alınmalıdır.

1.5.4.2.Millî Güvenlik Stratejisi

Güvenlik strateji denildiğinde ilk ve genellikle akla gelenlerden birisi millî güvenlik stratejisidir. Vestfalya Anlaşması ile beraber egemenlik ve toprak kavramlarının devletin temel unsurları olarak uluslararası sistemde kabul edilmesini müteakip Fransız İhtilali (1789) ile beraber ulus oluşturulması ve ulus-devletlerin uluslararası sistemin temel aktörleri olarak ortaya çıkmasına neden olmuştur. Hatta Napolyon ile birlikte vatandaşın güvenliğinin devletin görevi olduğu, bunun da askeri-diplomatik araçlarla sağlanabileceği yaklaşımı oluşmaya başlamıştır. Hobbes ve Locke'u müteakip Jean-Jacques Rousseau'nun (1712-1789) toplum sözleşmesi konusundaki görüşleri[47] ile birlikte devlet güvenliği ile birey güvenliği iç içe geçmiştir. Ulus-devletler millî güvenliği sağlayarak; her üç analiz düzeyinde bireyin, devletin,

[47] Rousseau Jean-Jacques, Toplum Sözleşmesi (Fransızcadan çeviren Günyol, Vedat,2006),1762.

uluslararası sistemin güvenliklerini sağlamayı hedeflemeleri başarı için dikkate almalıdır.

Devletler genellikle güvenliklerini sağlamak maksadıyla hiyerarşik bir doküman yapısı oluşturmaktadırlar. Bu dokümanların başında devlet idaresinin temelini oluşturan Büyük Strateji (Grand Strategy) gelmektedir. Büyük strateji; millî ekonomik hedeflere ulaşılması, refahın sağlanması, aynı zamanda güvenliğin sağlanması için millî güç unsurlarının kullanılmasının ve koordinesinin anlatıldığı bir dokümandır. Büyük Strateji alt strateji ve planlara yeteri kadar yol gösterebilecek, ancak her bir durum için uygun tasarımın oluşturulabilmesi için yeterli esnekliği sağlayabilecek, yaratıcılığı engellemeyecek bir içerikte hazırlanmalıdır.

Büyük Stratejinin tarihi süreçte, tarım çağında bir savaş durumunda ülkenin bütün güç unsurlarını bir araya getirerek belirli bir savaşın kazanılması maksadıyla oluşturulduğu ifade edilebilir. Bu anlamda Osmanlı İmparatorluğu'nun tarım çağının güvenlik anlayışı çerçevesinde fetihler temelinde geliştirdiği ve tımar sistemi ile desteklediği Büyük Stratejisi örnek olarak verilebilir. Osmanlı İmparatorluğu'nun fethedilecek bölgelerin tespit edilmesi, olgunlaştırılması, ittifakların oluşturulması, ordunun bu bölgeye intikal ettirilmesi, kuşatmalara ve savaşlara hazırlanılması, savaşların icra edilmesi, fethedilen bölgelerde yeni yönetimlerin ve esas olarak toprağa bağlı bir düzenin kurulması içerisinde bulunulan çağın Büyük Strateji tasarımına iyi bir örnek teşkil etmektedir.

Büyük Strateji kavramının sanayi devrimi sonrası yaşanan Birinci Dünya Savaşını müteakip kullanılmaya başlandığı ifade edilebilir[48]. İkinci Dünya Savaşı'yla beraber Büyük Strateji kavramının daha da belirgin olarak kullanılmaya başlandığı görülmektedir. Bu dönemde yalnızca savaş zamanında değil öncesinde ve sonrasındaki barış döneminde millî güç unsurlarının oluşturulması, güçlendirilmesi dâhil Büyük Strateji kavramının kullanılması gerektiği yönünde değerlendirmeler bulunmaktadır.[49] Artık düşmanın yenilmesi, savaşın kazanılması için yeterli olmamaktadır. ABD'nin 2003 yılındaki Irak Savaşı'nda, çatışmaların sona ermesini müteakip istikrar harekâtını yeteri kadar dikkate almamasının önemli sonuçları olduğu bilinmektedir. Ayrıca savaşın yönetiminde kaynaklarla nihai hedef arasında bir dengenin kurulması Büyük Stratejinin en önemli fonksiyonlarından birisi olarak görülmektedir. Bu dikkate alınmadığı zaman bazen savaş kazanılmasına rağmen

[48]Brands, Hals, *What Good is Grand Strategy*, 2014, s.2.
[49] Brands, Hals, *What Good is Grand Strategy*, 2014, s.2

kaynakların tamamen tüketilmiş olması veya ordunun gücünün kalmaması önemli bir problem sahası olarak ortaya çıkmaktadır. MÖ 280'de yaşanmış olan Pirus savaşı bu duruma iyi bir örnek olarak verilebilir. Bu savaşta zafer kazanılmıştır. Ancak elde ordu kalmamıştır.[50]

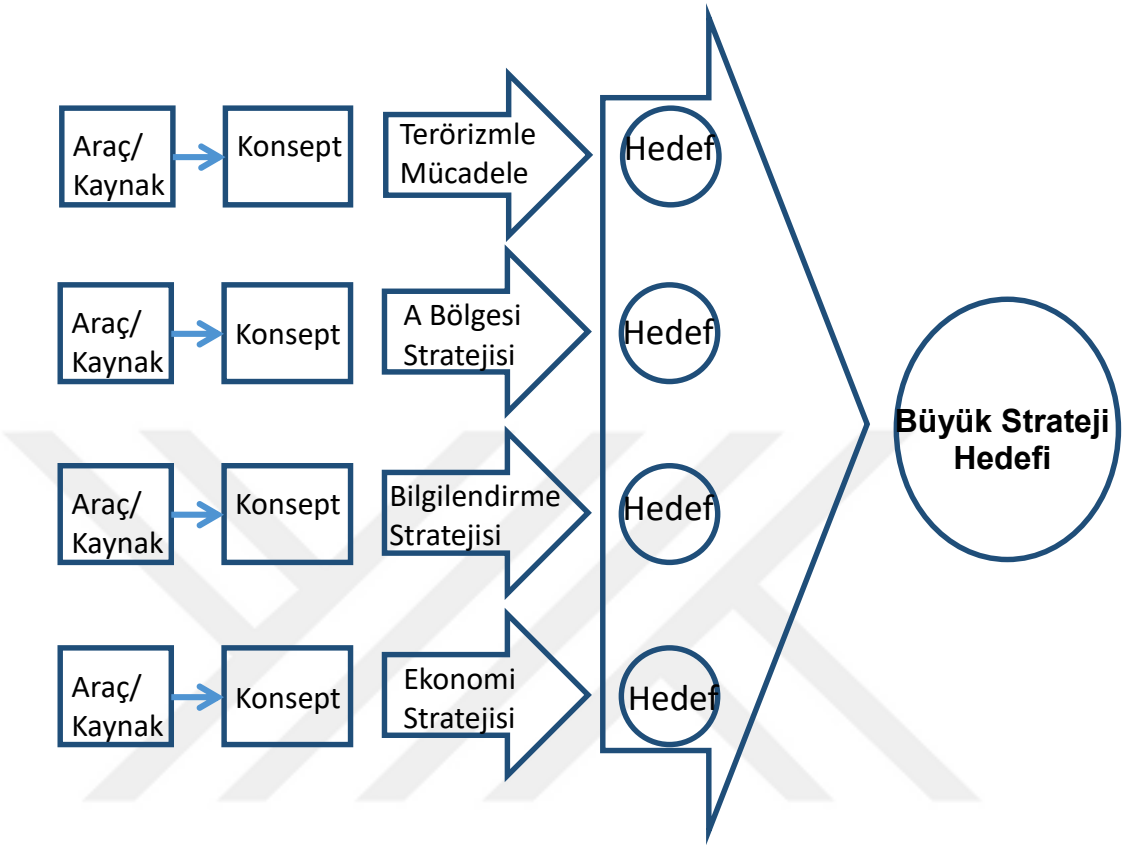
Büyük Strateji modeline bir örnek Şekil 1.2'de verilmiştir. Bu örnekte belirlenen başlıklar ülkelerin veya aktörlerin amaçlarına göre farklılık gösterebilir. Bu anlamda ABD'nin uygulayacağı Büyük Strateji ile Türkiye'nin uygulayacağı Büyük Strateji gerek başlıklar gerek tasarımda farklılıklar arz edecektir.

Araç/Kaynaklar (güç unsurları) her zaman sınırlı, ulaşılmak istenen hedefler ise sonsuzdur. Bu çerçevede kaynaklar ile hedefler arasında bir uzlaşı ve uyum sağlanmalıdır. Elde yeterli kaynak olmadan ulaşılamayacak hedeflerin seçilmesi Büyük Strateji çerçevesinde başarıya ulaşılmasında sıkıntılar ve riskler yaratabilecektir. Bu durumda gerekli veya ana hedefler belirlenmeli, kısıtlı kaynaklar ile uyumlu hale getirilmelidir.[51] Bu husus küresel veya bölgesel güç konumundaki aktörlerin Büyük Strateji hazırlamada en sık karşılaştığı problemlerden birisi olarak ortaya çıkmaktadır. Örneğin ABD bu hususlarda zor kararlar almak ve Büyük Strateji tasarımda bazı hedeflere öncelik verirken diğer hedeflerden vazgeçmek zorunda kalabilmektedir.

Dolayısıyla Büyük Strateji tasarımı ve yönetimi oldukça zordur. Ancak başarılı bir devlet idaresinin en önemli fonksiyonlarından birisi Büyük Stratejiye sahip olunmasıdır. Kaynaklar hiçbir zaman eldeki tehditler ile baş etmek veya fırsatları değerlendirmek için yeterli olmayacaktır. Bunun yanında bir devletin millî güç unsurları ile orantısız olarak birçok bölgeye yayılması, operasyonlar yapması başka aktörler tarafından istismar edilebilecek önemli bir zafiyet veya hassasiyet olarak ortaya çıkmaktadır. Bu nedenle Büyük Stratejinin mantık çerçevesinin iyi kurulması hayati önemi haizdir.

[50] Merriam Webster, https://www.merriam-webster.com/words-at-play/pyrrhic-victory-meaning, 26 Mart 2023
[51] Brands, Hals, *What Good is Grand Strategy*, 2014, s.3.

Şekil 1.2: Büyük Strateji (Örnek)



Büyük Strateji çerçevesinde hazırlanacak millî güvenlik Stratejisi güvenliğin sağlanması maksadıyla millî güç unsurlarının geliştirilmesi, kullanılması, koordine edilmesini sağlayan bir dokümandır. Millî Güvenlik Strateji Belgesi Büyük Strateji görevi görmektedir. NATO'da ise stratejik konsept aynı şekilde görülebilir.

Millî Güvenlik Stratejisi esas alınarak güvenliğin sağlanmasında temel teşkil eden askeri strateji, iç güvenlik stratejisi, dış güvenlik stratejileri tasarlanabilir. Bu stratejilerin her biri güç unsurlarının millî hedeflere ulaşmak için belirlenen kendi konularına yönelik hedeflere ulaşılabilmesi için ilgili güç unsurlarının barış ve savaşta kullanılmasını ve hatta geliştirilmesini içerebilir.

Ulus-devletler vatandaşlarının güvenliğini, toprak bütünlüklerini ve egemenliklerini millî güvenlik stratejilerini oluşturarak korumaktadırlar. Oluşturulacak millî güvenlik stratejisinde iç ve dış güvenlik beraber ele alınmalı ve

uyum içerisinde olmalıdır. Yalnızca dış güvenliği veya iç güvenliği esas almak yeterli olmayacaktır. Dış ve iç güvenlikten hangisine öncelik verilebileceği ise söz konusu devletin millî menfaatleri, risk ve tehdit durumu, uluslararası konjonktür gibi hususlar göz önüne alınarak belirlenebilir. Bunun yanında özgürlük ve güvenlik dengesi göz önünde bulundurularak, bireyin özgürleştirilmesinin güvenliğin sağlanmasında önemi bir parametre olarak ortaya koyan yaklaşım çerçevesinde millî güvenlik stratejisinin sağlam temellere oturtulması sağlanabilir. Millî güvenlik strateji belgesi diğer stratejilere ve planlamalara ışık tutacak çatı veya referans dokümandır. Bu çalışmada, bahse konu dokümanın genel yapısının aşağıdaki başlıkları kapsaması gerektiği önerilmektedir.

- Giriş
- Millî Menfaatler, Haklar, Değerler
- Stratejik Durum Özeti
- Mevcut ve Potansiyel Tehditler/Fırsatlar
- Nihai Durum ve Hedefler
- Millî Güç Unsurları
- Savunma Politikası
- İç Güvenlik Politikası
- Dış İlişkiler Politikası
- Diğer Güvenlik Politikaları
- Riskler ve Risk Yönetimi
- Millî Güvenlik Stratejisi Yönetimi
- Sonuç

Millî Güvenlik Stratejisinin en önemli bölümlerinden birisi Millî Menfaat, Haklar, Değerler kısmıdır. Bu bölümde devletin bütün kurum ve kuruluşların üzerinde mutabakat sağladığı menfaatlerin, hakların, değerlerin ortaya konulması müteakip aşamada hazırlanacak alt stratejilere referans veya başlangıç noktası oluşturabilecektir. Yine tehditlerin ortaya konulması önemli bir başlangıç noktası verebilir. Ancak bu tehditler üretilecek alt stratejilerin özelliklerine göre uyarlanmak durumunda kalınabilir. Millî Güç Unsurları genel olarak ifade edilerek kullanım esasları belirtilebilir. Riskler ve Risk Yönetimi bölümünde ise Millî Güvenlik Stratejisine risk oluşturan ve bu stratejiden kaynaklanan riskler ortaya konularak nasıl yönetilebileceği açıklanabilir. En son olarak da stratejinin nasıl yönetileceği belirlenir ve devletin

kurumlarından periyodik raporlama ve değerlendirmeler istenebilir. Millî Güvenlik Stratejisinin genel anlamda yön ve direktif vermesi, detaya girmemesi ve alt stratejilerin Büyük Strateji ile uyumlu olarak detaya girmesi ile bütüncül bir yaklaşım sağlanabilir. Daha önce de belirtildiği gibi Millî Güvenlik Stratejisi yani Büyük Strateji yol gösterebilecek, ancak yeterli esnekliği sağlayabilecek, yaratıcılığı engellemeyecek bir içerikte hazırlanmalıdır.

Bu prensipten hareketle klasik strateji tasarımına göre Millî Güvenlik Strateji Belgesinin en önemli özelliklerinden birisi detaya girilmemesi, alt stratejilerin tasarlanabilmesi için gerekli alt yapının hazırlanabilmesidir. Bu çerçevede stratejinin konsept veya hedeflere nasıl ulaşılacağı oldukça genel hatlarla ifade edilebilir. Büyük Stratejinin yönetimi alt stratejilerin koordinesi ve aynı hedefe odaklanabilmesi için önem arz etmektedir. Bu nedenle raporlama, değerlendirme, karar sisteminin kurulması ve takip edilmesi, alt kurulların oluşturulması tasarlanabilir.

Millî Güvenlik Strateji belgesinin direktifleri doğrultusunda; savunma, dışişleri, iç güvenlik, terörizmle mücadele, kamu diplomasisi ve stratejik iletişim, istihbarata karşı koyma, istihbarat, siber güvenlik, bilgi güvenliği, salgın hastalıklarla mücadele, kritik tesislerin savunulması gibi konularda ayrıca stratejiler hazırlanır. Bu stratejilerin gerek birbirleri ile gerek ise ana belge olan Millî Güvenlik Stratejisi ile uyumlu olmasına dikkat edilir. Bu stratejilerin haricinde bölgesel veya fonksiyonel stratejiler de hazırlanması gerekebilir.

Birçok stratejinin hazırlanması oldukça karmaşık bir durumun oluşmasına neden olabilecektir. Bu nedenle stratejilerin Millî Güvenlik Stratejisi çatı doküman olacak şekilde hiyerarşik olarak hazırlanması sorumlulukların belirlenmesine yardımcı olurken, dublikasyonu engelleyebilecek, stratejilerin birbirlerini olumsuz etkilememelerini, millî güç unsurlarının etkin kullanımını ve stratejilerin birbirleriyle uyumlu olmasını, etkilerini artırmasını ve yönetimin etkin olmasını sağlayabilecektir.

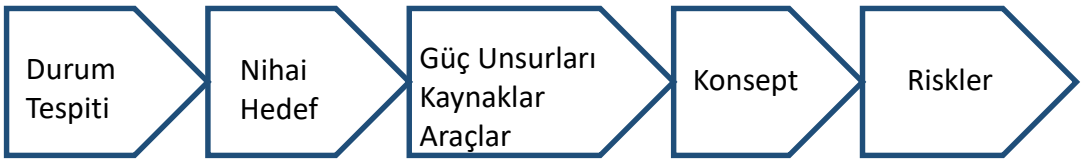
Bu nedenle strateji tasarımı ile görevlendirilen uzmanların öncelikle çatı doküman olan Millî Güvenlik Stratejisi başta olmak üzere mevcut stratejilere hâkim olmaları, onların mevcut durumları ve gelinen aşamayı iyi bilmelidirler. Strateji uzmanı üzerinde çalıştığı stratejinin yukarıda açıklanan sistem elemanlarını taslak olarak hazırlamalı ve başta Millî Güvenlik Stratejisi olmak üzere diğer stratejiler ile sistemin uyumlu olup olmadığını kontrol etmelidir. Gerekli değişikliği yaparak uyumlu hale getirmelidir.

Bu çerçevede ABD'nin Soğuk Savaş'ta kullandığı "çevreleme" stratejisi değişik kaynaklarda Büyük Strateji veya iyi bir Millî Güvenlik Stratejisine örnek olarak gösterilmektedir. ABD'nin çevreleme stratejisi ana strateji olurken, bu stratejiyle uyumlu olarak; Marşal Planı, Kore ve Vietnam savaşları, en son "Yıldız Savaşları Projesi" gibi alt stratejiler hazırlanmış ve başarıyla uygulamaya konulmuştur. Nükleer bir savaş tehlikesinin olduğu bir ortamda SSCB'nin içeriden çökmesi ana hedef olarak alınmış ve başarıya ulaşılmıştır. SSCB'nin yıkılmasından sonra ise NATO'nun genişlemesi, terörizmle mücadele gibi yeni stratejilerin uygulamaya konulduğu bilinmektedir. Bu değişimin farkında olmak ve yeni bir strateji ortaya koymak ayrı bir uzmanlık istemektedir. Dolayısı ile Millî Güvenlik Stratejileri sürekliliği olan, gerektiğinde güvenlik ortamının değişimiyle birlikte tasarımının yenilenmesi gereken stratejilerdir. Bunun yanında destekleyici stratejilerin de aynı işleme tabi tutulması ve ihtiyaç duyulan stratejilerin oluşturulması gerekmektedir. Burada süreklilik ve değişim iç içe geçmiştir. Bu değişim yapılırken güvenlik ortamındaki; eski hususlardan geçerli olanların, geçerliliğini yitirmiş olanların, yeni ve geçerli olanlar ile yeni ve geçersiz olanların tespit edilmesi sağlanmalıdır. Eğer bu değişimin parametrelerini zamanında fark edip gerekli değişikliği yapılmazsa mevcut stratejiler geçmişin hikâyeleri olarak kalabilecektir.

Millî Güvenlik Stratejisi tasarımı dört şekilde sonuçlanabilir. Bunlar reaktif, aktif, preaktif ve proaktiftir. Bunu açıklamak için araba kullanan bir sürücüyü örnek verelim. Eğer sürücü dikiz aynasından aracı kullanıyorsa, geçmişteki olaylara müdahale edecek reaktif kalacaktır. Eğer yan aynaları kullanarak arabayı kullanıyorsa, aktif olacak yakınında gerçekleşen olaylara reaksiyon göstererek aktif olacaktır. Sürücü önüne, ileri bakarak arabayı kullanıyorsa olaylar gerçekleşirken görecek ve tedbir alabilecek, preaktif olarak sürüşü gerçekleştirebilecektir. Sürücü yola çıkmadan hava durumu, trafik durumu, yol durumu gibi faktörleri hesaplayarak güzergâhını tanımlayıp sürüşü gerçekleştirebiliyorsa proaktif sürüş gerçekleşebilecektir. Stratejik tasarımdan beklenen proaktif bir yaklaşımla stratejik ortamın millî menfaatler çerçevesinde, durum üstünlüğü sağlanabilecek şekilde durumun şekillendirilebilmesidir.

Klasik güvenlik stratejisi tasarımı bir süreç takip edilerek yapılmaktadır. Bu sürecin safhaları Şekil 1.3'te gösterilmiştir.

Şekil 1.3: Güvenlik Stratejisi Tasarım Süreci



1.5.4.3.Güvenlik Stratejisi Tasarım Süreci

1.5.4.3.1.Stratejik Durum Analizi

Stratejik tasarımın ilk adımı stratejik durum analizidir. SunTzu'nun "Hem düşmanınızı hem de kendinizi tanıyorsanız yüz tane savaştan bile korkmanıza gerek yok" ifadesi stratejik durum analizinin önemini en iyi vurgulayan sözlerden birisidir.[52] Durum analizi tasarım faaliyetlerine önemli bir zemin ve girdi sağlayabilecektir. Stratejik durum analizi stratejik tasarımın başında yapılan bir faaliyet olarak görülmesine rağmen, stratejinin yönetimi aşamalarında ağırlıklı olarak sürekli kullanılacak önemli bir yapıdır. Bu nedenle durum analizi sistematiği bu husus göz önünde tutularak, başlangıçtan itibaren süreç içerisinde etkin bir şekilde kullanılabilecek bir yapıya oturtulmalıdır. Güvenlik stratejisinin icrası esnasında oluşturulan bu sistematik sürekli kullanılacak ve elde edilen sonuçlarla stratejiye yön verilebilecektir.

Bu çerçevede karar verici veya herhangi bir organizasyon, etrafında olanları gözetler, odaklanır, karar verir ve kararı icra eder. İnsanın çevresinde gözetlemesi gereken birçok şey vardır. Ancak insanın amacı veya ilgilendiği konulardan kendi ilgi sahasına girenler üzerine odaklanması gerekir. Karar vericinin/organizasyonun üzerine odaklandığı konuları amaçları doğrultusunda anlaması, değerlendirmesi, yani analiz etmesi gerekmektedir. Karar verici ancak bu değerlendirme sonucunda nihai hedefine ulaşması için neler yapması gerektiğini ortaya koyabilecektir. Özet olarak teşhis-karar-değerlendirme sürecinin oluşturulması stratejinin başarıya ulaşmasında önemli bir faktör olarak ortaya çıkmaktadır.

Stratejik durum analizinin başlıkları veya parametreleri stratejinin tasarım amacına göre değişebilir. Örnek olarak eğer tasarım amacı bir ülkenin etki altına

[52] Sun Tzu on the Art of War, Allandale Online Publishing, 2000, s.11

alınmasıysa sistem yaklaşımıyla hedef ülkenin bütün millî güç unsurlarının incelenmesi; askeri bir harekât icra edilmesi amaçlanıyorsa hedef ülkenin ordusunun yapısının incelenmesi uygun olacaktır.

Millî Güvenlik Stratejisi tasarlandığı düşünüldüğünde; küresel, bölgesel ve kendi Türkiye'nin durumunun incelenmesi dikkate alınabilir. Ancak burada cevap verilmesi gereken en önemli soru incelemede kullanılabilecek analiz düzeyi ve referans noktalarıdır. Bu hususlar belirlenmeden yapılacak inceleme tasarımın müteakip aşamalarında beklenen faydanın sağlanmasını engelleyebilecektir.

Yukarıda belirtildiği gibi strateji tasarımcısı, genellikle tasarıma boş bir kâğıtla başlar ve bu nedenle soracağı en önemli soru tasarımın amacı ve tasarıma nereden başlayacağı sorusudur. Buna ilave olarak strateji tasarımcısı ilgili birimlerden strateji tasarımını yönlendirebilecek yeterli direktif alamayabilecektir. Bu nedenle millî menfaatler, haklar ve değerler iyi birer referans noktası teşkil ederek bu sorunun en güzel cevabını oluşturabilir ve stratejik durum analizinde öncelikli olarak ortaya konulması gereken hususlardan birisidir.

Durum analizi genellikle "stratejik çerçeve" başlığı altında stratejik tasarım dokümanlarında yer almaktadır. Tasarımcıların yaptıkları en önemli hata yukarıda belirtildiği gibi stratejinin amacına göre durum analizinin içeriğini oluşturamamaları, yani stratejik çerçeveyi çizememeleridir. Bu bölüme ilgili ilgisiz konuların doldurulması analizin kalitesini etkilerken, tasarımcının dikkatini dağıtabilecek, yanlış bir istikamete odaklanmasına neden olabilecektir. Doğal olarak bu husus zincirleme olarak tasarım sürecinin diğer safhalarını da olumsuz etkileyebilecektir. Bir kez daha stratejinin amacının sürekli göz önünde bulundurulması gerektiğinin vurgulanması uygun olacaktır. Durum analizinde faydalanılabilecek bazı yöntemler ve parametreler müteakip maddelerde incelenmeye çalışılmıştır.

1.5.4.3.1.1.Millî Menfaatler, Haklar ve Değerler

Millî menfaat; takip edildiği takdirde bir devletin refahını artıran ve davranışlarını yönlendiren uzun vadeli temel ihtiyaçları veya arzuları olarak anlaşılabilir. Millî menfaatler; güvenlik, refah, millî değerler olarak sınıflandırılabilir. Millî menfaat kavramı ulaşılabilir belirgin hedefler olarak düşünülmemeli, bunun yerine uzun vadeli yol gösterici tanımlamalar, idealler olarak algılanmalıdır.

Bazı ülkelerin stratejilerine ışık tutacak idealler geliştirdikleri ve bu idealleri inatla tarihi süreçte takip ettikleri görülmektedir. “Büyük A ülkesi”, “Büyük ideal“ olarak tanımlanan benzer yaklaşımları, Türkiye’nin komşularında görmek mümkündür. Bu idealler barışçı olmaktan çok uzak olsalar da ülkelerin millî güvenlik stratejilerine önemli ve uzun vadeli net vizyonlar tanımlayan yaklaşımlardır. Bu yaklaşımların ayrıca millî birlik ve beraberliğin de korunmasına önemli katkıları bulunmaktadır.

Millî menfaatlerle bir devletin uluslararası anlaşmaların sonucunda elde ettiği veya jeopolitik konumu gibi nedenlerden dolayı sahip olduğu haklar da olabilir. Örneğin Türkiye’nin Ege Denizi ve Akdeniz’deki hakları buna iyi örneklerdir. Bu hakların korunması da millî menfaatler gibi güvenlik stratejilerine yön veren önemli referans noktaları olarak görülebilir.

Millî değerler de menfaatler ve haklar kadar önemli yol göstericilerdir. Millî değerler; devletlerin veya milletlerin kültürlerinin sonucu olarak iyi, arzulanan, faydalı olduğuna yönelik genel kabul gören inançlarıdır. Bunlardan bazıları; bağımsızlık, özgürlük, barış, adalet gibi değerlerdir.

Millî menfaatlerin tanımlanmasından sonra önem derecesine karar verilmelidir. Önem derecesinin tespit edilmesi millî menfaatlerin muhafaza edilmesi, korunması veya daha da geliştirilmesinin sağlanması için tahsis edilecek enerji, gayret ve kaynak konusunda bir karar verilmesine yardımcı olabilecektir. Bu maksatla kullanılabilecek bir ölçek bulunmamaktadır. Genel olarak kabul gören çalışmalarda; hayati menfaatleri korumak için devletlerin savaş dâhil birçok şeyi göze alabilecekleri; önemli menfaatleri korumak için harekete geçmeleri gerektiği, aksi takdirde devletin zayıflayabileceği; ikinci derecede önemli menfaatlerin korunmasının ancak tahsis edilecek kaynaklar asgari olduğunda kabul edilebileceği ifade edilebilir. Bu değerlendirmede kullanılan parametreler liderler ve zaman gibi faktörlere göre değişim gösterebilecektir. Bu nedenle durumla birlikte sürekli takip edilip önem derecelerinin değerlendirilmesi uygun olacaktır. Burada üzerinde durulması gereken konu; menfaatler tehdit edildiğinde veya fırsatlar yakalandığında önem dereceleri göz önüne alınarak karar verilmesi değerlendirmeye anlam kazandırabilecektir. Benzer hususların millî değerler ve haklar için de geçerli olacağı düşünülebilir.

1.5.4.3.1.2. Tehdit

Karşılaşılan bir durum millî menfaatleri olumsuz etkiler, zarar verebilir veya tehlikeye sokuyorsa tehdit olarak kabul edilebilir. Tehdit potansiyel bir yapıda olsa da tedbir alınmasını gerektirmektedir. Tehdit değerlendirmesindeki en önemli yol göstericilerden birisi tarihtir. Söz konusu aktörün tarihi süreçteki davranış analizinin yapılması önemli bilgiler verebilecektir. Bu çerçevede millî menfaatler gibi millî menfaatlerin tehdit edilip edilmediğine de karar verilmesi stratejik bir bakış açısı gerektirmektedir. Stratejik durum analizinde sorulabilecek en temel soru bu olabilir. Stratejist en tehlikeli, en muhtemel ve en iyi senaryolar üzerinde çalışarak bu soruların cevaplarını arayabilir. Bunun yanında rakibin uygulayabileceği hal tarzlarının ortaya konulması da sağlanabilir. Bu çalışmayla birlikte bir tehdit önceliklendirmesi yapabilir. Bunun sonucunda tehdidin bertaraf edilebilmesi için benimsenebilecek en iyi hal tazının ortaya çıkarılması sağlanabilecektir. Bu çerçevede hayati önemi olan bir menfaate ciddi bir tehdit olması ile ikinci derecede önemli bir menfaate dikkate değer olmayan bir tehdit durumuna uygulanacak hal tarzları doğal olarak farklılık arz edecektir.

Daha önce özet olarak bahsedilen tehdit değerlendirmesinde genel olarak tehdit = niyet x imkân kabiliyet formülü kullanılabilir. Herhangi bir aktörün niyetinin belirlenmesinde liderlerin söylem analizleri ve/veya eylemleri dikkate alınabilir. Liderlerin söylemlerinde güvenlikleştirdikleri konunun tehdit teşkil edip etmediği ve bu söylemin söz konusu aktörün halkı tarafından kabul edilip edilmediği, istihbarat kaynakları tarafından tespit edilen eylemler ile desteklenmesi, niyetin belirlenmesinde önemli parametreler olarak karşımıza çıkabilir. Söz konusu aktörün niyeti olabilir ancak imkân kabiliyeti olmayabilir. Örneğin bir ülkenin "Büyük A ülkesi" olma niyeti olmasına rağmen imkân kabiliyetini belirleyecek millî güç unsurlarının yeterli olmaması tehdit olma özelliğini azaltmaktadır. Ancak birçok aktörün aldatma tedbirlerini çok zekice uygulayarak niyetini ve/veya imkân kabiliyetini saklayarak tehdit olarak değerlendirilmesini ve tedbir alınmasını engellemeye çalıştığı dikkate alınmalıdır.

Tehdit değerlendirmesinde en önemli konulardan birisi tehdidin yapısının, özelliklerinin sürekli değişmekte olduğunun akılda tutulması gerektiğidir. NATO'nun Soğuk Savaş sonrasında SSCB'yi tehdit kategorisinden çıkarması, bu çerçevede güvenlik stratejisini yeniden tanımlaması çok iyi bir örnek teşkil etmektedir.

Günümüzde ise NATO'nun tekrar tehdit değerlendirmesi üzerinde çalıştığı bilinmektedir.

Bu çalışmada, tehdit değerlendirmesinin dört kategoride yapılması önerilmektedir. Bunlar; tehdit, potansiyel tehdit, risk ve tehdit değil. Herhangi bir aktörün tehdit olma özelliği niyet ve imkân kabiliyet olarak yukarıda belirtilmiştir. Potansiyel tehdit ise bunlardan birisinin var olduğu durumda gündeme gelebilmektedir. Bir aktörün niyeti vardır, ancak imkân kabiliyeti yoktur veya tam tersi olarak imkân kabiliyeti vardır, ancak şimdilik niyeti yoktur veya zayıftır. Risk olarak değerlendirme ise her ikisinin de ileride oluşabileceği ihtimalinin olması olarak ifade edilebilir. Bunlardan her ikisi de yoksa makul bir sürede ihtimal de görülmüyorsa tehdit olma özelliği yok olarak değerlendirilebilir. Bu kategorilerin sürekli değişmekte olduğu, bu nedenle sürekli bir değerlendirmenin yapılması ve zamanında gerekli tespitin yapılması gerektiğini tekrar vurgulamak uygun olacaktır. Bu çerçevede iyi bir stratejik istihbarat yapılanmasının önemi ortaya çıkmaktadır.

1.5.4.3.1.3. Fırsat

Uzman bir stratejist millî menfaatlere yönelik oluşan tehditlerin yanında, millî menfaatlerin pekiştirilmesi, geliştirilmesi için oluşan fırsatların stratejik seviyede, yeteri kadar zaman önce farkına varabilmesi gerekmektedir. Bu çerçevede Soğuk Savaşın bitmesi bazı aktörler için tehdit ortamının değişmesiyle beraber, değişik fırsatların da ortaya çıkmasına neden olmuştur. Bu fırsatların değerlendirilmesi millî menfaatlerin gelişimini olumlu etkileyebilecektir. Bu husus özellikle, bazı dost ve müttefik ülkeler veya NATO, AB gibi kuruluşlarda yapılan çalışmaların incelenmesiyle daha belirgin ortaya konulabilir. Soğuk Savaş sonrasında tehdit ortamı değişime uğrarken ve NATO için tehdit kalmadığına karar verilmesiyle beraber, NATO ve bazı aktörler için fırsatlar daha fazla ön plana çıkmıştır. Örneğin ilgi veya etki alanında olan bir bölgeye yönelik NATO'nun kriz yönetimine yönelik bir operasyonu başta AB olmak üzere değişik aktörler için uygun fırsatlar ortaya çıkarabilmiştir. Soğuk Savaş sonrası Balkanların durumu bunun için iyi bir örnek teşkil etmektedir.

1.5.4.3.1.4. Faraziyeler

Durum analizi yapılırken özellikle stratejik seviyede birçok sorunun, bilinmezin cevabının bulunmasında sorunlar yaşanacaktır. Stratejik tasarımın yapılabilmesi için bu soruların veya bilinmezliklerin cevaplandırılabilmesi için doğruluğu başlangıçta teyit edilemeyecek bazı varsayımlar kabul edilmek durumunda kalınacaktır. Bu varsayımlar faraziye olarak adlandırılmaktadır. Bu faraziyeler iyi belirlenmeli, uzmanlar tarafından iyi değerlendirilmelidir. Günümüz koşullarında bile durum analizi aşamasında birçok sorunun cevabı bulunamamakta, faraziyeler kullanılmak durumunda kalınabilmektedir. Bu faraziyeler rakiplerin, tarafsızların veya diğer aktörlerin imkân ve kabiliyetleri, niyetleri, küresel durumun dinamikleri, ülke içerisindeki dinamikler konusunda olabilir. Bu nedenle faraziyeler millî güvenlik stratejilerine yönelik gelişmelerin şekillendirilmesinde ve yönlendirilmesinde önemli bir yere sahiptir. Faraziyeler amaca uygun, üzerinde yeteri kadar düşünülerek, yeteri kadar titizlik gösterilerek yapıldığında stratejik tasarımın başarısını artırabilir. Bunun tam tersi olduğunda tasarımın başarısını olumsuz etkileyebilir. Stratejik tasarım esnasında ihtiyaca binaen birçok faraziyenin kabul edilmesi gerekebilecektir. Strateji uzmanları tasarımın başarısında esas olan faraziyeleri olumsuz sonuçlarını da değerlendirerek belirlemelidir. Stratejik istihbarat kaynaklarının bu faraziyeler konusunda daha ayrıntılı bilgi almak ve doğruluğunun teyit edilmesi için yönlendirilmesi uygun olacaktır. Faraziyelerin değişmesi stratejik tasarımın önemli ölçüde değişmesine etkisi olabileceği için uygulama boyunca da faraziyelerin yakından takip edilmesi gerekebilecektir. Strateji tasarımının genel özelliklerinden dolayı bu seviyede kabul edilen faraziyelerin daha alt seviyelerde ve stratejinin icraata dönüştürülmesi için hazırlanacak planlara önemli etkileri olabilecektir. Doğal olarak stratejik seviyede daha fazla faraziye üzerinde çalışılması gerekebilecektir.

1.5.4.3.1.5. Problemin Tanımlanması

Durum analiziyle birlikte stratejik tasarımın doğru soruna odaklanması ve sürecin parametrelerinin doğru belirlenebilmesi için kısa, açık, paydaşlar tarafından kabul edilebilen bir problem tanımlaması yapılması esas alınmalıdır. Bu şekilde strateji tasarımda çalışan bütün personelin aynı probleme odaklanması sağlanabilir. Problem tanımlaması; oluşan durumun hangi millî menfaatin tehdit altında olduğunu veya geliştirilmesi için fırsat oluşturduğunu içerebilir. Bu çerçevede bir örnek olması

açısından, A terör örgütünün B bölgesinde oluşturduğu terör kamplarının(durum); sınır güvenliğimize (millî menfaat) tehdit oluşturduğu; A terör örgütünün bu kampları kullanarak icra edeceği terör saldırılarının sınır bölgemizdeki vatandaşlarımızın güvenliğini tehdit edeceği (sebep) gibi bir problem tanımlaması yapılabilir. Bu çalışmada problemin tanımı maksadıyla kullanılacak bir formül önerilmektedir. Durum + millî menfaat + tehdit/fırsat oluşturma gerekçesi = problem tanımı. Bunun yanında askeri planlamalarda vazifenin ifadesinde kullanıldığı gibi; kim, ne maksatla, ne zaman, nerede, ne yapacak şeklinde örnek bir problem tanımı yapılabilir. Başka yöntemler de kullanılabilir. Ayrıca problem tanımı tasarım sürecinde sürekli gözden geçirilerek güncellenmelidir.

1.5.4.3.1.6.Küresel Durumun Analizi

Stratejik düşünme süreci genellikle uluslararası durumun değerlendirilmesiyle başlayabilir. Küresel değerlendirme; ülke dışında meydana gelen bütün olayları, faaliyetleri, durumları ve şartları içerebilir. Bilindiği gibi değerlendirilmesi gereken birçok olay ve faaliyet vardır. Stratejik düşünme yeteneği gelişmiş bir uzman bunlardan ülkenin ilgi ve etki sahasında olanları ve stratejinin tasarım amacını göz önüne almalı, olayları sistem yaklaşımıyla bütüncül olarak analiz edebilmelidir. Günümüzde uluslararası sistemin en etkili aktörü hâlâ ulus-devletler olarak görülmekle birlikte başta uluslararası örgütler, devlet dışı aktörler, terör örgütleri, uluslararası şirketler, güvenlik şirketleri gibi yeni aktörler ortaya çıkmıştır. Bu aktörlerin davranış kalıpları ve bu kalıpların oluşmasına neden olan karakterleri birbirinden oldukça farklıdır. Bu çerçevede bir devletin davranış kalıbı ile terör gurubunun davranışları ve eğilimleri farklılık arz edebilecektir. Durumu daha da karmaşıklaştıran millî menfaatleri etkileyen yalnızca rakip veya düşman aktörler olmayacak, tarafsız ve müttefiklerin de davranışları dikkate alınmak zorunda kalınacaktır. Buna ilave olarak bir etki veya ilgi sahasında; ulus-devletler, terör grupları, uluslararası şirketler, müttefikler, müzahir yerel gruplar, güvenlik şirketleri gibi değişik aktörler aynı anda bulunabilecektir. Hatta bu gruplar arasındaki ittifaklar günlük olarak değişebilecektir. Her bir aktör birbirinden farklı özelliklere sahip davranış kalıpları sergileyebilecektir. Bu nedenle stratejinin tasarım ve icra süreçlerinde her bir aktörün davranış kalıbının oluşturulabilmesi için ilave tedbir alınmalı, sürekli yakından izlenmelidir. Küresel durum analizinin en önemli

faydalarından birisi durum analizinin geniş bir görüş açısıyla ve bütüncül bir değerlendirme yapılabilmesidir. Bu husus küreselleşen bir dünyada daha da önemli bir hale gelmiştir.

1.5.4.3.1.7.Bölgesel Durumun Analizi

Günümüzde küresel analiz yapılmadan bölgesel bir analiz yapılması yeterli olmayacaktır. Büyük güçlerin veya varsa küresel güçlerin analize konu olan bölgeye yönelik menfaatleri veya eğilimleri mutlaka dikkate alınmalıdır. Her devletin etki ve ilgi alanı bulunmaktadır. Etki ve ilgi alanlarının sınırlarının tespit edilmesinde; millî güç unsurlarının imkân ve kabiliyetleri, tarihi geçmiş, jeopolitik, millî menfaatler, haklar, değerler etkin faktörler olarak dikkate alınabilir. Değişen küresel veya bölgesel konjonktür çerçevesinde etki ve ilgi alanlarının değiştirilmesi gündeme gelebilecektir. Yine bu da strateji uzmanının veya karar vericilerin stratejik düşünme kabiliyetlerinin bir parçası olarak görülebilir.

Bölgesel değerlendirmede, en önemli konulardan birisi bölgesel aktörlerin sınıflandırılmasının ve hangi aktörün daha etkin olduğunun ve küresel veya bölge dışı aktörler ile olan ilgisinin dikkate alınmasıdır. Bölgesel anlamda tarihi süreçten ve anlaşmalardan kaynaklanan haklar daha ön plana çıkabilecektir. Bölgesel olaylara tepki süresi oldukça düşük olduğu için barış zamanından itibaren söz konusu aktörlerin başlangıç analizlerinin hazır olması uygun olacaktır.

1.5.4.3.1.8.Ülke İçi Durumun Analizi

Küresel, bölgesel ve ülke içi durum birbiri ile bağlantılı olarak bütüncül bir şekilde incelenmelidir. Ülke içerisindeki başta terör örgütleri olmak üzere değişik aktörlerin, unsurların tehdit durumu incelenirken; devletin millî güç analizinin de yapılması gerekmektedir. Bu maksatla millî güç unsurlarının durumları, diğer stratejik olaylara angajman durumları gibi stratejinin tasarlanmasına yönelik iç dinamikler dikkate alınarak analiz yapılmalıdır. Özellikle millî güç unsurlarından silahlı kuvvetlerin durumu, politik durum, ekonomik durum gibi hususlar dikkatlice değerlendirilmelidir. Millî kültür bu analizde ayrı bir öneme sahiptir. Bu anlamda bazı milletler insan kaybına tahammül edemezken, bazı ülkeler bekâlarının sağlanması çerçevesinde insan kaybına millî bilinç sayesinde göğüs gerebilirler. Yine karar vericilerin değişik

kararlar alırken kamuoyunun görüşünün de dikkate alınması, önemli konuların kamuoyunda tartışılması faydalı olabilecektir.

1.5.4.3.1.9. Tahditler

Tahditler stratejik tasarım sürecinin hareket kabiliyetini sınırlandıran somut ve somut olmayan faktörlerdir. Bu çerçevede kısıtlamalar belirli stratejik hedeflere ulaşılmasında tasarımcıların seçeneklerini sınırlandırabilirler. Örneğin yeterli ekonomik gücün olmaması, mali kaynakların yeterli olmaması, nükleer silahların öldürücü etkisi, müttefiklerin millî menfaatleri, zaman gibi faktörler bu kısıtlamalardan bazıları olarak görülebilir. Bu kısıtlamalar ülkenin kendisinden kaynaklanan kısıtlamalar olabileceği gibi ülke dışından uluslararası konjonktürden, uluslararası hukuktan, anlaşmalardan, üyesi olunan ittifaktan veya örgütten de kaynaklanabilir. Bu nedenle özellikle hukuk danışmanlarının görüşleri önemli veriler oluşturabilir.

1.5.4.3.1.10. Sistem Analizi

Bilindiği gibi uluslararası sistem oldukça karmaşık hatta kaotik bir yapıya sahiptir. Uluslararası sistem analizi veya bir ulus-devletin/aktörün analizi; Politik, Askeri, Ekonomik, Sosyal, Bilgi, Altyapı (PAESBA) başlıkları altında yapılabilir. Bu başlıkların her biri bir alt sistemi, aktörün/devletin kendisi ise ana sistemi temsil edebilir. Yani sistemlerin sistem analizi yapılabilir.[53] Bu nedenle ulus-devletler/aktörler, hatta uluslararası ortam sistem yaklaşımı esas alınarak incelenebilir. Sistem yaklaşımı bir suç örgütünün, terör örgütünün veya bir şirketin analizi için de kullanılabilir.

Sistem: Birbiri ile fonksiyonel, davranışsal ve fiziksel olarak ilişkilendirilen elemanlardan oluşan bir bütündür. Başta insan olmak üzere dünyamızdaki birçok yapı veya olay sistem olarak ele alınabilir.

Sistem teorisi: Sistemin yapısından kaynaklanan özellikleri ve davranışları incelemeyi hedefler. Genel olarak fiziksel sistemler için geçerli olmasına rağmen sosyal sistemlere de uyarlanabilir. Bilindiği gibi dünya da bir sistem olarak

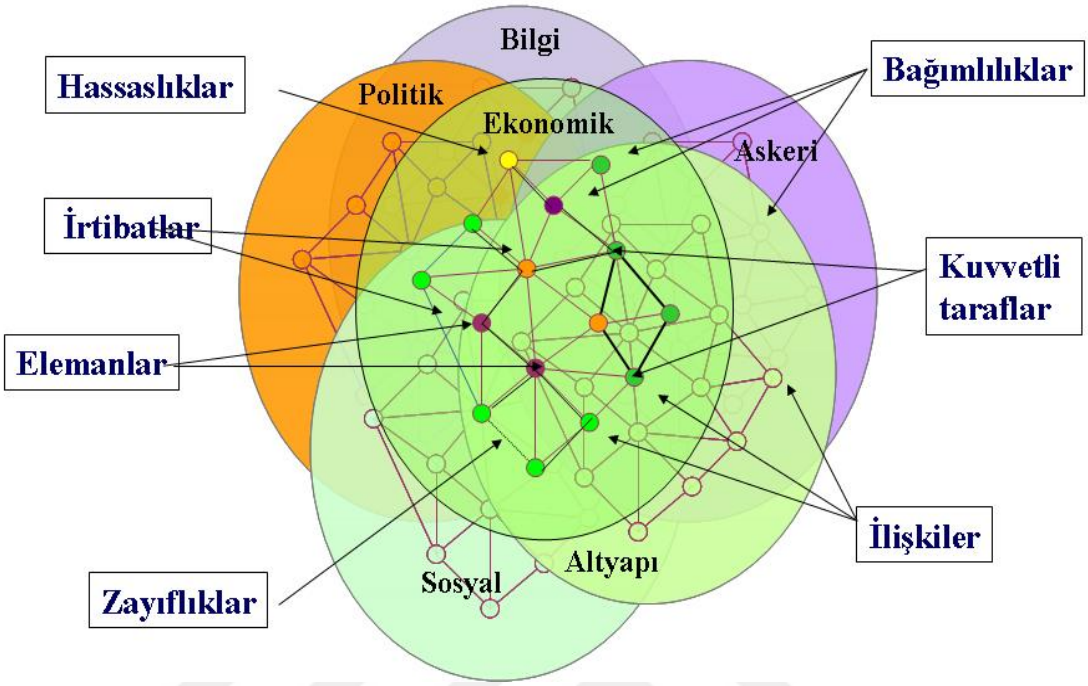
[53]Planner's Handbook for Operational Design, 2011, s IV-6

düşünülebilir. Sistem teorisinde sistemin yapısı ve çalışma mantığı üzerinde durulur. Sistemin yapısı sistemin elemanlarının birbirlerine göre konumları ve aralarındaki ilişki anlamındadır. Sistemin çalışması ise sistemin fonksiyonları neticesinde ortaya çıkan sonuçtur.

Sistem analizi ise, düşmanın, rakibin, içerisinde bulunulan ortamın, tarafsızın, dost unsurların; karmaşık, kendini değişik durumlara uyarlayabilen bir sistem olarak incelenmesi ve bu sistemin yapısının, davranışlarının tanımlanması, kuvvetli, hassas tarafları ile elemanları arasındaki ilişkinin belirlenmesi demektir. Sistemin bu şekilde analiz edilmesinin ana sebebi; sistemin özelliklerinin ortaya konulmasını müteakip, stratejik düşünme sistemi çerçevesinde millî güç unsurları kullanılarak, sistemin yapısının ve fonksiyonlarının millî menfaatler doğrultusunda şekillendirilebilmesi, yönlendirilmesidir.

Sistem analizi; sistemi oluşturan kritik aktörlerin davranışları, imkân ve kabiliyetleri, birbirleri ile olan etkileşimleri hakkında belirlenen amaca uygun olarak kullanılabilecek faydalı bilgi yaratılmasına yönelik sürekli bir faaliyettir.

Şekil 1.4: Sistem Analizi



Kaynak: Joint Staff, Planner's Handbook for Operational Design, 2011, s IV-6.

Sistem analizinde önce herhangi bir konu veya dünyanın bir bölgesine yönelik veri toplanarak durumsal farkındalık geliştirilir. Veriler bilgi haline dönüştürülerek sistem oluşturulur. Oluşturulan sistem modelinin etkilere tepkileri ölçülür. Burada üzerinde durulması gereken önemli konulardan birisi faydalı bilgi ile ham veri arasındaki farktır. Değerlendirilmiş bilgi hedefe veya amaca yönelik olarak elde edilen verilerin yorumlanması anlamındadır. Sistem elemanlarının birbirleri arasındaki ilişkileri, zayıflıklar, hassaslıklar, kuvvetli taraflar gibi yorumlar faydalı bilgi olarak kullanılmaktadır.

Sistem analizinin en önemli sonuçlarından birisi ağırlık merkezidir. Ağırlık merkezi sistemin gücünü aldığı bir imkân kabiliyet, millî güç unsuru, herhangi bir düğüm noktası olabilir. Ağırlık merkezinin tespit edilmesi söz konusu sistemin millî menfaatler doğrultusunda tespit edilen nihai hedef doğrultusunda aktörün faaliyetlerinin ekonomik ve etkin yönlendirmeler ile şekillendirilmesini sağlar.

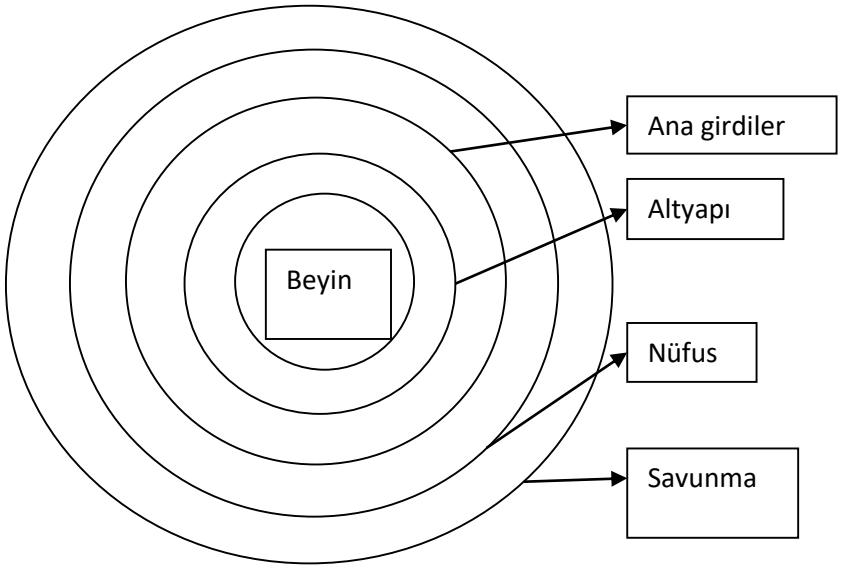
Genellikle verilecek karar hedefler ile nihai olarak etki altına alınmaya çalışılabilir. Ancak sistem analizi yönteminin kullanılması ve sürdürülmesi oldukça zordur.

1.5.4.3.1.11. Beş Halka Metodu

Sistem analiz metotlarından diğer biri de Beş Halka Metodudur.[54] Bu metot John A. Warden tarafından 1995 yılında ortaya atılmış bir uygulamadır. Söz konusu metot daha ziyade Ağırlık Merkezi tespitinde de kullanılabilir. Bunun yanında herhangi bir sistemin veya organizasyonun analizi için de kullanılabilir.

Bu yöntemde, insan vücudu gibi her sistemin beş ana fonksiyonu olduğu kabul edilir. Bunlar yönetim (beyin), sistemin ana girdileri (oksijen), altyapı (damarlar), nüfus (hücreler), savunmadır (savunma mekanizması).[55] Bu yöntem kullanılarak terörist organizasyonlar, devletler gibi karmaşık sistemler modellenebilir. Bunların alt sistemleri de aynı şekilde modellenebilir. Bu şekilde sistemin modellenmesi karmaşık sistemlerin daha anlaşılır ve basit olmasını sağlayabilecektir.

Şekil 1.5: Beş Halka Metodu



[54]Finney K. Nathan, *On Strategy: A Primer*, 2020, s 79
[55]Chappel, George G, *A Terrorist Organization as a System: Unleashing Warden's Five-Ring Model,* 2002, s.4

1.5.4.3.1.12. Faktör Analizi Metodu

Stratejist durum analizi yaparken önemli veya stratejik tasarıma ışık tutabilecek faktörleri ortaya koyabilmelidir. Günümüzde strateji uzmanlarının karşılaşabileceği en önemli sorunlardan birisi oldukça fazla bilgi bombardımanına maruz kalmaktır. Bu kadar fazla bilgi bombardımanına maruz kalan uzman ehem ile mühimi ayırt etmekte, bilgileri stratejik seviyede tespit etmekte, gelecekte oluşabilecek senaryoları tahmin etmekte zorlanacaktır. Uzmanlar strateji olarak birçok kelimeden oluşan metinler ortaya koyabilecek, ancak tanımlanan problemin çözümü için etkin bir yapı oluşturamayacaktır.

Bu çalışmada faktör analizinin Tablo 1.1'deki düşünme sistemi kullanılarak yapılması önerilmektedir. Faktör analizi yapabilmek maksadıyla Tablo1.1'in birinci sütununda belirtildiği gibi öncelikle bir stratejik çerçeve çizilmeli veya mevcut stratejik çerçeve hatırlatılmalıdır. Bu çerçeve dikkate alınarak stratejinin tasarımına veya yönetimine etki olabilecek olay, eğilim, değerlendirme ikinci sütunda olduğu gibi tespit edilmelidir. Tespit edilen stratejik faktörün stratejinin tasarımına etkisi, önemi ortaya konulabilir. Son sütunda ise stratejik faktörün olumsuz etkisinin ortadan kaldırılması veya olumlu etkisinden faydalanılması maksadıyla yapılacak işlem ifade edilebilir.

Tablo 1.1: Faktör Analizi

Stratejik Çerçeve	**Stratejik Faktör** (Stratejiye etkisi olabilecek olay analizi/eğilim)	**Çıkarım** (Bu faktörün önemi nedir?)	**Sonuç** (Ne tedbir alınması gerekir ?)
Stratejik Tasarımın Amacı Suriye stratejisi tasarlamak (Bölgesel strateji) Millî Menfaat, Hak, Değer Göçün engellenmesi Tehdit/Fırsat Suriye iç savaşı nedeniyle göç tehdidi	Sığınmacı sayısının artması	İç güvenliğin olumsuz etkilenebileceği	Hudut emniyeti için kritik yerlerin tespiti, ilave tedbir alınması

Kaynak: Yazar tarafından oluşturulmuştur.

1.5.4.3.1.13.Güçlü Zayıf Tehdit Fırsat (GZTF) Analizi

GZTF (SWOT: Strength, Weakness, Opportunity, Threat) analizi herhangi bir aktörün genellikle statik analizi yapılırken kullanılabilir. Bu çerçevede; Güçlü, Zayıf taraflar aktörün yapısını (İç değerlendirme) ilgilendirirken, Tehdit ve Fırsatlar dışarıdan söz konusu aktöre olabilecek etkileri (Dış değerlendirme) ortaya koymada faydalanılabilir. GZTF'nin sonuçları kullanılarak; Tehdit-Fırsat-Zayıf-Güçlü (TFZG) analizi (TOWS: Threat, Opportunity, Weakness, Strength) yapılabilir. Bu yöntemde her bir başlık diğer başlıklar ile beraber analiz edilerek tedbir alınabilir veya stratejik hamleler yapılabilir. Bu sayede GZTF'den statik anlamda elde edilen verilerin analiz edilerek tedbir alınması sağlanabilir. Bu analizin amaçlarından bazıları: Tehdit seviyesini düşürmek, fırsatlardan faydalanabilmek, güçlü taraflardan istifade edebilmek, zayıf tarafları ortadan kaldırmak olarak özetlenebilir. Bu analizde; potansiyel fırsatlardan güçlü taraflarınızla istifade edebilir veya tehditleri ortadan kaldırabilirsiniz. Ayrıca

fırsatlardan istifade ederek zayıf taraflarınızı ortadan kaldırabilir veya koruyabilirsiniz. Ancak TFZG analizi stratejik durum analizi yapılarak sürekli gözden geçirilmesi gerekmektedir.

1.5.4.3.1.14. Bilgi Hiyerarşisi

Bilgi hiyerarşisi; ham veri, bilgi, değerlendirilmiş (faydalı) bilgi, anlama, erdem (raw data, information, knowledge, understanding, wisdom) olarak ifade edilmektedir[56]. Ham veri, elde edilen bütün işlenmemiş, gerçekler, olgulardır. Bu gerçeklerin format veya rapor haline getirilmesi ile bilgi haline gelmesi sağlanabilecektir. Aynı zamanda ham verinin değişik kaynaklardan teyit edilmesi uygun olacaktır. Bilginin amaca göre karar vericinin karar vermesine yardımcı olacak şekilde işlenmesi değerlendirilmiş veri elde edilmesini sağlayacaktır. Gelecekteki muhtemel olayların tahmin edilmesini sağlayacak şekilde analizlerin yapılması, örtük bilgi kullanılarak geleceğin tahmin edilmesi ve içgüdüsel olarak gelecekte meydana gelebilecek olayların tahmin edilebilmesi karşımıza erdem olarak çıkabilecektir.

Örnek vermek gerekirse Suriye konusunda bir çalışma yapılacaksa, Suriye'nin yüz ölçümü, nüfusu, etnik yapısı, dili, yönetim şekli gibi veriler ham verilerdir. Bu bilgilerin bir formata veya harita üzerine yerleştirilmesi ham verinin bilgi haline gelmesini sağlayacaktır. Bu bilginin Suriye'deki durumun güvenlik durumu çerçevesinde analiz edilmesi, incelenmesi değerlendirilmiş (faydalı) bilginin elde edilmesi anlamına gelecektir. Bu veri alt yapısı ile Suriye'nin gelecekte alacağı şeklin, atılacak adımların tahmin edilmesi ise erdem olarak kabul edilebilir.

Stratejik durum analizi kapsamında önce ham veriler elde edilir. Raporlar, haritalar veya tablolar gibi bir formata yerleştirilerek bilgi haline getirilir. Bilgi haline getirilmesi "ne" sorusuna cevap verir. Analiz edilerek stratejinin amacına yönelik kullanışlı hale getirilebilir. Analiz ile "nasıl" sorusuna cevap verilir. Rakibin davranışlarının özellikleri bilindiğinden dolayı yapacağı hamleler tahmin edilebilir ve önceden tedbir alınabilir veya stratejik durum şekillendirilebilir. Anlamak, öğrenme ve adapte olmayı kolaylaştıracak şekilde sistemin, yapının ortaya konulması olarak görülebilir. Bu aynı zamanda bilgi üretiminin verimliliğini artırabilecektir. Son aşamada "niçin" sorusuna cevap verilir. Bu safhada ise artık "en iyi kararın verilmesi"

[56] Ackoff, Russell, *From data to wisdom*, 1989

söz konusudur. Bu çerçevede son safha hariç diğerleri yapılan faaliyetlerin doğru yapılıp yapılmadığı ile ilgilenirken son safha doğru şeyin yapılmasına karar verilmesidir.

1.5.4.3.1.15. Stratejik Durum Analizi Özeti

Stratejik durum analizinin iyi yapılması tasarımın başarısını direkt etkileyen, oldukça karmaşık, ancak önemli bir safhadır. Bu nedenle buraya kadar açıklanan hususların özetlenmesi uygun olacaktır. Stratejist boş bir kâğıtla başladığı tasarım çalışmasında birçok hususu bu safhada şekillendirebilecektir. Tehdit, fırsatlar, faraziyeler, aktörlerin tutumları gibi tasarımın müteakip safhalarında ve icra esnasında ihtiyaç duyulabilecek, stratejinin mantığının oluşmasını sağlayabilecek birçok husus bu safhada belirlenebilecektir. Bunu yaparken de sistem yaklaşımı, beş halka metodu, faktör analizi, GZTF gibi tekniklerden yararlanabilir. Hangi tekniğin ne zaman kullanılabileceğine yine stratejist tarafından karar verilmesi gerekmektedir. Millî menfaat, hak, değer bağlamında tasarımın temel taşlarını oluşturacak stratejik faktörlerin ve bu faktörlerin etkilerinin tespit edilmesi stratejik tasarımın temelini oluşturmaktadır. Bu safhadaki en önemli hususlardan birisi, Clausewitz'in 1832'de yayımlanan "Savaş Üzerine" adlı eserinde "coup d'œil" olarak ifade ettiği komutanın/liderin bir bakışta stratejik durumu anlaması, faktörleri belirlemesi ve gerekli tedbirleri düşünebilmesi olarak tanımlanan kabiliyeti stratejislerin kazanması hayati önemi haizdir[57]. Yapılabilecek en önemli hatalardan birisi gereksiz, ortaya konulan güvenlik stratejisi amacına yönelik olmayan bilgilere yer verilmesidir. Bu amaçlanan konuya karar vericilerin odaklanmasını ve hatta bazen yanlış karar vermesine neden olabilecektir.

1.5.4.3.2.Nihai Stratejik Hedefin Tanımlanması

Nihai hedef, stratejik tasarımın uygulanması neticesinde elde edilmesi düşünülen nihai durum olarak açıklanabilir. Nihai hedefin tanımlanması, millî güç unsurlarının ortaya konulacak konseptle stratejik tasarımın başarıya ulaşmasını sağlayacak önemli adımlardan birisidir. Strateji mevcut durum ile arzulanan durum arasında bir köprü

[57]Clausewitz, carl von, *On War*, 1976, s.106

olarak görüldüğünde nihai hedeften geriye doğru mevcut duruma kadar tasarlamanın yapılması nispeten daha kolay olacaktır. Bu çerçevede nihai hedeften önceki adımların ortaya konulması, mevcut durumdan yola çıkarak müteakip adımların ortaya konulmasından daha gerçekçi ve daha kolay değerlendirmelerin yapılmasını sağlayabilecektir.

Güvenlik stratejisi tasarımında ne yapılacağı, nasıl yapılacağından çok daha önemlidir. Ne yapılacağı istenen amaca uygun olarak belirlenmediği takdirde daha başlangıçta stratejinin istikameti yanlış olacak, nasıl sorusu burada daha başlangıçta önemini yitirecektir. Ne yapılacağının doğru olarak belirlenebildiği bir durumda, nasıl yapılacağı konusunda sıkıntı olsa bile düzelmek için fırsat olabilecektir. Ancak ne yapılacağı yanlış olarak belirlendiğinde düzeltme yapılması çok daha zor olabilecektir.

Nihai hedefin belirlenmesinde millî menfaatler, haklar ve değerler belirleyici bir rol oynamalıdır. Ancak millî menfaatlerin, hakların veya değerlerin direkt olarak nihai hedef olarak verilmesi yeteri kadar somut yol gösterici veri ihtiva etmeyebileceği için tasarımın başarısını olumsuz etkileyebilecektir. Bu çerçevede millî menfaatlere, haklara veya değerlere tehdit oluşturan veya oluşan fırsat nedeniyle bu hususların geliştirilmesini sağlayan somut nihai hedefe karar verilmesi tasarımın etkinliği için önem arz etmektedir. Doğal olarak nihai hedefin tespit edilmesinde başka yöntemler de kullanılabilmektedir.

Strateji tasarımcısının nihai hedefi verilen politik direktif çerçevesinde millî menfaatlerin gerçekleşmesini engelleyen tehdidin bertaraf edilmesi veya stratejik durumun millî menfaatler çerçevesinde şekillenmesinin sağlanmasıdır. Strateji tasarımcısına verilen direktif bazen yeteri kadar açık olmayabilir. Stratejistin görevi mevcut politik direktifi stratejinin amacını da göz önüne alarak belirgin nihai hedefe dönüştürebilmektir. Bunun yanında stratejik durum analizi bölümünde ortaya konulan problem tanımı da nihai hedefin belirlenebilmesine katkı sağlamalıdır. Böylece tasarım sürecinin belirgin bir hedefe odaklanması sağlanarak, tasarımın başarısı artabilecektir. Nihai hedefin iyi bir şekilde tanımlanamadığı bir stratejik tasarımın icrası esnasında başarı durumu, nihai hedefe ulaşılıp ulaşılmadığı, yapılacak değişikliklerin neler olduğunun belirlenmesi yapılamayacaktır.

Nihai hedefin ortaya konulması stratejik tasarımın sanatsal yönünü ortaya çıkartan önemli bir süreçtir. Stratejist nihai duruma karar verirken millî menfaatlerin yanında stratejik durum analizinde elde ettiği diğer stratejik faktörleri ve çıkarımları

da hesaba katmak durumundadır. Bunun yanında rakibin millî gücünün durumu, dost tarafın gücü, güç mukayesesi, uluslararası konjonktürün durumu, tarafsızlar ve diğer aktörlerin durumlarının da dikkate alınması gerekmektedir. Karar verilen nihai hedefe ulaşılması maksadıyla harcanacak kaynak, alınacak risk de göz önüne alınmalıdır. Bu ve benzeri birçok faktör dikkate alınarak verilecek kararlar çerçevesinde nihai hedefin içgüdüsel olarak belirlenmesinin konunun sanatsal yönünü ortaya koyduğu ifade edilebilir.

Tarihi süreçte genellikle üretilen stratejiler askeri ağırlıklı olduğu için nihai durumun ortaya konulması nispeten daha kolay olmaktaydı. Günümüzde ise güvenliğin hem genişliğine hem de derinliğine şekil değiştirmiş olması nihai hedefin ortaya konulmasını daha da önemli hale getirmektedir. Genişliğine, askeri boyutun yanında, ekonomik, sosyal, iç güvenlik gibi yeni boyutlar eklenmesinin yanında; derinlik olarak uluslararası sistem, devlet, birey analiz düzeylerinin eklenmesi tasarımın daha kapsamlı düşünülmesine neden olmaktadır. Bu nedenle stratejinin başarıya ulaştığını ifade edebilecek nihai hedefin yalnızca askeri değil diğer boyutlar da dikkate alınarak ortaya konulması uygun olacaktır. Ayrıca günümüzde millî güç unsurları sadece askeri boyut ile sınırlı değildir. Diğer millî güç unsurlarının da nihai hedefin elde edilmesinde kullanılacağı düşünüldüğünde nihai hedefin tasarımının daha geniş çaplı incelenmesi gerekebilecektir.

Nihai hedefin belirlenmesi neticesinde bazı istenmeyen sonuçların da ortaya çıkması muhtemeldir. Bu istenmeyen durumlar başka bir stratejik alanda millî menfaatlere zarar da verebilir. Bunun yanında sadece kendisinin değil müttefiklerinin veya müdahil olduğu ittifakın menfaatlerini de olumsuz etkileyebilir. Böyle bir durumla karşılaşıldığında kar-zarar hesabı yapılarak bir uzlaşı alanı aranabilir. Bu nedenle nihai hedefin bütüncül bir yaklaşımla bu faktörler de dikkate alınarak belirlenmesi uygun olacaktır.

Bir devletin birçok konuda güvenlik stratejileri olduğu ve bunlardan bazılarının icraatının devam ettiği dikkate alındığında; seçilen nihai hedefin icrası devam eden stratejiler ile de uyumlu olması gerekmektedir. Yine bu stratejilerin gerçekleşmesi maksadıyla tahsis edilen kaynak ve millî güç unsurlarının angajman durumları önemli bir faktör olarak karşımıza çıkabilecektir.

Nihai hedefle uyumlu olarak alt hedeflerin belirlenmesi en az nihai hedef kadar önemlidir. Her bir alt hedef konsept tasarımı aşamasında millî güç unsurlarının

gruplandırılarak odak noktası oluşturacak, nihayetinde strateji başarıya ulaşabilecektir. Bu nedenle nihai hedef ve alt hedefler millî güç unsurlarının koordineli olarak yönetilebilmesinde önemli rol oynayacaktır.

Burada nihai hedefe veya alt hedefe ulaşılmasında eldeki millî güç unsurlarının etkin kullanılmasını sağlayabilecek, stratejik durum analizinde tespit edilen ağırlık merkezlerinin dikkate alınması uygun olabilecektir. Ağırlık merkezi bir sistemin gücünü aldığı bir imkân kabiliyet, kaynak, organizasyon olabilir. Bu şekilde sistem yaklaşımı çerçevesinde stratejik ortamın millî menfaatler doğrultusunda etkin şekilde şekillendirilmesi mümkün olabilecektir.

Stratejik tasarımın elemanlarının belirli bir noktaya odaklanabilmesi için birbirleri arasında uyumlu ve bir düşünce sistematiğini takip etmesi gerekmektedir. Bu çerçevede aşağıda belirtilen düşünce sistematiği bu çalışmada önerilmektedir. Stratejik tasarımın uyumlu olması demek;

- Tehlikede olan/fırsat oluşmuş olan millî menfaat/menfaatler,
- Bu millî menfaatin korunması/geliştirilmesi için ortaya konulan politik amaç,
- Bu politik amacın gerçekleşmesi için bertaraf edilmesi gereken tehdit veya faydalanılması gereken fırsat için belirlenen hedefler,
- Belirlenen millî menfaatlerin korunması veya daha da geliştirilmesi arasındaki uyum/ilişki,
- Hedef-konsept-millî güç unsurunun uyumlu olması olarak ifade edilebilir.

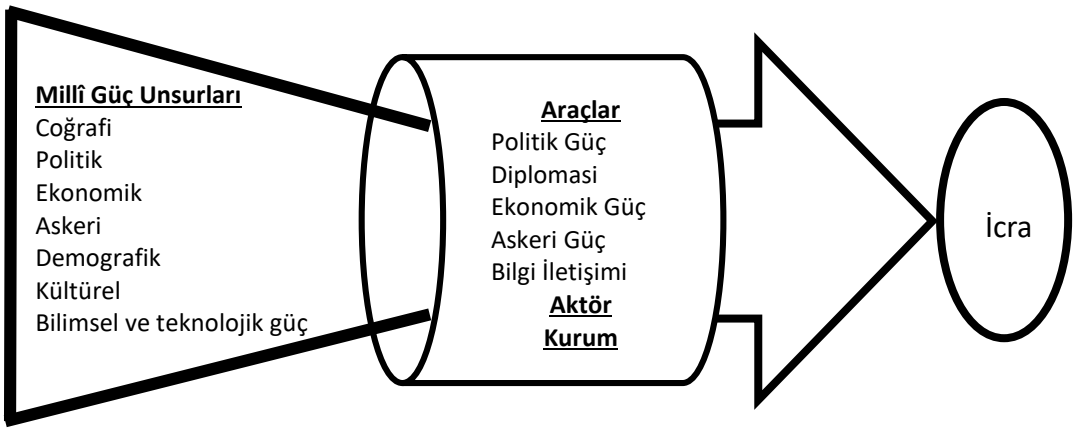
Günümüzde nihai hedefin ele geçirilmesi bazen bir safhadan diğerine geçilmesi için bir mihenk noktası veya ara hedef olarak karşımıza çıkmaktadır. Yani stratejik icraat sona ermemektedir. Buna en güzel örneklerden birisi ABD'nin Irak'ı işgal etmesidir. ABD Irak'ı işgal ederek nihai hedefe ulaştığı düşünülmüşken, direnişin başlaması yeni bir sorun kaynağı oluşturmuştur. Bunun yanında iş hayatında karşılaşılan stratejik süreçlerde hiçbir zaman süreç sonlanmamakta, nihai hedefin ele geçirilmesiyle yeni bir nihai hedefe ulaşmak için yeni bir süreç başlatılmaktadır.

1.5.4.3.3.Millî Güç Unsurları

Millî güç unsurları konusunda bir devletin millî gücünü belirleyen üzerinde anlaşmaya varılmış bir liste veya formül bulunmamaktadır. Genel olarak coğrafi, politik,

ekonomik, askeri, demografik, kültürel, bilimsel ve teknolojik güç olarak yedi başlık altında toplanabilir. Ancak bu listeye günümüzde başta sağlık alt yapısı, doğal kaynaklar (Coğrafyadan ayrı olarak değerlendirilmesi gerekebilir.) olmak üzere ilave unsurlar da eklenebilir. Burada kritik olan husus herhangi bir aktörün bu listede yer alan unsurları stratejik hedeflere ulaşılması için kullanılabilecek imkân ve kabiliyetlere dönüştürebilme kapasitesidir. Bu kapasite devlet yönetimi, idaresi olarak da adlandırılabilir. Bu anlamda devlet yönetimi gittikçe önemi artan bir güç unsuru haline gelmektedir. Millî güç unsurlarının her biri diğerleri ile irtibatlı olabilir. Bu nedenle birinin kullanımı diğerini etkileyebilir. Millî gücün seviyesi her bir olaya, duruma göre farklılık gösterebilir. Bu nedenle iyi değerlendirilmedir. Bazı millî güç unsurları aynı zamanda araç olma özelliğine de sahiptir. Yani hem güç unsuru hem de araç veya yöntem olarak kullanılabilme özelliğine sahiptir. Aracın veya yöntemin fonksiyonu; güç unsurunun etkin olarak kullanılabilmesini, yani güç haline gelmesini sağlamak olarak özetlenebilir. Müteakip maddelerde ve Şekil 1.6'da bu husus açıklanmaya çalışılmıştır.

Şekil 1.6: Millî Güç Unsurlarının İcraya Dönüştürülmesi



Kaynak: Yazar tarafından oluşturulmuştur.

Coğrafi güç: Bir ülkenin konumu, topraklarının yüzölçümü, coğrafi özellikleri, toprak yapısı, iklimi gibi hususlar coğrafyanın millî güce olan katkısını belirleyen en önemli unsurlardandır. Devletlerin coğrafi özelliklerini izledikleri politika ve güvenlik

stratejilerinin bir parçası haline getirmeleri oldukça önemli bir güç sağlamaktadır. Jeopolitika ve Jeostrateji bu çerçevede gündeme gelmektedir.

Ülkelerin coğrafi konumları izledikleri veya izleyecekleri güvenlik politikalarını belirleyen önemli bir etkendir. Örneğin ada devletleri ana kıtalardan ayrıldıklarından dolayı fiziksel emniyetlerini daha kolay sağlayabilirken, Polonya gibi güçlü devletlerin arasında kalmış olan ülkeler fiziksel emniyetlerini sağlamada zorlanmakta, güvenlik politikalarını ve stratejilerini bu çerçevede oluşturmak zorunda kalmaktadır.

Türkiye'nin iki önemli boğaza sahip olması, üç tarafının denizlerle çevrili olması, petrol ve doğal gaz ihraç eden ülkeler ile ithal eden ülkeler arasında bir konumda olması, başta Ortadoğu, Balkanlar, Kafkaslar ve Doğu Akdeniz gibi kriz bölgelerine yakın olması jeopolitik, jeostratejik açıdan oldukça önemlidir. Bu nedenle güvenlik stratejilerinin tasarlanmasında önemle dikkate alınmak zorundadır.

Günümüzde her ne kadar başta internet ve gelişmiş haberleşme imkânları olmak üzere teknolojik gelişmelerin coğrafi gücün önemini azalttığı öne sürülüyor ise de, Türkiye gibi stratejik bir konuma sahip olan ülkeler ve bölgelerin önemini devam ettirdiği kabul edilen bir gerçektir.

Politik güç (araç) : Politik (siyasi) gücün iki bölümü olabilir. Bunlar iç ve dış politik güçtür. İç politik güç; anayasal düzen ve yasalar, iktidarın şekli, devlet yapılanması, bürokratik yapı gibi hususları içerebilir. Özellikle karar verme sistemi bu çerçevede önemli bir yere sahiptir. Dış politik güç ise Dışişleri bakanlığının yapısı, personelinin uzmanlığı, yabancı ülkelerdeki teşkilatlanması, uluslararası örgütlerdeki konumu gibi hususları kapsayabilir. Dış politik güçte önemli olan uluslararası sistemi iyi okuyabilmek ve bu çerçevede millî menfaatler doğrultusunda gerekli politikaları üretebilmektir. Devletin; diplomasideki etkinliği, diğer aktörleri millî menfaatler ve hedefler doğrultusunda etkileme ve bu alandaki verimliliğidir. Uluslararası ilişkilerdeki saygınlığı ve dinamizmidir. İç politikanın sağlam bir zemine oturmuş olması dış politikanın daha etkin icra edilebilmesini sağlayabilecektir.

Politik güç, millî güç unsurlarını sevk ve idare eden, etkinliğini arttıran; aynı zamanda bütün millî güç unsurlarından etkilenen bir millî güç unsurudur. Bu çerçevede politik güç, statik konumda bulunan millî güç unsurlarına dinamik nitelik kazandırır, yani faaliyete geçirilmesini sağlar. Tanımdan da anlaşılabileceği üzere politik gücün hem millî güç unsuru hem de araç veya yöntem olarak dikkate alınması

gerekmektedir. Bu çerçevede politik güç diplomasi ve devlet yönetimi olarak iki bölümde incelenebilir.

Diplomasi(araç): Diplomasi denildiğinde bir devletin diğer bir devletle, devlet dışı aktörle veya uluslararası sistem içerisinde millî menfaatlerini gerçekleştirmeye yönelik icra ettiği faaliyetler akla gelmektedir. Bu çerçevede bir ülkenin diplomatik olarak tehdit edilmesi, yaptırım uygulanması, savaş ilan edilmesi, diğer bir ülke ile ortak millî menfaatlerin belirlenmesi, ittifak kurulması, müzakere yapılması, mevcut anlaşmaların uygulanması gibi hususları içerebilir. Yaptırım uygulanması gittikçe daha fazla kullanılan bir araç olarak karşımıza çıkmaktadır. Bu kapsamda yalnızca devletlere değil kişilere, liderlere, devlet dışı aktörlere, kuruluşlara ve şirketlere karşı da kullanılan bir araç olarak görülmektedir. Diplomasinin her ne kadar dışişleri bakanlığı tarafından yürütüldüğü genel olarak kabul görmesine rağmen, günümüzde başta askeri olmak üzere enerji, ekonomi, bilim ve teknoloji olmak üzere değişik alanlarda da diplomatik faaliyetlerin yürütüldüğü bilinmektedir. Genel olarak diplomasi kapsamında dört faaliyet icra edilebilir. Bunlar; temsil, müzakere, icra ve diplomatik baskıdır.

Temsil: Genellikle her devletin esas olarak uyguladığı diplomatik faaliyettir. Bu çerçevede; günlük ilişkilerin devam ettirilmesi, belirlenen bir tutumun savunulması, açıklanması veya deklare edilmesi ve söz konusu tutuma diğer aktörlerin desteğinin sağlanması veya en azından karşı çıkılmamasının sağlanması gibi görevler icra edilebilir. Özellikle NATO ve BM gibi örgütlerde uluslararası güvenlik ortamının takip edilmesi, tutum belirlenmesi, caydırıcılık kapsamındaki faaliyetlere katılım sağlanması diplomasinin güvenlik alanındaki önemli görevleri arasında sayılabilir.

Müzakere: Güvenliğin sağlanması, ihtilafların çözümlenmesi, menfaatlerin sağlanması maksadıyla tarafların karşılıklı olarak görüş alış verişinde bulundukları diplomatik bir süreç olarak görülmektedir. Müzakerelerin icrası da oldukça teknik, sanatsal yönü bulunan önemli bir süreçtir. Bu nedenle uzman ve deneyimli diplomatların diğer kurumlar ile koordineli olarak müzakerelere yön vermesi başarı şansını artırabilmektedir. Müzakerelerin sonuçsuz kalması neticesinde millî menfaatlerin korunması anlamında sıcak çatışmaların yaşanabileceği bir süreç gündeme gelebilmektedir.

Anlaşmaların icrası: Anlaşmalarda mutabakat sağlanmasını müteakip bazı anlaşma şartlarının yerine getirilmesi bir diplomatik görev olarak algılanabilir. Bu

çerçevede koalisyonların devam ettirilmesi, teknik yardım sağlanması, değişik ziyaret, görüşme ve toplantı faaliyetleri, uluslararası hukukun yerine getirilmesi gibi görevler olabilir. Anlaşmaların icrasında özellikle iç hukuk düzenlemeleri ile karşı tarafın söz konusu anlaşmaya uygun hareket etme seviyesi dikkate alınması gerekmektedir. Ayrıca iç hukuk açısından ülkede yapılacak bazı uygulamaların karşılıklı mutabakat ile imzalanan anlaşmalara dayandırılması gerekmektedir.

Diplomatik Baskı: Bu yöntemde hedef aktörün istenilen istikamette karar vermesini sağlamak maksadıyla uluslararası ortamda tecrit edilmesi, çok kısa zaman aralıkları ile değişik heyetler tarafından ziyaretlerin icra edilmesi, diplomatik olarak tehdit edilmesi gibi baskı yöntemleri kullanılarak hedefe ulaşmaya çalışılabilir. Diplomatik baskı; başta askeri, ekonomi olmak üzere diğer güç unsurları ile koordineli uygulanması, ittifakın diğer üyeleri ile koordineli hareket edilmesi başarı şansını artıran unsurlardır. Örnek olarak bir aktörün askeri yığınak yaparken, bununla koordineli olarak diplomatik olarak da hedef aktör ile angajmana girmesi verilebilir.

Devlet Yönetimi (araç): Politik gücün önemli bölümünü devlet idaresi oluşturmaktadır. Bu çerçevede kamu düzeninin, güvenliğinin sağlanması, devletin ekonomi, savunma, sağlık gibi bütün fonksiyonlarının uyumlu şekilde belirlenen hedeflere ulaşmasını sağlayacak şekilde idare edilmesi devletin yönetim sisteminin iyi organize edilmesine bağlıdır. İyi organize edilmiş bir devlet sistemi bütün güç unsurlarının hazırlanması ve yönetilmesi, stratejik kararların zamanında alınabilmesi için vazgeçilmezdir.

Weber tarafından 20. YY. başlarında ortaya atılan Geleneksel Kamu Yönetimi (GKY) anlayışı günümüzde dâhil olmak üzere uzun yıllar devlet bürokrasisini şekillendirmiştir. Ancak İkinci Dünya Savaşı sonrasında oluşan yeni şartlara özellikle de 1970'li yıllarda yaşanan dünya ekonomik krizi ile birlikte Keynesyen refah devleti anlayışı sorgulanmaya başlanmış, Weberyan bürokrasi ise kamu bürokrasisinin ihtiyaçlarına cevap verememeye başlamıştır. Bu nedenle Geleneksel Kamu Yönetimini çağa uygun hale getirmek maksadıyla arayışlar başlamıştır. Bu arayışlar neticesinde 1980'li yıllardan itibaren neo-liberal politikalar çerçevesinde şekillenen Yeni Kamu Yönetimi (YKY) sistemi yaklaşımı hâkim olmaya başlamıştır. Ancak dünya genelindeki pek çok ülkede yaklaşık olarak otuz yıllık bir deneme süresinin akabinde YKY sistemi de 2000'li yıllarda sorgulanmaya başlamıştır. Gündeme gelen yeni arayışlardan Neo Weberyan Devlet (NWD), Yeni Kamu Yönetişimi (YKYö),

Kamu Değer Yönetimi (KDY) ve en son olarak da Dijital Çağ Yönetişimi (DÇY) ön plana çıkmıştır. Bu yaklaşımların hepsinin güvenlik bürokrasisine ve strateji tasarımına etkilerinin olması kaçınılmazdır. DÇY ise bu yaklaşımlardan günümüzde güvenlik bürokrasisine en fazla etkisi olanıdır. Müteakip bölümlerde bu konu daha detaylı incelenecektir.[58]

Güvenlik Bürokrasinin Yapısı: Güvenlik bürokrasisi denildiğinde genel olarak akla ilk olarak millî güvenlik sistemi gelmektedir. Millî güvenlik sisteminin ana elemanları olarak; değişik kanunlar, güvenlik teşkilatları, bu teşkilatların süreçleri ve mevzuatları güvenlik stratejileri ifade edilebilir.

Özet olarak ifade etmek gerekirse genel olarak ülkelerin ilgili meclislerinden çıkarılan kanunlar veya genelgeler ile güvenlik teşkillerinin meşruiyetleri, görev tanımları ve teşkilatları ortaya konulmaktadır. Çizilen bu çerçevede güvenlik kurumları kendi teşkillerini ve süreçlerini oluşturabilmektedirler.

Millî güvenlik iç ve dış güvenlik olarak ikiye ayrılmaktadır. İç güvenlik ile milletin, toplumun ve bireyin emniyeti, asayişi, huzuru, güvenliği sağlanırken; dış güvenlik ile dışarıdan gelen tehditlere karşı yine milletin, toplumun ve bireyin güvenliğinin sağlanması esas alınmaktadır. Günümüzde iç ve dış güvenliğin özgürlük-güvenlik çerçevesinde beraber sağlanması gerekmektedir.

Türkiye'de güvenlik bürokrasisi kapsamında akla gelen kuruluşlar; Cumhurbaşkanlığı, İçişleri Bakanlığı, Millî Savunma Bakanlığı, Dışişleri Bakanlığı, Millî Güvenlik Kurulu Genel Sekreterliği, Türk Silahlı Kuvvetleri, Emniyet Teşkilatı, Jandarma Teşkilatı, Sahil Güvenlik, Millî İstihbarat Teşkilatı olarak sıralanabilir. Bu kurumlardan bazıları iç tehdit ile uğraşırken, bir kısmı da dış tehditle mücadele etmektedir.

Güvenlik teşkilatları oluşturdukları stratejiyi uygularken; güvenlik ortamını takip eder, değerlendirmeler yapar, kararlar alır, ana ast unsurlarına bu kararları iletirler. Ast unsurların uyum içerisinde, belirlenen stratejide kendilerine düşen görevleri yapabilmeleri, yasalar çerçevesinde hareket etmeleri, tahsis edilen kaynakları verimli kullanmaları, tekrardan kaçınmaları, faaliyetlerini koordine etmeleri devlet yönetiminin hayati önemi haiz unsurlarını oluşturur.

[58] Özer Akif ve İrdem İbrahim, Çıkmazların Karşısında Bürokrasi ve Ötesi, 2020

Ekonomik güç (araç): Bir ülkenin her türlü mal ve hizmet üretimi kapasitesi, ekonomik sistemi, borsasının işlem hacmi, ihracat kapasitesi, uluslararası ekonomik ilişkileri gibi hususları kapsayabilir. Bu çerçevede toplam ve kişi başına düşen millî gelir, büyüme hızı, satın alma gücü, kredi notu, parasının değeri gibi parametreler kullanılarak diğer elemanlara göre daha rahat ölçülebilir parametreler elde edilebilir.

Ekonomik güç, çağımızda diğer millî güç unsurlarına göre daha etkin sonuçlar üretebilmekte ve bir devletin millî gücünün büyüklüğü konusunda belirleyici bir niteliklerin başında gelmektedir. Küresel aktör ve bölgesel aktör gibi kavramlar, ülkelerin sahip oldukları ekonomik güçle yakından ilgilidir. Hemen belirtmek gerekir ki ekonomik gücü çok fazla olan ancak millî güç olarak yeterli kapasitesi olmayan ülkeler de bulunmaktadır. Özellikle Ortadoğu'da bu çerçevede ülkeler tespit edilebilir. Bunun yanında günümüzde, artık güvenliğin sağlamasında bir toplumun ve ülkenin ekonomik refahı direkt ilişkilidir. Bu çerçevede birçok millî güvenlik stratejisinde millî hedeflerden birisi veya nihai hedef olarak ekonomik refahın sağlanması verilmektedir. Aslında birçok mücadelenin veya savaşın nedeni de ekonomiktir. Birinci ve İkinci Dünya savaşlarının asıl nedenlerinden birisinin, bilindiği gibi hammadde kaynakları, yani ekonomik gücün geliştirilmesi olduğu bilinmektedir.

Silahların öldürücülüğünün artması, devletlerin karşılıklı ekonomik bağlılıklarının artması, vatandaşların refah seviyesinin artması sonucunda ekonomik araç daha da önem kazanmıştır. Hatta en önemli araçlardan birisi haline gelmiştir. Diplomasi, hammadde kontrolü gibi diğer konseptler ile birlikte kullanıldığında daha da etkin hale geldiği ifade edilebilir. Ekonomik araç kullanılarak hedef aktörün ekonomik kapasitesinin artırılması veya olumsuz etkilenmesi amaçlanabilir. Günümüzde ekonomik yaptırımlar gibi yöntemler ile karar vericilerin etki altına alınması gibi hususlar da gündeme gelmektedir. Bu maksatla beş faaliyet icra edilebilir: Ticaret, finans, hammadde kontrolü, yaptırım ve yardım.

Ticaret: Ticaretin artırılması veya azaltılmasıyla hedef aktörün refah seviyesi kontrol altına alınabilir. Hatta ekonomik bağımlılığı artırılabilir. Diplomasiyle koordineli olarak gümrük tarifelerinin artırılması veya azaltılması günümüzde önemli bir yöntem olarak karşımıza çıkmaktadır. Bu çerçevede aktörler arası ticaret savaşları günlük hayatın bir parçası haline gelmiştir. Özellikle başta sosyal medya şirketleri olmak üzere uluslararası şirketlerin faaliyetleri bu çerçevede önemli bir yer

oluşturmaktadır. Bu nedenle aktörler bu şirketlerin ticaret savaşlarının etkilerini iyi değerlendirmelidirler.

Finans: Finansal marketlerin kontrol edilmesi, para piyasalarının yönlendirilmesi, kontrol altında tutulması, faiz artırımı direkt olarak devletlerin ekonomilerine etki etmektedir. Bu çerçevede "Bretton Woods sisteminin"[59] başta ABD olmak üzere küresel aktörler tarafından kontrol edilmesinin önemli sonuçları olmaktadır. Ayrıca devletlerin merkez bankalarının döviz rezervleri finansal kapasiteyi belirleyici önemli bir faktördür.

Hammadde Kontrolü: Hammaddenin önemli bir sanayi girdisi olduğu ve bir ülkenin ekonomik gücünü önemli ölçüde etkilediği bilinmektedir. Başta petrol olmak üzere değişik yeraltı zenginliklerinin kontrolü bir ülkenin ekonomisini üretim maliyetleri açısından etkileyebilecektir. Bu maksatla bir ülkenin önemli miktarda hammadde kaynaklarına sahip olması ekonomisini etkilerken, dünyanın değişik bölgelerindeki hammadde yataklarının diğer aktörler tarafından kullanılmasının engellenmesi ekonomik gücün ve dolayısı ile başta halkın refahı ve askeri imkân ve kabiliyetlerin geliştirilmesi olmak üzere birçok millî güç unsurunu etkileyebilecektir. Türkiye gibi dışarıdan petrol ihraç etmek durumunda olan devletler için hammadde oldukça önemli bir güç unsurudur.

Ekonomik Yaptırım: Özelikle küresel ekonomiye ve piyasalara hâkim güçler tarafından bir devlete, şahsa, devlet dışı aktöre yaptırım, ambargo uygulanması önemli sonuçlar ortaya çıkarmaktadır. Örneğin İran'a yıllardır uygulanan ekonomik yaptırımlar ve ambargolar halkın yaşamını olumsuz etkilemenin yanında devlet olarak millî gücün zayıflamasına neden olmaktadır. Yaptırımların şahıslar esas alınarak yapılması ise şahısların mal varlıkları ve hareket kabiliyetini etkileyerek verilecek kararları etkilemektedir.

Ekonomik Yardım: Belirli bir aktöre ekonomisini geliştirecek şekilde mali olarak, malzeme, hammadde veya hizmet olarak yardım etmek millî menfaatlerin gerçekleşmesinde önemli bir faktör olabilir. Bu yöntem sayesinde söz konusu aktörün ekonomik faaliyetlerinin veya sanayi üretiminin bağımlı hale getirilmesi de mümkün olabilmektedir. Bugün ABD tarafından başta Tayvan, Bangladeş gibi ülkelerin

[59] Bretton Woods sistemi: İkinci Dünya Savaşı sonrasında Amerika Birleşik Devletleri tarafından geliştirilen "Uluslararası Para Anlaşması" ile uluslararası ödemelerde kullanılan bir sistemdir.

mallarının iç piyasalarına ithalatına müsaade edilmesi önemli bir ekonomik yardım olarak görülebilir.

Askeri güç (araç) : Bir devletin savaşma gücünün yanında, caydırıcılık gücünü de oluşturmaktadır. Bu çerçevede askeri güç barışta caydırıcı, savaşta ise verilen politik hedefleri ele geçirme ve ülkeyi savunma kabiliyetine sahip olmalıdır. Ancak günümüzde askeri gücün yanında savunma sanayinin de güçlü bir alt yapıya sahip olması kaçınılmaz hale gelmiştir. Bir ülkenin askeri gücü değişik yöntemler kullanılarak ölçülebilmektedir. Bu maksatla genel olarak komuta yapısı, kuvvet yapısı, lojistik sistemi, ateş gücü, hava savunması, istihbarat elde etme kabiliyeti, karar verme süreçleri, deneyimi, millî değerleri, tarihteki zaferleri veya mağlubiyetleri gibi hususlar dikkate alınmaktadır.

Askeri araç; kuvvet kullanma tehdidini, kuvvet kullanmayı veya bir aktörün askeri kapasitesinin artırılmasını içerebilir. Genellikle güvenlik stratejilerinde ilk akla gelen araçtır. Askeri araçların kullanılması nükleer silahların kullanılmasından insani yardımı içeren daha yumuşak yöntemlere kadar değişen bir spektrumu içerir. Ancak askeri yöntemlerin kullanılması gerek mali, gerekse insan kaynağı açısından oldukça pahalı bir yöntemdir. Askeri yöntemlerin kullanılmasının ekonomik kaynakları azalttığı bu nedenle genellikle askeri araçların ekonomik menfaatlerin gerçekleşmesine yönelik petrol kaynaklarının ve ticaret yollarının kontrolü gibi hedeflere yönlendirilmesine dikkat edilmelidir.

Kuvvet Kullanma Tehdidi: Günümüzde kuvvet kullanmanın yıkıcı etkileri göz önüne alındığında, sadece kuvvet kullanma tehdidinde bulunulması veya önce kuvvet kullanma tehdidi müteakiben kuvvet kullanma seçenekleri dikkate alınabilir. Bunun yanında tehdit amacıyla sınırlı harp çerçevesinde yalnızca belirli, seçilmiş hedeflere karşı kuvvet kullanılması da düşünülebilir. Başarıya ulaşmadaki en önemli etken kuvvet kullanma tehdidinde bulunan aktörün inandırıcılığı, yeterli kapasiteye sahip olması ve niyetidir. Kuvvet kullanma tehdidinin birden bire sıcak savaşa da dönüşebileceği unutulmamalıdır. Doğal olarak kuvvet kullanma tehdidinin diplomasi ile çok yakın koordinasyon içerisinde uygulanması gerekmektedir.

Kuvvet Kullanma: Bir aktörün diğer aktörü imha etmek, baskı veya kontrol altına almak maksadıyla icra ettiği faaliyetler olarak özetlenebilir. Bu faaliyetler genel olarak açık, örtülü veya gizli icra edilebilir. Günümüzde vekâlet savaşları, hibrit savaş, siber taarruzlar gibi yeni güç kullanma yöntemleri muharebe sahasında görülmeye

devam etmektedir. Kuvvet kullanma yöntemi stratejinin başarısı için önemli bir unsurdur. Amaca veya nihai hedefe göre uygun kuvvet kullanılmalı, bazen de kuvvet kullanılmaması daha etkin sonuç üretebilecektir. Özellikle iç güvenlik harekâtında kuvvet kullanarak sivillere zarar verilmesi kuvvet kullanılmamasından daha önemli sonuçlara neden olabilecektir.

Günümüzde gittikçe yaygınlaşan bir eğilimle askeri araç olarak vekâlet savaşları kullanımı artmaya devam etmektedir. Devletler hem iç kamuoyu hem uluslararası kamuoyunun olumsuz etkilerini asgariye indirebilmek maksadıyla kendi silahlı kuvvetleri yerine bölgede bulunan veya kendileri tarafından teşkilatlandırılan grupları kullanarak stratejik hedeflerini gerçekleştirmeye çalışmaktadırlar. Aslında vekâlet savaşları yeni bir askeri araç değildir. Tarihte de bazı devletler benzer yöntemlere başvurmuşlardır. Geçmişte Osmanlı İmparatorluğunun Cezayir ve Tunus'taki yerel unsurları Akdeniz'de kullanması bu çerçevede vekâlet savaşına verilen örnekler arasındadır. Günümüzde ise İran'ın Hizbullah'ı kullanması aynı çerçevede değerlendirilmektedir.

Vekâlet savaşlarının yanında Askeri Şirketler de muharebe sahasında daha sık görülmeye başlamıştır. Vekâlet savaşları için kullanılan gruplara benzer bir yöntemle özellikle ülkelerin emekli özel kuvvetler personeli tarafından organize edilen silahlı gruplar stratejik hedeflerin ele geçirilmesi için kullanılabilmektedir.

Günümüzde Hibrit savaş önemli bir askeri araç olarak karşımıza çıkmaktadır. Bu savaş yönteminde; klasik savaş yanında gayri nizamı savaş, hatta terörizm ve organize suç örgütlerinin kullanılabildiği, ihtiyaca göre siber savaş, bilgi harekâtının kullanıldığı bir askeri araç olarak karşımıza çıkmaktadır. Burada amaçlardan birisi belirsizlik yaratarak hedef ülkenin veya aktörün karar verme mekanizmasının sekteye uğratılması ve stratejik hedeflerin bu süre zarfında ele geçirilmesidir. Bu araç da geçmişte tarihte kullanılan askeri araçlar arasındadır.

Askeri Kapasitenin Artırılması: Herhangi bir aktörün kuvvet kullanma imkân ve kabiliyetinin artırılması maksadıyla eğitim, öğretim, danışmanlık, silah ve malzeme tedarik edilmesi gibi faaliyetleri kapsayabilir. Bu yöntemle söz konusu aktörün kuvvet kullanma kapasitesi artırılarak diğer aktörlere göre güç kazanması ve bölgesel bir güç dengesi oluşturulması hedeflenebileceği gibi beraber çalışılabilirliğin artırılması da hedeflenebilir. Beraber çalışılabilirlik sayesinde söz konusu aktör ile beraber harekât

icra edebilme kabiliyeti kazanılarak bölgesel veya küresel millî menfaatlerin dolaylı olarak gerçekleştirilmesi sağlanabilir.

Demografik güç: Bir ülkede yaşayan toplumun, yani milletin nitelik ve nicelik açısından değeri demografik gücü oluşturur. Bu çerçevede toplam nüfus, genç nüfus, eğitim ve öğretim düzeyi gibi hususlar bu değerlendirmenin yapılmasında önem taşımaktadır. Eğitimli ve yaratıcı insanların sayısının fazla olması bir demografik gücün en önemli parametrelerinden birisi olarak görülmektedir. Geçmişte nüfus sayısı önemli bir parametre olarak görülmekte ise de günümüzde ikinci derecede bir öneme sahiptir.

Büyük bir nüfusun, güçlü bir devlet için önemli olduğu ifade edilebilir. Ancak tek başına güçlü bir devletin göstergesi olarak alınması yanlış sonuçlara neden olabilir. Nüfus, potansiyel bir güçtür. Ancak eğitimli ve üretken nüfus ne kadar fazla olursa, devletin o kadar güçlü olduğunu söylemek doğru olacaktır. Diğer taraftan, nüfusun fazlalığı, işgücü kapsamında, gelişmişlik düzeyi bakımından eş değer veya yakın durumdaki devletlerarasında farklılık yaratabilecek bir güç göstergesi oluşturabilir.

Kültürel güç: Üyeleri aynı politik otoriteye tabi olan, ortak bir toprak parçasını işgal eden, ortak kültüre sahip ve aynı kimliği paylaşan insan grubu toplum/millet olarak adlandırılabilir. Kültürün değişik tanımları bulunmaktadır. Türk Dil Kurumu Sözlüğünde kültür, "Tarihsel, toplumsal gelişme süreci içinde yaratılan bütün maddi ve manevi değerler ile bunları yaratmada, sonraki nesillere iletmede kullanılan, insanın doğal ve toplumsal çevresine egemenliğinin ölçüsünü gösteren araçların bütünü, hars, ekin" olarak ifade edilmektedir[60]. Bir toplumun/milletin veya ülkenin tarih boyunca ortaya koyduğu ve yeni kuşaklara aktardığı, maddi ve manevi özelliklere kültür diyebiliriz. Kültür, toplumun/milletin veya ülkenin kimliğini oluşturur, onu diğer toplumlardan/milletlerden veya ülkelerden ayırır. Kısaca kültür, yaşam, düşünme ve iş yapma tarzı olarak da özetlenebilir. Sağlam ve köklü bir kültüre sahip toplumlar tarih boyunca varlıklarını muhafaza etmişlerdir.

Bilimsel ve teknolojik güç: Günümüzde gittikçe önemi artan bir millî güç unsurudur. Bir ülkenin teknoloji üretme kabiliyeti, bilimsel ve teknolojik alt yapısı başta savunma sanayi olmak üzere bütün sanayi yapısının temel unsuru haline gelmiştir. Günümüzde bilim ve teknoloji neredeyse bütün millî güç unsurlarını

[60] Türk Dil Kurumu Sözlüğü (sozluk.gov.tr), 26 Mart 2023

etkileyen, bir ülkenin gelişmişliğinin önemli bir göstergesi olarak değerlendirilmektedir. Teknolojik gelişmeler neticesinde bilgi iletişimi önemli bir stratejik iletişim aracı haline gelmiştir.

Bilgi İletişimi(araç): Bilgi iletişimi günümüzde önemi gittikçe artan, yeni teknikler ve teknolojilerle daha da etkin hale gelen bir araçtır. Bilgi iletişim aracı kapsamında hangi hususların yer aldığı birçok kaynakta farklılık içermektedir. Genel olarak kamu diplomasisi, stratejik iletişim, psikolojik hareket, siber güvenlik, istihbarat, kritik lider görüşmesi (kanaat önderi), bilgi harekâtı gibi faaliyetler bilgi iletişim aracı içerisinde değerlendirilebilir. Bu faaliyetler günümüzde iş hayatı, hükümetler, akademisyenler, askeri çevreler tarafından değişik formatta kullanılabilmektedir. Bu faaliyetler algı yönetimi, bilginin dağıtımı, analiz edilmiş bilginin kontrolü gibi konular üzerinde odaklanabilir.

Algı Yönetimi: Algı yönetimi dört safha olarak icra edilebilir. Birinci bölüm; verinin toplanması, işleme tabi tutulması, birleştirilmesi, analiz edilmesi ve yorumlanmasından oluşur. Bu faaliyet, sistemin, hedef kitlenin veya uluslararası konjonktürün anlaşılmasını sağlar. İkinci safha söz konusu hedef kitlenin davranışlarını veya tutumunu değiştirmek için gerekli mesajların üretilmesi aşamasıdır. Üçüncü safha uygun araçlarla mesajların iletilmesi ve son safha ise bu mesajların sonuçlarının ölçülmesi ve değerlendirilmesidir.

Bilgilendirme: Belirli bir kitleye bilginin iletilmesi olarak tanımlanabilir. Algı yönetimine göre daha pasif, daha gayri resmi olarak icra edilebilir. Bilgi kaynağının güvenirliği, mesaj ile kaynak arasındaki ilişki, kitlenin önyargıları, kültürü, dili, iletişim metodu ve kabiliyeti, iletişim süresi gibi hususlar amacın gerçekleşmesinde önemli parametreler olarak görülebilir.

Bilginin Kontrolü: İstenen sonucun alınabilmesi için bilginin ortadan kaldırılması, manipüle edilmesi, kısıtlanması, iletişim zamanının tespiti gibi konuları içerebilir. Bu çerçevede öncelikle hedef kitlenin içinde bulunulan durumu kavraması veya tepki göstermesi engellenirken; dost ve müzahir unsurlara karşı tarafın benzer mahiyetteki maksatlı mesajlarının engellenmesi hedeflenebilir. Aldatma faaliyetleri, siber taarruzlar bu faaliyetlerin içerisinde sayılabilir.

Kamu Diplomasisi: Günümüzde gittikçe önemi artmaktadır. Özellikle gelişen teknolojik imkânlar sayesinde hedef aktörün kamuoyunun, kanaat önderlerinin ve

aydınlarının etkilenmesi, yönlendirilmesi, hatta şekillendirilmesi mümkün hale gelmiştir.

1.5.4.3.3.1.Millî Güç Sistemi

Millî güç unsurlarının yanında bu gücün kullanılma yöntemi; yani sistemi önemlidir. Bu aynen potansiyel bir gücün kinetik güç haline getirilmesine benzetilebilir. Millî Güç Sistemi; millî güç unsuru, aktör veya kurum, araçtan oluşabilir[61]. Bu sistemde millî güç unsuru banka hesabında bulunan kaynak veya hammadde olarak algılanabilir. Bu unsurlar kullanılarak milletin refahının sağlanmasının yanında güçlü devlet kuruluşlarının oluşturulması, geliştirilmesi sağlanır. Ancak bu unsurlar sonsuz değil, sınırlıdır. Bu güç unsurlarının, hesapsızca kullanılması, zayıflaması devletin zayıflaması anlamına gelecektir. SSCB'nin çöküşü bu anlamda örnek olarak gösterilebilir. Millî güç unsuru tek başına istenilen etkiyi yaratamaz. Örneğin askeri gücünüz caydırıcılık sağlayabilir ancak istenilen etkinin üretilebilmesi için yukarıda belirtilen şekilde kullanılması gerekmektedir. Yani bir araç olmalıdır. Güç kullanım sistemi yukarıda belirtilen üç unsurun bir araya getirilmesiyle potansiyel gücün kinetik hale getirilmesini sağlayabilir. Ancak önerilen bu sistemin anlaşılması, oluşturulması ve güvenlik stratejisinin icrası anlamında idare edilmesi oldukça zordur. Daha basit yöntemler üzerinde çalışılabilir.

Güvenlik stratejilerinde kullanılabilecek araçlar genelde dört bölümde incelenmektedir. Bunlar diplomatik, ekonomik, askeri ve bilgi (DEMI; Diplomatic, Economic, Military, Information) olarak sıralanmaktadır[62]. Günümüzde bu dört araca mali, istihbarat ve kolluk gücü de eklenmiştir. Her bir araç değişik imkân ve kabiliyetlerden meydana gelmektedir. Stratejik tasarımdaki en önemli husus mevcut durum karşısında hangi imkân ve kabiliyetin en iyi sonuç verebileceğine ve nasıl kullanılabileceğine karar vermektir. Bu çerçevede; her bir aracın faydasının, kabiliyetlerinin, kısıtlamalarının, hangi konseptle veya yöntemle kullanılabileceğinin, maliyetinin ve risklerinin iyi bilinmesi gerekmektedir. Bunların yanında ilave araçlar da gündeme gelebilir.

[61]Heffington Steven, Oler Adam, Tretler David, A National Security Strategy Primer, 2019, s. 32
[62] Heffington Steven, Oler Adam, Tretler David, A National Security Strategy Primer, 2019, s. 22

Bir devletin sadece kaynaklarının veya imkân ve kabiliyetlerinin olması güçlü olduğu anlamına gelmemektedir. Bu kaynakları veya imkân ve kabiliyetleri işe veya sonuca dönüştürebilmesi için araçlara ihtiyacı bulunmaktadır. Örneğin Suudi Arabistan'ın oldukça zengin petrol kaynakları ve mali imkânları olmasına rağmen beklediği sonuçları alamamaktadır. Bunun tam tersi de doğru olabilir. Çok güçlü araçlar olabilir ancak kaynaklar yeterli olmayabilir. Bu kaynak veya imkân ve kabiliyetlerin millî menfaatler doğrultusunda kullanılabilmesi için araçların kullanılması gerekmektedir. Kaynak/imkân ve kabiliyetler ile araçların etkin kullanılabilmesi için bir sistem yani mekanizma yaratılması gerekmektedir. Bu sistem veya mekanizmanın bütününe millî güvenlik sistemi diyebiliriz.

1.5.4.3.3.2.Güvenlik Stratejisi Savunma Planlaması İlişkisi

Güvenlik stratejisi tasarımının önemli bir parçası savunma planlamasıdır. Savunma planlaması; askeri güç unsurunun mevcut görevleri icra etmeye devam ederken; millî güvenlik stratejisinde belirtilen gelecekteki muhtemel görevleri de başarıyla icra etmesi hedeflenmektedir. Soğuk savaş döneminde güvenliğin ağırlıklı olarak askeri unsurlar esas alınarak sağlandığı dikkate alındığında güvenlik stratejisi tasarımı ile savunma planlaması birbirlerini tamamlayan iki önemli süreç olarak karşımıza çıkmaktaydı. Günümüzde de benzer şekilde savunma planlaması caydırıcılığın sağlanması, krizlerin yönetilmesi, savaşın kazanılması için önemini korumaya devam etmektedir.

Askeri güç kapasitesinin savunma planlaması ile istenilen seviyeye ulaşması diğer millî güç unsurlarının geliştirilmesinden çok daha zordur. Çünkü askeri imkân ve kabiliyetler genellikle sivil piyasada bulunmayan, devlet tarafından uzun bir süreçte geliştirilmesi gereken sistemlerdir. Para olsa dahi bazen satılmayan, parası önceden ödenmiş olsa dahi teslim edilmeyen silah sistemleri savunma planlamasının öneminin ve zorluğunun ortaya konulması için yeterlidir. Diğer taraftan rakip aktörler için karşı tarafın savunma planlamasının baltalanması, kendi güvenliklerinin sağlanmasında önemli hedef olarak karşımıza çıkmaktadır. Hatta bazen dost aktörler bile savunma planlamasının gelişmesini istemeyecek, kendilerine bağımlı kalınmasını isteyebilecektir. Bu sayede gerçek millî güvenlik kaygıları değil onların güvenlik kaygıları esas alınarak güvenlik stratejisi tasarlanması ve icrası söz konusu olabilecektir. Buna ilave olarak savunma teknolojilerinin geliştirilmesi için personel

yetiştirilmesi de oldukça zordur. Neredeyse bütün aktörler savunma teknolojisi geliştirilmesi maksadıyla öğrenci yetiştirilmesini kabul etmemekte, savunma şirketlerinde yabancı personelin çalıştırılmasını engellemektedir. Bu nedenle savunma teknolojisi için verilecek eğitim de savunma planlaması ile paralel yerli ve milli olmak zorundadır. Bunun için iyi bir planlama yapılması gerekmektedir.

Savunma planlaması da güvenlik stratejisi tasarımı gibi bir süreç takip edilerek yapılmaktadır. Güvenlik stratejisi ile savunma planlamasının uyum içerisinde olması güvenliğin sağlanmasında önemli bir parametre olarak karşımıza çıkmaktadır. Bu çerçevede güvenlik stratejisi tasarımında belirlenen tehdidin bulunduğu coğrafya, tehdidin imkân kabiliyetleri gibi hususlar savunma planlamasında referans olarak alınan temel unsurlardan bazılarıdır.

Savunma planlaması ihtiyaçların tespit edilmesiyle başlamaktadır. İhtiyaçların tespit edilmesinde halen icra edilen harekâtlardan elde edilen tecrübeleri temel alan girdiler, güvenlik stratejisinde belirtilen muhtemel senaryolarda başarılı olmak için gerekli imkân ve kabiliyetler, geleceğin muharebe sahası, teknolojik gelişmeler göz önüne alınmalıdır. Askeri güç unsurunun icra ettiği harekâtlardan elde edilen deneyimler hem halen icra edilen harekâtların başarılı olabilmesi hem de gelecekte ihtiyaç duyulabilecek imkân ve kabiliyetler için çok önemli girdiler sunabilecektir. Mevcut harekâtlara ilave olarak güvenlik stratejisinde tehdit olarak belirlenen aktörler ile gelecekte girilebilecek bir mücadelenin senaryosu çerçevesinde ihtiyaç duyulabilecek imkân ve kabiliyetlerin tespit edilmesi de gerekmektedir. Bu çerçevede güvenlik stratejisinde tehdit olarak belirlenen aktörlere yönelik başta harp oyunlaması olmak üzere çeşitli yöntemler kullanılmak suretiyle üstünlük sağlanması için ihtiyaç duyulabilecek silah sistemlerinin tespit edilmesi sağlanabilmektedir. Buna ilave olarak gelecekteki muharebe sahasının alabileceği şekil tahayyül edilerek geleceğin silah sistemlerinin de belirlenmesi gerekmektedir. En son olarak da teknolojik gelişmelerin mevcut silah sistemlerine etkisinin yanında yeni silah sistemlerinin inşasına olan etkisinin ortaya konulması ve ihtiyaçların ortaya konulması gerekmektedir. İhtiyaç belirleme tehdit olarak belirlenen aktörler esas alınarak yapılabileceği gibi jenerik olarak ortaya konulan senaryolar esas alınarak da yapılabilir.

İhtiyaç belirleme işleminin sonunda mevcut sistemlere ilave sistemler temin edilmesi istenebileceği gibi mevcut olmayan yeni silah sistemlerinin imal edilmesi de istenebilecektir. Örneğin çok basit olarak belirlenen bir tehdidin etkisiz hale

getirilebilmesi maksadıyla 200 adet ilave tanka, 100 adet topçuya, 20 uçağa, 5 firkateyne ihtiyaç olduğu analiz sonucu ortaya çıkabilir. Bunun yanında muharebe sahasının gelecekte alabileceği şekil ve teknolojik gelişmeler neticesinde yepyeni bir silah sistemi ortaya konulabilir. İnsansız Hava Araçları (İHA) bunlara iyi birer örnek teşkil etmektedir. Yukarıda belirtildiği gibi bu silah sistemlerinin nasıl temin edileceği, tasarlanabileceği savunma planlamasının önemli parçalarından birisini oluşturmaktadır. Doğal olarak yalnızca silah sistemleri ihtiyaç olmayacak bu silah sistemleri ihtiyacı ile paralel personel, alt yapı gibi diğer ihtiyaçlar da gündeme gelecektir.

İhtiyaçların belirlenmesini takiben belirlenen ihtiyaçların tedarik edilebilmesi için bir plan yapılması gerekmektedir. Bu tedarik planı iki bölümden oluşabilir. Birinci bölümde mevcut harekâtlar için ihtiyaç duyulan sistemlerin tedariki, ikinci bölümde ise uzun vadeli olarak 10 yıllık, 20 yıllık bir süreçte tedarik edilecek sistemlerin planlaması yapılmalıdır. Bu planlamanın da belirli sürelerde güncellenmesi gerekmektedir.

Tedarik planı yalnızca silah sistemlerinden oluşmayacaktır. Örneğin insan kaynakları planı, mevcut sistemlerin idame planı, alt yapı inşa planı gibi belirlenen ihtiyaçların da tedarik edilebilmesi için alt programlar oluşturulması gerekmektedir. Yine bu çalışmalar ile uyumlu ihtiyaç tabanlı olarak bir araştırma geliştirme planı da yapılması gerekmektedir.

İhtiyaç belirlendikten sonra tedarik programının yapılması ve en son olarak da bütçenin yıllara sarih olarak tahsis edilmesi gerekmektedir. Bütçe tahsisinin uzun vadeli olarak yapılması projelerin uzun bir süreçte gerçekleşmesi için önemli bir etkiye sahip olacaktır. Yine bütçe tahsis programının da belirli aralıklar ile gözden geçirilmesi gerekmektedir.

Buraya kadar özet olarak incelenen savunma planlama sistemine dikkatle bakıldığında klasik strateji planlama kalıbına uymakta olduğu görülebilir. İhtiyaçlar nihai hedef, tedarik programı konsept veya yöntem, bütçeleme ise kaynaklara karşılık gelmektedir. Dolayısı ile strateji tasarım sürecinde ortaya konulan hususlardan bazıları burada da geçerlidir. Örneğin bu üç unsurun birbirleri ile uyumlu olması gibi. Yeterli kaynak olmadığı veya iyi bir tedarik programı olmadığında ihtiyaçların tedarik edilmesi, yani nihai hedefe ulaşılması gerçekleşemeyecektir.

Savunma planlaması çoğu zaman güvenlik stratejilerinin temelini oluşturmaktadır. Savunma planlaması ile tehdit veya rakip olarak belirlenen aktörlere karşı üstünlük sağlayabilecek askeri güç unsurunun geliştirilebilmesi daha başlangıçta güvenlik stratejisinin başarılı olması için önemli bir avantaj sağlayabilecektir. Askeri güç unsurunun nispi olarak üstün olması başta diplomasi gibi diğer güç unsurları için de önemli bir destek olabilecektir. Bu nedenle sadece savunma planlaması sayesinde üstün bir askeri gücün oluşturulabilmesi ve idamesini nihai hedef alan güvenlik stratejilerinin tasarlandığına da rastlanabilmektedir.

Güvenlik stratejisinde karşılaşılan bilinmeyen hususlar aynı şekilde savunma planlaması için de geçerli olacaktır. Hatta bu bilinmeyenlerin savunma planlamasına direkt etkisi de olabilecektir. Örneğin tehdit olarak belirlenen aktörün imkân ve kabiliyetleri, gelecekte benimseyebileceği hal tarzlarının tam olarak belirlenememesi ihtiyaçların da tam olarak belirlenememesine neden olabilecek, sonuç olarak savunma planlamasının başarısını olumsuz olarak etkileyebilecektir.

Savunma planlamasını ve icrasını iyi yapan bir aktör güvenlik stratejisi tasarımında önemli bir avantaj elde edebilecektir. Savunma tasarımı ile askeri güç unsuru güçlü bir konuma gelen bir aktör millî güvenlik stratejisi çerçevesinde belirlenmiş millî menfaatlerini korumak ve gerçekleştirmek için daha avantajlı bir konumda olacaktır. Hatta bazen çatışmaya ihtiyaç kalmadan amaçlarını gerçekleştirebilecektir. Ancak savunma planlaması iki ucu keskin bir kılıç gibidir. Eğer iyi bir şekilde gerçekleştirilirse güvenlik stratejisinin hedeflerine ulaşmasını sağlarken, başarısız olunması durumunda ise güvenlik stratejisinin de başarılı olma şansı olmayacaktır.

Diğer taraftan savunma planlamasının kendisi güvenlik stratejisinin önemli bir aracı veya kaynağı olarak karşımıza çıkabilir. Bu çerçevede savunma planlamasıyla elde edilen silah teknolojisinin dost ve müttefik bir ülkeye tahsis edilmesi, yüksek teknoloji içeren silahların verilmesi söz konusu ülkenin girdiği mücadelelerden galip çıkmasını sağlayacak, dolaylı olarak millî menfaatlere de hizmet edebilecektir. İyi bir savunma planlamasıyla askeri güç unsurunu ve hatta diğer bütün güç unsurlarının kapasitesini ve etkinliğini artıran aktör her zaman daha avantajlı konumda olabilecek, güçlü konumundan dolayı hata yapsa bile telafi edebilme şansı olabilecektir.

Sonuç olarak güvenlik stratejisi tasarımı yapılırken savunma planlamasının cevap aradığı soruların cevaplarının verilmesi, iyi bir savunma planlaması ile askeri

güç unsurunun güçlendirilmesi, yerli ve millî teknolojiye ağırlık verilerek savunma sanayinde bağımsızlığın kazanılması başarı için vazgeçilmezdir. Savunma planlaması diğer millî güç unsularının geliştirilmesi için de önemli bir örnek teşkil etmektedir. Savunma planlama sisteminin ilgili kuruluşlar tarafından istenen güç unsurunun geliştirilmesine uyarlanabilmesi güç unsurlarının geliştirilmesi için önemli katkılar sağlayabilecektir.

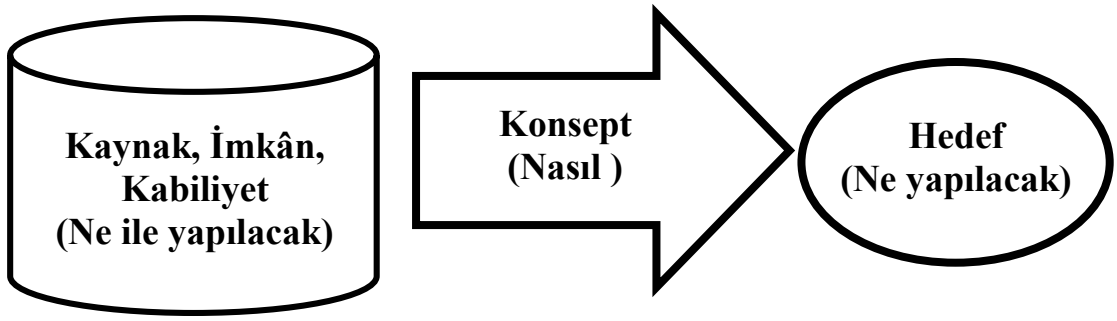
1.5.4.3.4.Stratejik Konseptin Tasarımı

Güvenlik stratejileri tasarımının en zor bölümlerinden birisi, belki de en zoru; millî menfaatler çerçevesinde, kaynak ve imkân, kabiliyetler millî güç unsurları kullanılarak bir sistem dâhilinde hedeflerin ele geçirilmesi için bir yol haritası hazırlanmasıdır. Hedefler "ne" yapılacağını, kaynaklar ve imkânlar, kabiliyetler "ne ile yapılacağını", yol haritası ise "nasıl yapılacağını" ortaya koyacaktır (Şekil 1.7). Eldeki kaynak ve imkân, kabiliyetlerin sınırlı olması bu bölümün zor olmasının temel nedenlerinden birisini oluşturmaktadır. Bu bölümün zor olmasının diğer bir nedeni ise araçların birbirlerinin etkilerini olumsuz etkilemeyecek şekilde koordine edilmesidir. Aynı aracın birden fazla hedefe angaje olması ve birden fazla kurumu/kuruluşu ilgilendirmesi zorluğu daha da artırmaktadır.

Bu nedenle önceliklendirme ve/veya sıklet merkezi yapılması önem taşımaktadır. Tasarımcının hedeflerden, araçlardan, hedeflere giden yol haritalarından hangisinin sıklet merkezini oluşturduğuna da karar vermesi gerekmektedir.

Tasarımın diğer adımlarında olduğu gibi konsept oluşturulmasında stratejik seviyenin altında kalan operatif ve taktik seviyelerde planlamanın nasıl yapılabileceği de düşünülmelidir. Hatta operatif ve taktik seviyeler de sistemin bir parçası olarak dikkate alınmalıdır. Bu maksatla ast kademeler ile planlama; sıralı, paralel veya beraber yapılabilir. Sıralı planlamada üst kademe planı yapıp ast kademeye gönderir. Ast kademe planlamasını üst kademenin planına uygun olarak yapar. Paralel planlamada kademelerin aynı anda planlama yapması söz konusudur. Günümüzde geçerli olan ise beraber planlama yapılmasıdır. Bu çerçevede kademeler arası anlayış birliği oluşabileceği gibi planlara uygun katkılar yapma imkânları olabilecek, planın stratejik seviyeden taktik seviyeye kadar uyumlu hazırlanması sağlanabilecektir.

Şekil 1.7: Stratejik Konsept Hazırlanması



Kaynak: Yazar tarafından oluşturulmuştur.

Araçların uyumlu olarak kullanılabilmesi için ilave tedbirler alınması gerekmektedir. Bu maksatla stratejist herhangi bir zaman ve mekânda stratejik tasarımda her bir güç unsuru veya araçtan ne beklendiğini iyi değerlendirmelidir. Bunun sonucu olarak bir aracın öncelikli kullanılmasına, diğer araçların destekleyen pozisyonunda olmasına karar verilebilir. Destekleyen araçların öncelikle kullanılmasına karar verilen aracı olumsuz etkilememesi için gerekli tedbirler alınmalıdır.

Araç uyumu çalışması; araçların birbirleriyle uyumlu bir şekilde kullanılması için tedbirlerin alınmasını kapsamaktadır. Millî Güvenlik Stratejisi çalışmalarında Millî Güvenlik Kurulunun tasarım ve icra aşamasında sekretarya görevi yaparak bu uyumu sağlaması yaygın olarak kullanılan bir yöntemdir. Bunun yanında koordinatör bir kurum/kuruluş veya uygun seviyedeki bir devlet görevlisi de tespit edilerek görev verilebilir. Buna ilave olarak araç uyumunun sağlanması için; önceliklendirme, safhalandırma, karar noktaları, ara hedefler, hedeflerin her birine giden yol haritaları, ağırlık merkezleri gibi kontrol tedbirleri belirlenerek uyumun sağlanması gerçekleşebilir.

Stratejinin amacına göre konsept bölümü değişik başlıklar altında hazırlanabilir. Bunlardan bazıları;

- Millî menfaatler, stratejinin esasları,
- Millî menfaatler, stratejinin esasları, nihai hedef ve alt hedefler,

- Millî menfaatler, stratejinin esasları, nihai hedef, alt hedefler ve millî güç yol haritaları,
- Millî menfaatler, stratejinin esasları, nihai hedef, alt hedefler, konsept ve stratejik hedef planı,
- Millî menfaatler, stratejinin esasları, nihai hedef, alt hedefler, stratejik niyet,
- Sistematik konsept tasarımıdır.

Yukarıda belirtilen başlıklar bu çalışmada konsept yazılması için önerilmektedir. Sıralamada aşağıya doğru gittikçe detay artmaktadır. Örneğin ilk maddede yalnızca millî menfaatlerin ve stratejinin esaslarının ortaya konulması yeterliyken; sona doğru bu iki başlığa ilave olarak nihai hedef, alt hedefler ve stratejik niyetin belirtildiği bir yazılım yapılabilir.

Millî menfaatler, stratejinin esasları:

Bu yöntemde millî menfaatlerin belirlenmiş olması stratejinin genel istikameti hakkında çok temel bilgileri vermektedir. Bunun yanında esasların veya prensiplerin ortaya konulması bu başlıklarla bağlantılı olarak temel bir konsept işlevi olarak kullanılabilir. Ancak bu esaslara dayalı daha ayrıntılı stratejilerin veya konseptlerin hazırlanması gerekmektedir. Bu esaslar yapılması gereken görevleri de içerebilir. Bu çerçevede verilen bu esaslar, prensipler veya görevler çerçevesinde fonksiyonel veya bölgesel alt stratejiler hazırlanabilir. Bu yöntem tasarımda genel istikameti verirken hazırlanabilecek alt stratejiler için esneklik sağlamaktadır.

Alt stratejilere en iyi örneklerden birisi askeri stratejiler olabilir veya uygulama dokümanları hazırlanabilir. Askeri strateji veya uygulama dokümanının amacı politik seviyede verilen direktiflerin askeri dile veya görevlere tercüme edilmesidir. Bunun sonucunda stratejinin gerçekleştirilebilmesi maksadıyla askeri güç tarafından komuta kontrol maksadıyla kullanılacak komuta yapısı, kuvvet yapısı ortaya konulabilir.

Millî menfaatler, stratejinin esasları, nihai hedef ve alt hedefler:

Bu yöntemde millî menfaatlere ve stratejinin esasları yanında tehditlerin ortadan kaldırılması veya fırsatlardan faydalanılabilmesi maksadıyla kullanılabilecek nihai

hedefler ve alt hedefler de belirtilebilir. Bu yöntem biraz daha bağlayıcı olmakla birlikte alt stratejilere biraz daha fazla yol gösterici olabilecektir. Ancak bu yöntemde de yukarıda belirtildiği şekilde alt strateji ve konseptlerin hazırlanması stratejik tasarımın başarısı için önemlidir.

Bu yöntemde nihai hedef ve alt hedeflerin ortaya konulabilmesi için millî menfaat, tehdit veya fırsat, hedef ilişkisinin kurulmuş olması gerekmektedir. Bu çerçevede tehdidin ortaya konulmuş olması ilave bir açıklık getirmiş olacaktır.

Millî menfaatler, stratejinin esasları, nihai hedef, alt hedefler ve millî güç unsurları :

Bu yöntemde millî güç unsurları, kaynaklar, imkân ve kabiliyetler ile hedeflerin nasıl buluşturulacağı veya ele geçirileceği yol haritaları esas alınılarak ortaya konulabilir. Bu yol haritaları her hedefe ulaşılacak konsepti içerisinde barındırabilir. Bir hedefe ulaşılabilmesi için birden fazla yol haritası kullanılabilir. Yol haritaları tasarlanırken zaman, mekân ve kuvvet faktörlerinin dikkate alınması etkinliği artıracaktır. Zaman faktörü; kısa, orta, uzun vadeli olarak tasarlanabileceği gibi hazırlık, icra ve sonuç olarak da planlanabilir. Yol haritaları hedeflere ulaşılmasını sağlayabilecek ağırlık merkezlerinin etki altına almasını da amaçlayabilir. Bunun yanında yol haritalarında karar vericilerin kararlarını zamanında verebilmeleri maksadıyla karar noktaları da belirlenebilir. Bu karar noktaları herhangi bir olay, kriz veya durum gerçekleşmeden yeteri kadar zaman önce karar vericilerin karar vermesini sağlayabilir. Bu maksatlar gelişmelerin yakından takip edilmesi önem taşımaktadır.

Millî menfaatler, stratejinin esasları, nihai hedef, alt hedefler, millî güç unsurları konsept ve stratejik hedef planı:

Bu yöntemde konsept ve stratejik hedef planları ayrı ayrı ele alınabilir. Genel olarak tanımlanan bir stratejik tasarımı müteakiben öncelikle bu stratejinin gerçekleşebilmesi için nasıl bir konseptle millî menfaatlerin gerçekleştirilebileceği açıklanabilir. Bu çerçevede silahlı kuvvetlerin söz konusu stratejisi esas alınarak nasıl savaşmayı düşündüğünü ifade eden müşterek harekât konsepti hazırlanabilir. Bu harekât konsepti esas alınarak eldeki silah, teçhizat ve imkân, kabiliyetler gözden geçirilerek eksik olan harekât ihtiyaçları ortaya konulabilir. Bu harekât ihtiyaçlarının yıllara sarih olarak

tedarik edilebilmesine yönelik bir tedarik planı hazırlanabilir. Bu tedarik planı hazırlanırken yalnızca mevcut harekât ihtiyaçları değil aynı zamanda muharebe sahasının gelecekte alabileceği şekil, teknolojideki muhtemel gelişmeler de dikkate alınarak bir tasarım yapılabilir. Bu planın yalnızca imkân ve kabiliyetlerin artırılmasına yönelik tedarik veya modernizasyon planı yanında; araştırma ve geliştirme, personel, idame gibi alt planları da olabilir. Bu plandan hedeflenen millî güç unsurlarından özellikle uzun vadede geliştirilmesi gerekenlerin planlı, programlı bir şekilde yıllara sarih şekilde geliştirilmesi ve tedarik edilmesidir. Bu plan Stratejik Hedef Planı (SHP) olarak adlandırılmaktadır. Bu planın bütçelenmesi için ayrı bir bütçeleme planı yapılması gerekmektedir. Bu stratejik planların birbirleriyle uyum içerisinde olması ve sürekli gözden geçirilmesi stratejik tasarımın başarıya ulaşması ve güncel kalması için önem taşımaktadır.

Millî menfaatler, stratejinin esasları, nihai hedef, alt hedefler, stratejik niyet veya direktif:

Bu yöntemdeki en kritik konu stratejik niyetin ortaya konulmasıdır. Bu çerçevede nihai hedef ve alt hedeflerin öncelikleri, ağırlık merkezleri, bu çerçevede yapılması gereken önemli görevler, stratejinin safhaları, görevlerin ve hedeflerin safhalara göre dağıtılması, stratejinin başarısını etkileyebilecek riskler, faaliyetlerde sıklet merkezinin oluşturulması, kaynakların ve imkân, kabiliyetlerin kullanılması gibi konulara yer verilebilir.

Bu yöntem stratejiyi icra edecek kurumların kendi planlarını hazırlamaları için yeterli ayrıntıyı içermelidir. Görevlerin veya faaliyetlerin zamanında ve istenen şekilde icra edildiğinin takip edilebilmesi için iyi bir raporlama sistemi kurulması uygun olabilecektir.

Sistematik Konsept Tasarım Yöntemi [63]:

Bu sistematik yaklaşım ABD Millî Savunma Üniversitesi tarafından kullanılan bir yaklaşımdır. Bu sistematik yaklaşımda dört safhalı bir konsept tasarımı yapılmaktadır. Birinci safhada stratejik bir yaklaşım seçilmesi gerekmektedir. İkinci safhada

[63]Heffington Steven, Oler Adam, Tretler David, A National Security Strategy Primer, 2019, s.37

yaklaşımın yöntemi belirlenmelidir. Üçüncü safhada ise hangi millî güç kullanım sisteminin kullanılabileceğine karar verilmelidir. Dördüncü safhada ise seçilen millî güç unsurlarının uyum içerisinde kullanılabilmesi için neler yapılması gerektiği ortaya konulmalıdır.

Stratejik yaklaşım olarak; gözlem, rakibin menfaatlerini veya amaçlarını tanıma (kabul etme), şekillendirme, ikna etme, kapasite artırımı, teşvik etme-zorlama (havuç-sopa),boyun eğdirmek, etkisiz hale getirmek şeklinde tedrici bir yaklaşım sergilenebilir. Zorlama, boyun eğdirme ve etkisiz hale getirme kuvvet kullanımı ve çatışmayı gerektirebilir.

Yaklaşımın yöntemi olarak; direkt-dolaylı, tek taraflı-çok taraflı, ardışık-gittikçe artan, gerçek-muhtemel, proaktif-reaktif, açık-örtülü faaliyetler verilmiştir.

Millî güç unsurlarının belirlenen hedeflere yönelik olarak başarıyla kullanılabilmesi maksadıyla bir kurum veya aktörün koordinatör veya sorumlu olarak belirlenmesi gerekmektedir.

En son olarak bütün parçaların birbirleriyle uyumlu olarak nasıl çalışacağı ortaya konulması gerekmektedir. Bu maksatla hedeflerin önceliklerinin verilmesi ve önem sırasına göre millî güç unsurlarının tahsisinin yapılması öngörülmektedir. Ayrıca hedeflerin ulaşılma sırası da ortaya konularak uyum artırılabilir. Millî güç unsurlarının birbirlerinin etkilerini olumsuz etkilememesi için de önlem alınmalıdır.

Özet olarak anlatılan ABD Millî Savunma Üniversitesi konsept tasarım yönteminin incelenmesi neticesinde sistemin güvenlik stratejisi tasarımında kullanılması ve stratejinin icrasında bazı problemlerle karşılaşılabileceği değerlendirilmektedir. Bu problemlerden bazıları koordinasyonun sağlanması, yeteri kadar esneklik olmaması, icranın sonuçlarının takip edilebilmesinde sorunlarla karşılaşılması gibi hususlar olarak değerlendirilebilir. Ayrıca sistemin ağırlıklı olarak dış güvenlik maksadıyla kullanılabileceği, terörizm gibi fonksiyonel veya başka stratejilerin tasarımında kullanılmasının zor olduğu sonucu çıkarılabilir.

1.5.4.3.5.Maliyet/Risklerin Değerlendirilmesi

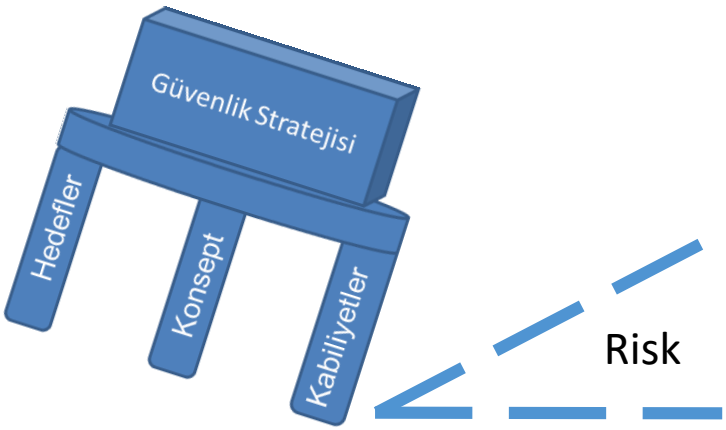
Güvenlik stratejisi maliyet/risk analizi proje yönetimi veya planların maliyet/risk analizinden çok daha farklıdır. Strateji tasarımında birçok bilinmeyen hususun bulunması, kararlar verilmesi, faraziyeler kabul edilmesi, durumun sürekli değişmesi,

rakip aktörlerin eylemlerinin sürekli dikkate alınması gerektiği hususları değerlendirme planı yapılmasını zorunlu kılmaktadır. Belirli aralıklarla yapılan değerlendirmeler, başlangıçta öngörülen hedeflere ulaşılıp ulaşılmadığının anlaşılmasını ve stratejinin güncel kalmasını sağlamaktadır. Değerlendirme süreçleri etkin olarak planlanmadığı ve icra edilmediği takdirde güvenlik stratejisi güncelliğini yitirebilecek, anlamı kalmayacaktır.

Güvenlik stratejileri tasarımındaki önemli adımlardan birisi maliyet/risk analizidir. Bu analiz tasarım safhasında yapılacağı gibi icra safhasında da yapılması gereken önemli bir işlemdir. Hatta strateji tasarlanırken icra safhasında maliyet/risk analizi yapılması gerektiği dikkate alınarak tasarımda gerekli düzenlemelerin yapılması ve buna ilave olarak bir stratejinin değerlendirme planının yapılması özellikle önemlidir.

Başlangıçta yapılacak maliyet/risk analizinde; nihai hedef/hedefler-kaynaklar/kabiliyetler-araçlar/konseptler arasında bir dengenin ve uyumun olduğu teyit edilmelidir. Bu unsurlar arasında bir uyum olmadığı takdirde risk oluşabilecektir. Böyle bir riskin oluşması güvenlik stratejisinin temelini oluşturan saç ayaklarının bir tarafa doğru dengesinin bozulmasına benzetilebilir[64](Şekil 1.8).

Şekil 1.8: Maliyet/Risk Analizi



[64] Lykke, Arthur F. Jr., Defining Military Strategy, *Military Review*, C. 69, 1989, s. 5.

Bu çerçevede değerlendirme planına esas bir model Şekil 1.7'de oluşturulmuştur. Bu modelde öncelikle doğru bir hedef seçilip seçilmediği kontrol edilmesi maksadıyla "doğru işi mi yapıyoruz" sorusu sorulmalı, müteakiben "bu işi doğru mu yapıyoruz" sorusu sorularak hazırlanan konseptin uygun olup olmadığı kontrol edilebilir. Eldeki kaynakların, kabiliyetlerin, millî güç unsurlarının yeterli olup olmadığı değerlendirilir. Her bir unsur değerlendirildikten sonra üç unsur arasında bir uyum var mı, denge bozulmuş mu kontrol edilir. ABD'nin Afganistan'ın işgalini sorgulaması ve Taliban ile barış görüşmelerine başlaması "doğru işi mi yapıyoruz" sorusunun sonucu olduğu ifade edilebilir. ABD'nin Irak'ın işgalinden sonra 2007 yılında geniş kapsamlı bir terörle mücadele konsepti yürürlüğe koymak zorunda kalması "işi doğru mu yapıyoruz" konusuna iyi bir örnek teşkil edebilir.

Değerlendirme planının en önemli kısımlarından birisi sahadan belirlenen esaslar dahilinde raporların alınmasıdır. Raporun formatı ve raporda belirtilen hususların nasıl, hangi periyodlarla analiz edileceği dikkatle planlanmalıdır.

Maliyet, stratejinin değerlendirilmesinde önemli bir yere sahiptir. Bu maliyet ekonomik, insan zayiatı, ülkenin bir kısmının zarar görmesi, hatta ülkenin işgale uğraması gibi hususları kapsayabilir. Strateji tasarlanırken bir kısım maliyetler öngörülebilir ve hesaplanabilir. Ancak bazılarının hesaplanması oldukça zordur. Stratejiyi tasarlayanların stratejinin hayata geçirilmesi konusunda karar vericilere veya liderlere maliyetler konusunda iyi bilgi vermeleri gerekmektedir. Bu şekilde karar vericilerin strateji sonucunda elde edilecek hedefler ve bu hedeflere ulaşmak için harcanacak maliyetleri mukayese etmesi sağlanabilir. Maliyetler belirlenen hedeflerin değerinden fazla ise stratejinin tasarımının tekrar gözden geçirilmesi gerekecektir. Bunun yapılmaması, göz ardı edilmesi veya ihmal edilmesinin önemli sonuçları olacaktır. Bu nedenle ülkenin millî menfaatlerinin ve haklarının iyi bir şekilde belirlenmesi, bu menfaatlerin veya hakların değerinin tespit edilmesi, bu menfaat veya haklara tehdidin belirlenmesi, tehdidin ciddiyetinin belirlenmesi önem kazanmaktadır. Tasarımcı maliyet etkinliği çerçevesinde, oluşturduğu güvenlik stratejisinin makul bir maliyetle tehdide karşı millî menfaatlerin korunmasını sağlaması veya fırsatların değerlendirmesini yapması ve karar vericilere sunması gerekmektedir. Hatta gerekirse tasarımın başında hedeflerin daha makul belirlenmesini kapsayacak şekilde tasarımda değişiklik de yapabilmelidir. Tasarımcının diğer göz önünde tutacağı önemli bir konusu ise uygulanacak strateji ile ülkenin gücünün artması, azalmamasıdır. Bu çerçevede özellikle belirlenecek hedeflerin uzun vadede ülkeye ekonomik sorun olarak

geriye dönmesi, ilave kaynak sağlamak yerine kaynaklarının azalmasına neden olması oldukça önemli bir sorun kaynağıdır. Diğer taraftan millî menfaatlerin tehdit altında olduğunun tespit edilmesi, buna karşın harekete geçilmemesi, strateji tasarlanmaması da başka bir sorun olarak karşımıza çıkacaktır.

1.6. SONUÇ

Strateji kavramının tanımı konusunda bir uzlaşı bulunmamaktadır. Genel bir tanımın olmaması, tarihi süreçte strateji kavramının sürekli değişmesi, insan beyninin genel olarak bugünü basit olarak düşünmeyi tercih etmesi, stratejinin sanatsal yönünün ağır basması strateji kavramının anlaşılmasını zorlaştıran önemli nedenler arasında sayılabilir. Bununla beraber günümüzde strateji devlet yönetimi, politika, felsefe, tarih, işletme, kamu yönetimi, spor, pazarlama, şirket yöntemi gibi birçok alanda kullanılmaktadır.

Tarihi süreçteki örneklerin incelenmesi strateji kavramının açıklanmasına yardımcı olmaktadır. Bu maksatla Thucydides, Sun Tzu, Carl von Clausewitz gibi düşünürlerin eserlerinin okunması stratejinin kavramsal boyutunun anlaşılmasına yardımcı olmaktadır. Doğal olarak tarihi süreçte tarım toplumundan sanayi toplumuna geçiş; güvenlik stratejisi tasarımını, çalışmalarını, yapısını önemli ölçüde değiştirmiştir. Aynı çerçevede günümüzde, dijital çağda güvenlik stratejisi tasarımı bir kez daha değişime uğramıştır. Müteakip bölümlerde bu konudaki incelemelere yer verilecektir.

Güvenlik stratejisi denildiğinde akla ilk gelen millî güvenlik stratejisi kavramı olmaktadır. Strateji gibi güvenliğin de tarihi süreçte değişikliğe uğraması ve genel bir tanımının olmaması güvenlik stratejisi tasarımının anlaşılabilmesini zorlaştırmaktadır. Vestfalya Anlaşmasını müteakip devletlerin uluslararası güvenlik sisteminin temel aktörü olarak daha belirgin şekilde ortaya çıkmaları ve sanayi devrimiyle gelen ulus-devlet anlayışı güvenliğin sağlanmasında millî güvenlik stratejisini temel alan yaklaşımları zorunlu hale getirmiştir. Ayrıca millî güvenlik stratejisi yapısının devlet idaresinin temel çatışını oluşturduğu ifade edilebilir. Millî güvenlik stratejisi belgesi Büyük Strateji olarak referans alınarak alt güvenlik stratejileri ve planları hazırlanması, bu çerçevede güvenlik stratejileri dokümanlarının hiyerarşik bir mantıkla tasarlanması oldukça sık karşılaşılan bir yöntemdir.

Güvenlik stratejisi tasarımında genel olarak klasik stratejisi tasarımı olarak; Arthur F. Lykke Jr tarafından ABD Kara Harp Akademisinde 1989 yılında ortaya konulan ve denklem olarak da ifade edilen yaklaşım kabul görmektedir. Strateji = Hedef + Konsept + Kaynak[65] (Güç unsuru). Bu çerçevede; durum tespiti, nihai hedefin belirlenmesi, güç unsurlarının belirlenmesi, konseptin hazırlanması, risklerin tespit edilmesi safhalarından oluşan bir süreç kullanılabilir. Söz konusu süreçte her bir safha stratejinin tasarımında değişik hususlara dikkat edilmesini gerektirmektedir.

Süreç analizi çerçevesinde durum tespitinin yapılmasında; sistem yaklaşımı, beş halka metodu, Güçlü Zayıf Tehdit Fırsat (GZTF) analizi, faktör analizi gibi yöntemler kullanılabilir. Bu safhada özellikle problem tanımının iyi yapılması, gereksiz bilgiye yer verilmemesi, stratejinin belirlenen amacına göre analizlerin yapılması önem arz etmektedir.

Nihai hedefin yani ne yapılacağının belirlenmesi sürecin diğer bütün safhalarını etkileyen bir safhadır. Nihai hedef yanlış belirlendiğinde diğer safhaların doğru icra edilmesi stratejinin başarısını etkilemeyecektir. Nihai hedefin belirlenmesinde millî menfaatlere tehdidin ortadan kaldırılmasını veya ilerletilmesini sağlayabilecek somut hedeflerin belirlenmesi esas alınmalıdır.

Millî güç unsurları nihai hedefe ulaşılmasında kullanılan kaynaklar, imkân kabiliyetler, araçlar olarak tanımlanabilir. Coğrafya, demografik yapı gibi güç unsurları kaynak olarak nitelendirilirken, bu kaynakların hedefe ulaşılabilmesi için harekete geçirilmesini sağlayan politik, askeri güç unsurları bulunmaktadır.

Millî güç unsurları kullanılarak nihai hedefe nasıl ulaşılabileceği ise konsept ile ortaya konulmaktadır. Konsept oluşturulmasında yeteri kadar yol gösterici olunmalı, müteakip aşamada hazırlanacak planların tasarımını olumsuz etkileyebilecek kısıtlamalar olmamalıdır.

Sürecin son safhasında nihai hedef, mili güç unsurları ve konsept arasında bir uyum olması kontrol edilmeli, muhtemel bir uyumsuzluk risk olarak algılanarak tedbir alınmalıdır.

Klasik strateji tasarlama süreci her ne kadar Lykke'nin makalesinde bir formül olarak ifade edilmekteyse de strateji tasarımının sabit formül ile tanımlanması uygun

[65] Lykke, Arthur F. Jr., Defining Military Strategy, *Military Review*, C. 69, S. 5, 1989.

bir hal tarzı olarak görülmemelidir. Çünkü değişik durumlar, amaçlar, konular için değişik strateji tasarım modelleri ve mantıkları kullanılabilecektir. Belirli bir durum ve amaç için kullanılan strateji tasarım modeli ve mantığı başka bir durum için geçerli olmayacaktır. Bu çerçevede tasarımın içeriği ve formatı da değişik olabilecektir. Strateji uzmanının deneyimi, bilgisi, eğitim düzeyi gibi hususlar tasarımın içeriğini etkileyen önemli parametrelerdir. Strateji tasarımında bu konu muhakkak göz önünde bulundurulmalı, sabit veya formüle dayalı bir yaklaşım benimsenmemelidir. Bununla beraber klasik strateji tasarım modeli başlangıç veya çekirdek model olarak alınabilir, içerisinde bulunulan durum ve tasarım amacı gibi faktörler dikkate alınarak uygun bir model oluşturulabilir. Nihai amaç icra edilebilir, amaçlanan hedefe ulaşılmasını sağlayan bir güvenlik strateji tasarımı gerçekleştirmektir.

İKİNCİ BÖLÜM

DİJİTAL ÇAĞIN ORTAYA ÇIKARTTIĞI ŞARTLARIN VE ETKİLERİN GÜVENLİK STRATEJİSİ TASARIMINA YANSIMALARININ İNCELENMESİ

Birinci bölümde tarım ve sanayi çağlarının güvenlik ortamlarının etkilerine yönelik değerlendirmeler yapılarak güvenlik stratejisi tasarımına etkileri ortaya konulmaya çalışılmıştır. Dijital çağ için benzer bir değerlendirme yapılması şimdilik oldukça zordur. Bunun en önemli sebebi dijital çağın etkilerinin halen yaşanmaya devam etmesi, değerlendirmeye zaman tanımayacak şekilde değişimin çok süratli gelişmesi ve netice olarak da bu konuda yeterli çalışmaların yapılamaması olarak gösterilebilir. Bu nedenle yapılacak değerlendirmelere esas teşkil edebilecek doküman sayısı oldukça azdır.

Diğer taraftan dijital çağ incelenirken yalnızca teknolojik gelişmelerin dikkate alınması, güvenlik stratejisi tasarımı çerçevesinde sağlıklı değerlendirmelerin yapılabilmesi için yeterli olmayabilecektir. Bilindiği gibi teknolojinin yanında; dijital çağda ortaya çıkan başta iklim değişikliği, doğal afetler, göç, ekonomik sorunlar, Kovit-19, nüfus artışı, Rusya - Ukrayna savaşının etkileri gibi faktörlerin çok yönlü olarak güvenlik stratejisi tasarımına önemli etkileri olmaktadır. Bu nedenle incelemenin, teknolojinin yanında bu hususlar dikkate alınarak yapılması daha sağlıklı sonuçlar verebilecektir.

Güvenlik yaklaşımlarının dijital çağda geçerliliği konusunda oldukça yeni olarak nitelendirilebilecek bazı çalışmalar yapılmaktadır. Aynı şekilde yukarıda belirtilen benzer nedenlerden dolayı bu konuda değerlendirme yapılabilmesi için yeterli kaynak bulunmamaktadır. Dijital çağın realizm, liberalizm ve inşacılık yaklaşımları üzerine etkileri konusunda bazı çalışmalar yapılmıştır[66]. Ancak yapılan çalışmaların geliştirilmesi gerektiği değerlendirilmektedir.

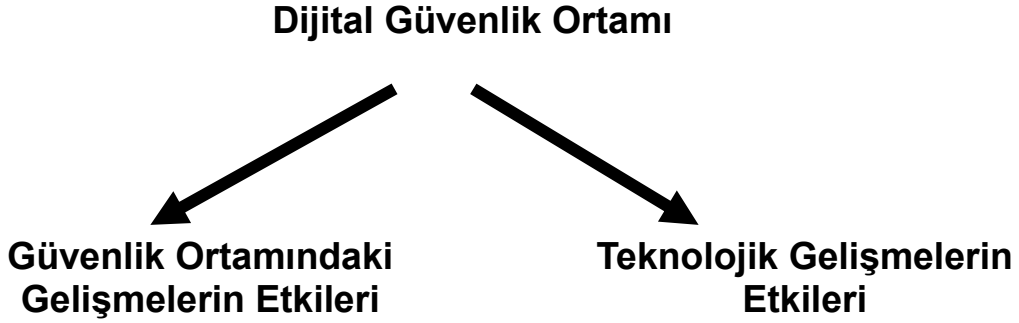
Yeterli kaynak bulunmaması konusu dikkate alınarak dijital çağ konusunda nitel çerçevede, sebep sonuç ilişkisi kullanılarak keşfedici bir yaklaşımla betimlemeler

[66]Eriksson, Johan ve Giacomello, Giampiero, *International Relations and Security in the Digital Age*, 2007, s. 32.

yapılmaya çalışılacaktır. Bu maksatla kısa bir süre olarak nitelendirilebilecek bir zaman zarfında, ağırlıklı olarak 2000'li yıllardan başlayarak günümüze kadar meydana gelen dikkate değer olaylar önce ortaya konulmaya, bu olaylardan yola çıkarak değerlendirmeler yapılarak sonuçlar çıkarılmaya çalışılacaktır. Bu olaylardan bazıları; 2004'de Facebook'un kullanılmaya başlanması, 2007'de Apple tarafından ilk Iphone'nun piyasaya sürülmesi, 2009'da Bitcoin'in kullanılmaya başlanması gibi olaylardır. Bu teknolojik gelişmelere ilave olarak önem taşıyan güvenlik olaylarından bazıları ise; ABD'deki 9/11 terör saldırısı, 2008 küresel mali kriz, 2010 Arap Ayaklanmaları, 2012 Libya'da ABD Büyükelçisinin öldürülmesi, 2016 İngiltere'nin AB'den ayrılması, 2019 Kovit-19 salgını, 2021 ABD Kongre Binasının işgali olarak sayılabilir. Teknolojik gelişmelerle birlikte bu önemli olayların oluşturduğu stratejik çerçeve, dijital çağın özelliklerinin ortaya konulması için önemli ipuçları verdiği, bu nedenle 2000'li yılların başlangıcının dijital çağın etkileri üzerinde çalışmak için başlangıç olarak alınabileceği değerlendirilmektedir.

Yeni gelişmekte olan teknolojiler olarak adlandırılan teknolojilerin gelişiminin takip edilmesinde, araştırma ve geliştirme faaliyetlerinde, geçmişteki yöntemler artık geçerli değildir. Bu teknolojiler sürekli geliştirilmekte olduğu için geçmişten farklı olarak geçmişin iyi bir şekilde değerlendirilmesinin yanında güncel gelişmelerin de değerlendirilmesine, elde edilen sonuçların araştırma geliştirme faaliyetlerinde kullanılması bir zorunluluk haline gelmiştir. Aynı yöntemde tez konusunun incelenmesi çerçevesinde faydalanılmasının uygun olacağı değerlendirilmektedir.

Şekil 2.1: Dijital Güvenlik Ortamı



Teknolojinin günümüzde güvenlik stratejileri tasarımını daha fazla etkilemesi kaçınılmazdır. Bu çerçevede dijital çağda kullanılan büyük veri, yapay zekâ, otonom

sistemler, internet gibi teknolojilerin güvenlik stratejilerine olan etkilerinin keşfedici bir şekilde analiz edilmesi dijital çağa uygun bir güvenlik stratejisi tasarımı modeli ortaya konulmasında önemli bir parametreyi teşkil etmektedir. Dolayısı ile hem güvenlik ortamındaki gelişmeler hem de teknolojik alandaki gelişmeler dijital çağ güvenlik ortamının şekillenmesinde önemli faktörler olarak karşımıza çıkmaktadır. Dijital çağ güvenlik ortamının değerlendirilebilmesi için güvenlik ortamının ve teknolojinin güvenlik ortamına etkilerinin Şekil 2.1'de belirtildiği gibi incelenmesi faydalı olacaktır.

Son 22 yılı içeren bir değerlendirme bazı normların oluşturulması, genel yaklaşımların ortaya konulması için her ne kadar yeterli olmasa dahi, dijital çağda ortaya çıkan teknolojiler ve güvenlik ortamının güvenlik stratejisi tasarımına olan etkileri konusunda mantıklı sonuçlara ulaşılmaya çalışılacaktır. Yapılan değerlendirmelerde meydana gelen olayların olgunlaşması için yeterli zaman geçmediği, yeterli belgelerin ortaya çıkmadığı her zaman göz önünde bulundurulmaktadır. Bununla beraber, başta süratli değişim olmak üzere dijital çağın özellikleri dikkate alındığında bu yöntem belki de dijital çağın bize bir zorunluluğu olarak daha sık kullanılmaya başlanılacaktır.

2.1. DİJİTAL ÇAĞDA GÜVENLİK ORTAMI DURUM TESPİTİ

Dijital çağın hemen öncesinde yer alan sanayi çağı güvenlik ortamına yönelik durum tespiti bir önceki bölümde ayrıntılı olarak yapılmıştır. Bir önceki bölümde yapılan değerlendirmeden çıkan sonuçların devamı olarak 2000'li yıllarda dijital çağın güvenlik ortamının özelliklerini anlamamıza yardımcı olabilecek önemli olaylar meydana gelmiştir. Bu olaylar ve olaylara yönelik değerlendirmeler aşağıda incelenmiştir.

Terör Saldırıları:

ABD'nin, 11 Eylül 2001 tarihinde terörist saldırıya uğraması ve akabinde Irak ve Afganistan'a müdahaleleri küresel güvenlik açısından yeni sorunlar ve endişeler ortaya çıkarmıştır. Bu ülkelerin halen istikrara kavuşamaması küresel ve bölgesel güvenlik açısından endişe yaratmaya devam etmektedir. ABD'nin 2011 yılında Irak'tan büyük oranda çekilmesi, Afganistan'dan ise Ağustos 2021 tarihinde çekilmesi önemli sonuçlara neden olmuştur. Özellikle, küresel bir güç olarak nitelendirilen bir

aktörün Afganistan'dan acele ile her hangi bir bilinçli planlama olmadan, apar topar geri çekilmesi olumsuz yorumlara neden olmuştur. Buna ilave olarak Taliban ile masaya oturulması ve diplomatik ilişkiler geliştirmesi, ulus-devletlerin yanında, devlet özelliği olmayan örgütlerin, hatta terörist olarak nitelendirilen bir örgütün muhatap alınması, uluslararası sistemin işleyişi açısından önemli soru işaretlerini akla getirmiştir.

Diğer taraftan, 11 Eylül saldırılarının yanında, Londra, Paris, Madrid, Boston, İstanbul başta olmak üzere birçok şehirde bazıları oldukça organize, bazıları ise yalnız kurt eylemleri şeklinde terör saldırıları gerçekleştirilmiştir. Bu ve benzeri saldırılar dijital çağda önemli bir tehdit olarak karşımıza çıkmaktadır.

DEAŞ'ın kuruluş ve çalışma şekli sanayi çağındaki alışıla gelmiş bir terör yöntemi değildir. DEAŞ dijital çağın sunduğu birçok teknolojik imkânı çok iyi kullanmıştır. Bu çerçevede sosyal medyada geliştirdiği yöntemler ile eleman temini konusunda önemli ilerlemeler sağlamıştır. Bu sayede başta Avrupa ve Asya olmak üzere birçok ülkeden teröristin Ortadoğu'ya gelmesini sağlayabilmiştir. Gelen teröristlerin çoğu zaman ailelerini beraber getirmeleri, yine daha önce karşılaşılmayan bir olaydır. DEAŞ internette değişik platformları kullanarak psikolojik harekât ve bilgi harekâtını başarıyla uygulayabilmiştir.[67] Hatta bu o kadar ileri gitmiştir ki iyi donatılmış Musul'daki Irak kuvvetleri, az sayıda teröristten oluşan DEAŞ karşısında dağılmıştır. Bunun sonucu olarak DEAŞ az bir kuvvetle Musul'u ele geçirmeyi başarmıştır. DEAŞ ile ilgili başka bir farklılık ise diğer terör örgütlerinden farklı olarak DEAŞ'ın toprak ele geçirmesi ve ele geçirdiği bölgelerde asayişin sağlanması, belediye hizmetlerinin yerine getirilmesi, vergi toplanması gibi bir ulus-devletin fonksiyonlarına benzer bir yapılanmaya gitmesidir.[68] DEAŞ teknolojik gelişmeleri çok iyi kullanarak başta maket uçaklar, dronlar, El Yapımı Patlayıcılar (EYP), bombalı araçlar gibi basit, piyasadan temin edilebilen malzemeler kullanılarak tasarlanabilen, kendisine özgün silah sistemleri geliştirmeyi başarmıştır. Özellikle basit yöntemler ile geliştirdiği maket uçaklar ve bombalı araçlar ile etkin sonuçlar alarak adını duyurmayı başarmıştır. Bu çerçevede DEAŞ'ın teknolojiyi iyi kullandığını gösteren bir örnek ise bombalı araçların drone kullanarak daha önce planlanan hedefe yönlendirilmesidir. Terör örgütü bu yöntemle yaklaşık 450'den fazla bombalı eylemi

[67]Aghuan, Ali, *The Cyber Dimensions of ISIS's Occupation of Mosul*, 2016.
[68]Caris, Charles & Reynolds, Middle East Security Report, *ISIS Governance in Syria*, ISW, 2014.

gerçekleştirebilmiştir. Özetle DEAŞ'ın dijital çağdaki terör örgütlerine bir örnek teşkil ettiği, önümüzdeki süreçte benzer örgütlerin ortaya çıkabileceği değerlendirilebilir.[69]

Arap Ayaklanmaları:

Arap Ayaklanması hiçbir emare vermeden, birden bire küresel anlamda önemli sonuçlara neden olacak şekilde ortaya çıkmıştır. Terör saldırılarına ilave olarak 2010 yılı sonunda başlayan Arap Ayaklanması güvenlik açısından daha da endişe verici bir durum arz etmektedir.

Tunus'ta başlayan olaylar dijital çağda krizlerin artık "stratejik şoklar" şeklinde uluslararası güvenlik ortamını önemli ölçüde etkileyebildiğini göstermiştir. Arap Ayaklanması başlangıçta geniş halk kitlelerinin demokrasi, özgürlük, ekonomik kalkınma gibi istekleri ile başlamış olmasına rağmen bir müddet sonra şiddetin hâkim olduğu, Kuzey Afrika ve Ortadoğu bölgelerinde güç boşluklarının oluştuğu bir ortama sebep olmuştur. Bu güvenlik boşluğundan başta DEAŞ olmak üzere radikal terör örgütleri faydalanmaya başlamıştır.

Arap Ayaklanması sırasında gösterilerin organize edilmesinde ve lojistiğinin sağlanmasında sosyal medyanın başarıyla kullanıldığı bilinmektedir. Bu gösterilerde aynı sloganların, afişlerin, benzer pankartların kullanılması da göstericilerin dijital teknolojileri ne kadar etkin kullandığının kanıtıdır. Bu çerçevede organize edilen gösteriler Mısır, Libya, Tunus, Suriye, Irak, Bahreyn, Yemen gibi ülkelerde önemli sonuçlara neden olmuştur. Sudi Arabistan'ın Yemen'e girmesi ise önemli sonuçlara neden olmaya devam etmektedir. Yemen'deki gelişmeler Sudi Arabistan ve Birleşik Arap Emirliği'ni tehdit etmeye devam etmektedir. Suriye'de başlayan iç savaş; değişik aktörlerin müdahalesine neden olmuştur. Ayrıca Suriye'deki gelişmeler PKK'nın önemli bir kolu olan YPG/PYD'nin oluşumuna neden olmuştur. Rusya Suriye'ye müdahale ederek Doğu Akdeniz'de önemli bir köprübaşı edinirken, İran Hizbullah ile irtibatını muhafaza ettirerek Şii hilalinin devamını sağlayabilmiştir. Bütün bu gelişmeler sosyal medyanın dijital çağda gerek ulus-devletlerin iç güvenliğinde, gerek bölgesel olarak ne gibi etkilere sebep olabileceğine yönelik önemli ipuçları vermektedir.

Arap Ayaklanmasının neden olduğu diğer önemli bir gelişme ise göç sorunudur. Arap Ayaklanması sonucunda göçmen sayısının oldukça fazla arttığı bilinmektedir.

[69] Balkan, Serkan, *DAESH Drone Strategy Technology and The Rise of Innovative Terrorism*, 2017.

Buna Afganistan'daki problemlerin ve iklim değişikliği nedeniyle ortaya çıkan sorunların eklenmesiyle göçmen sayısı daha da artmıştır ve artmaya devam edeceği yönünde kuvvetli emareler bulunmaktadır. Bu çerçevede Türkiye'de yaklaşık 3.6 milyon Suriyeli sığınmacının olduğu belirtilmektedir.[70]Sınırlarda oldukça etkin güvenlik tedbirleri alınması neticesinde göçmen akımı önemli ölçüde azalmasına rağmen, çok az sayıda olsa da devam etmektedir. Gelecekte göç etmek isteyen insan sayısının daha da artması ve göçün dijital çağda önemli bir sorun kaynağı olması beklenmektedir.

Göçmenlerin genel beklentisi Avrupa'da bir ülkeye geçmek ve iş bularak çalışmaktır. Ancak AB ülkeleri tarafından son yıllardaki göçmen akımı tarihteki kavimler göçüne benzetilmekte ve kendi iç dinamiklerini etkileyerek güvenlik sorunlarına neden olabileceği değerlendirilmektedir. AB ülkelerinde çokkültürlülük artmaya devam etmektedir. Bu nedenle AB ülkeleri tarafından oldukça kapsamlı tedbirler alınmaya devam edilmektedir.

Küresel Örgütler:

AB'nin geleceğini etkileyebilecek en önemli gelişmelerden birisi Birleşik Krallığın (BK) 2020 yılında örgütten ayrılmasıdır. BK'nın AB'den ayrılmasının güvenlik açısından en önemli sonuçlarından birisi NATO ve AB'nin güvenlik alanında işbirliğini olumsuz etkileyebilecek olmasıdır. NATO üyelerinin çoğu aynı zamanda AB üyesidir. Bu ülkelerin iki farklı savunma bütçesini yönetmesi mümkün görülmemektedir. BK'nın, ABD, Kanada, Norveç ve Türkiye gibi ülkeler ile bu işbirliğini engellemesi AB'nin Ortak Savunma ve Güvenlik Politikasını (OGSP) olumsuz etkileyebilecektir. Buna karşın bu ülkelerin AB'ye yönelmeleri ise NATO'yu olumsuz etkileyebilecektir. İlave olarak Fransa ve Almanya dengesinin AB'de bozulması hem AB'nin geleceğini olumsuz etkileyebilecek hem de Avrupa barışını olumsuz etkileyebilecektir. Bu paralelde Almanya'nın Rusya ile ilişkilerini özellikle hammadde bağlamında geliştirmeye çalışması oldukça dikkat çekicidir. Bu hususların Avrupa Güvenlik Mimarisinin bozulmuş olmasıyla beraber değerlendirilmesi oldukça olumsuz sonuçları işaret edebilecektir. En son yaşanan Rusya-Ukrayna savaşı, NATO-AB yakınlaşmasını şimdilik muhafaza edebilmiştir.

[70] Unhcr.org, *Türkiye'deki Mülteci ve Sığınmacılar*, 30 Haziran 2022.

Küresel güvenliği etkileyen uluslararası örgütlerin başında Birleşmiş Milletler Güvenlik Konseyi (BMGK), NATO, AB ve AGİT gelmektedir. BMGK İkinci Dünya Savaşından sonra barışın sağlanması maksadıyla kurulan küresel güvenlik için en önemli platformlardan birisidir. BMGK'nın en önemli özelliği herhangi bir ülkeye karşı kuvvet kullanmaya karar verebilmesidir. Ancak 5 ülkenin veto hakkının olması, bu ülkelerin veto haklarını kendi millî menfaatleri doğrultusunda kullanma eğiliminde olmaları, netice olarak birçok çatışmayı engelleyememesi; dijital çağın etkileri ile beraber dikkate alındığında BMGK'nın güvenirliği ve etkinliğinin daha da azaldığı ifade edilebilir. NATO ise, NATO-AB çekişmesi, üye sayısının oldukça fazla olması nedeniyle karar almadaki sıkıntılar, üyeleri arasındaki görüş ayrılıkları gibi konulardan dolayı etkinliğini muhafaza etmekte zorlanmaktadır. AGİT ise Rusya'nın itirazları neticesinde kuruluşunun temeli olan anlaşmaların boşa çıkması sonucu etkinliğini kaybetmiştir. Sonuç olarak dijital çağda, küresel anlamda güvenliğin sağlanması maksadıyla oluşturulmuş olan uluslararası örgütlerin etkinliğinin, kurulma amaçlarını gerçekleştirmek için yeterli olmadığı değerlendirilmektedir.

Bunun yanında Rusya'nın NATO benzeri bir anlayışla kurduğu Kolektif Güvenlik Anlaşması Örgütü (KGAÖ) en son 2022 yılının başında Kazakistan'daki olaylara müdahalesiyle bir kez daha adını duyurmuştur. Bu müdahale söz konusu örgütün kadife veya renkli devrimler olarak adlandırılan iç karışıklıklara müdahale maksadıyla kurulduğuna yönelik değerlendirmeleri kuvvetlendirmektedir. Ancak bu örgütün de etkinliğini gösteren yeterli emare bulunmamaktadır.

Neoliberal Sistem:

Dijital çağ çerçevesinde değerlendirilmesi gereken diğer önemli bir gelişme 2008 ekonomik krizidir. Bu kriz 1929 yılındaki büyük buhrandan sonra meydana gelen en büyük ekonomik kriz olarak tarihe geçmektedir. Bunun akabinde Avrupa'da, İzlanda, İrlanda ve Yunanistan'da meydana gelen borç ödeme krizleri küresel anlamda ekonomik krizin boyutlarını daha da arttırmıştır. Aslında bu gelişmeler ile diğer gelişmeler beraber değerlendirildiğinde küresel anlamda üzerinde yoğunlaşan neoliberal düzenin tehdit altında olduğunu ifade etmek yanlış olmayacaktır.

Neoliberalizim 1980'li yıllarda, 1970'li yıllarda yaşanan dünya ekonomik krizi ile birlikte Keynesyen refah devleti anlayışının sorgulanmasıyla ortaya çıkmış, 2008 yılında ortaya çıkan ekonomik kriz ile sorgulanmaya başlamıştır. Neoliberal düzende

sermayenin korunması ve teşvik edilmesi, devletlerin özel şirket mantığı ile yönetilmesi, vatandaşın müşteri gibi görülmesi anlayışı zengin ve fakir arasındaki makasın daha da açılmasına, gelir dağılımının daha da bozulmasına neden olurken işsizliğin de artmasına neden olmuştur. Bunun yanında dünya nüfusunun artması, insan ömrünün uzaması başta AB ülkeleri olmak üzere birçok ülkede olumsuzluklara neden olmuştur. Bu çerçevede bazı AB ülkelerinde emeklilik yaşının arttırılması, sağlık harcamalarının otomatikman yükselmesi önemli sıkıntılara ve halkta hoşnutsuzluğa neden olmuştur. Göçmen krizinin etkilerinin de katkısıyla birçok ülkede, yabancı düşmanlığı, aşırı sağcı ve popülist yaklaşımlar artmıştır. Bu gelişmelerin değişik güvenlik sorunlarına neden olma olasılığı gittikçe artmaktadır.

Çin'in 2001 yılından itibaren Dünya Ticaret Örgütü'ne üye olmasının, neoliberal sistemin kurucuları olan ABD ve AB ülkelerinin aleyhine işlemeye başlamasına neden olduğu ifade edilebilir. Hatta Çin neoliberal sistemi savunurken, geçmişte neoliberal geçinen bazı ülkeler neoliberal politikaların aksine hareket etmek durumunda kalmıştır. Bütün bu gelişmeler, dijital çağın getirdiği teknolojik imkânların para piyasaları ve dünya ticareti üzerindeki etkileri ile beraber değerlendirildiğinde neoliberal düzenin sonunun geldiği düşüncesinin gittikçe kabul edilmeye başladığını göstermektedir.

Hibrit Savaştan Klasik Savaşa Dönüş:

Rusya, Gürcistan (2008) ve Ukrayna'ya (2014) müdahaleleri ile NATO ve AB'nin genişlemesini durdururken önemli güvenlik sorunlarına neden olmuştur. Rusya'nın hibrit harekât stratejisi ile askeri ve askeri olmayan yöntemleri kullanması, rakip devletlerin iç istikrarını hedef alması, NATO'nun savunma stratejisini yeniden gözden geçirmesine neden olmuştur. Bunun sonucu olarak NATO'nun hibrit harekâta karşı tedbir almaya devam ederken tekrar Rusya'nın tehdit olarak algılandığı, klasik harekâtın esas alındığı, realist bir güvenlik anlayışına dönmeye çalıştığı görülmektedir. Özet olarak hibrit harekât önemini korurken klasik harekâtın da dikkate alınmaya başladığı görülmektedir.

Nitekim Rusya'nın 24 Şubat 2022 tarihinde Ukrayna'ya karşı başlattığı klasik savaş bölgesel ve küresel olarak birçok önemli değişikliği tetikleyecektir. Azerbaycan-Ermenistan savaşına ilave olarak Rusya-Ukrayna savaşı dijital çağda ulus-devletlerin millî menfaatleri doğrultusunda klasik anlamda savaşabileceklerinin önemli örnekleri

olarak görülebilir. Bu konuda değerlendirme yapmak oldukça erken olacaktır. Ancak müteakip çalışmalara esas olabilecek bazı değerlendirmeler yapılabilir. Rusya'nın başlattığı harekât her ne kadar klasik bir müşterek harekât olarak adlandırılabilse de, kara, deniz ve hava harekât alanlarına ilave siber ve uzayın da kullanıldığı bir şekle evirilmiştir.[71] Bu çerçevede bilgi harekâtı, siber savaş önemli bir güç unsuru ve araç olarak kullanılmıştır. Kriz yönetimi açısından ise ekonomik güç unsuru ağırlıklı olarak kullanılırken, NATO ve AB'nin birlik beraberlik içerisinde hareket etmeleri, NATO'nun tarihinde ilk defa NATO Mukabele Kuvvetini (NMK) kullanması oldukça dikkat çekicidir. Buna karşın Rusya'nın nükleer silahları, gıda ihracatını ve enerjiyi güç unsuru olarak devreye sokması önemli bir gelişme olarak görülmektedir. Rusya-Ukrayna savaşı genel olarak değerlendirildiğinde sanayi çağı harp prensiplerini benimseyen Rus Ordusu ile birçok ülkenin desteklediği, dijital çağ harp prensiplerini kısmen benimseyen Ukrayna Ordusunun mücadelesi olduğu görülmektedir.

Dijital çağda silahların öldürücü etkisi her geçen gün daha da artmaktadır. Bu çerçevede yıkımın boyutları dikkate alınarak ülkeler arasındaki nükleer savaş olasılığı düşmesi gerekmesine rağmen, Rusya-Ukrayna savaşı bunun aksini ispat eder mahiyette gelişmelere sahne olmuştur. Rusya'nın nükleer güçlerinin hazırlık seviyesini yükseltmiş olması önemli sonuçlar doğurabilecektir.

Bununla berber, stratejik iletişim, vekâlet savaşları, hibrit savaş, siber savaş, iletişim teknolojisindeki gelişmeler, internetin ve akıllı cep telefonlarının yaygınlaşması gibi yenilikler aktörlerin diğer ülkelerin iç işlerine müdahalesini kolaylaştırmaktadır. Küresel ekonominin gittikçe daralması, güvenlik anlayışının birey odaklı bir istikamete doğru kayması, bireylerin ihtiyaçlarının gittikçe artması, kültürel farklılıkların daha fazla dikkat çekmesi ülkelerin iç dayanıklılığını (resilience) test eder mahiyete gelmiştir. Bu çerçevede ülkelerin örtülü veya gizli dış tehditleri tespit edebilmesi ve etkisiz hale getirecek tedbirler almasını gerektirmektedir. Küresel ve bölgesel güvenlik ortamı çok süratli ve sürekli değişmeye devam etmektedir. Dolayısı ile gelişmelerin sürekli takip edilmesi ve güvenlik ortamının değerlendirilmesi önem arz etmektedir.

[71]Miller, Christopher; Scott, Mark; Bender, Bryan, *UkraineX: How Elon Musk's Space Satellites Changed the War on the Ground*, 2022.

Önemli Jeopolitik Gelişmeler ve Yeni Aktörler:

Rusya'nın Suriye'ye yardım etmek vasıtasıyla Doğu Akdeniz ve Ortadoğu'ya tekrar dönmesi gücünü ve etkinliğini daha da arttırmıştır. Söz konusu savaş çerçevesinde Rusya'nın bölgedeki gücünü muhafaza edip edemeyeceğini zaman gösterecektir. Ancak bugün için Rusya'nın Ukrayna harekât alanına daha fazla ağırlık verebileceğine yönelik emareler artmaya devam etmektedir.

Yukarıda da belirtildiği gibi Rusya ile birlikte, İran'ın, başta Irak ve Suriye olmak üzere Ortadoğu ülkelerinde etkinliğini arttırma gayretleri oldukça dikkat çekicidir. Kasım Süleymani ile başlayan Kudüs güçlerinin bölgede gayri nizami harp alt yapısını güçlendirme çalışmaları, halkı örgütleyerek Haşdi Şabi benzeri milis grupları oluşturabilmesi bölgede önemli sonuçlar ortaya çıkarma potansiyeline sahiptir. Ancak ABD'nin savaş ilan etmediği, örtülü bir savaş içerisinde olduğu bilinen İran'ın bir generaline dijital çağın önemli silah sistemlerinden İHA'ları kullanarak suikast düzenlemesi stratejik anlamda kullanılan yöntemlerin bilinenlerin veya alışılanların dijital çağda ne kadar dışına çıkılabildiğini göstermesi açısından önem taşımaktadır.

Örtülü operasyonlar veya vekâlet savaşları için kullanılan diğer bir hükümet dışı örgüt modeli askeri şirketlerdir. Başta ABD ve Rusya olmak üzere farklı ülkeler askeri şirketleri değişik bölgelerde, çeşitli görevlerde kullanmaktadırlar. Askeri şirketler sayesinde aktörler diğer aktörlerin hedefi olmadan, uluslararası hukuk kurallarına uyma mecburiyeti olmadan, örtülü olarak millî menfaatlerini gerçekleştirmek imkânı bulabilmektedirler. Benzer şekilde açık olarak görülmemekle beraber askeri şirketlerin nizami orduların icra ettiği birçok görevi icra edebildikleri vurgulanmalıdır.[72,73]

Ortadoğu geçmişte olduğu gibi günümüzde de stratejik şokların ve krizlerin her an ortaya çıkabileceği güvenlik açısından önemli bir coğrafyadır. Arap Ayaklanmalarının etkilerinin yanında Filistin sorunu, İran'ın nükleer silah edinme gayretleri dijital çağda öne çıkan sorunlar olarak karşımıza çıkmaktadır. Doğal olarak Rusya-Ukrayna arasındaki çatışmanın Ortadoğu'ya da yansılarının olması kaçınılmaz olabilecektir.

Çin ise bölgesindeki denizlerdeki hâkimiyetini pekiştirmeye, 2009 tarihinde ilan ettiği tek yol tek kuşak projesi ile yeni bir ekonomik düzen yaratmaya çalışmaktadır.

[72]McFate, Sean, *Mercenaries and War: Understanding Private Armies Today*, 2019.
[73]Tracol, Clement, *Private Military Companies in the Contemporary Security Context*, 2012.

Bunun yanında Çin'in özellikle hammadde ihtiyacını karşılamak maksadıyla Afrika'da, ayrıca mali kaynak sıkıntısı çeken Avrupa ülkelerinde, başta limanlar ve alt yapıya yönelik faaliyetleri önemli bir endişe kaynağı olarak görülmektedir. Buna ilave olarak Çin'in "Tek Çin" politikası çerçevesinde Tayvan'a baskıları artmakta, Güney Çin Denizi'nde hâkimiyetini geliştirmeye yönelik çabaları devam etmektedir. ABD ve Rusya'nın yanında Çin de önemli bir kutup olarak küresel güvenlik ortamında yerini almaya başlamıştır.

Bu şartlarda küresel anlamda en önemli tehditlerden birisi olarak Çin-Rusya ittifakının gerçekleşmesi olarak görülmektedir. Ancak Çin'in gelecekte Rusya için önemli bir tehdit olma potansiyeli bulunmaktadır. Rusya'nın geniş topraklara sahip olması buna karşın nüfusunun az olması ve azalma eğilimi göstermesi; buna karşın Çin'in nüfusunun fazla olması, ancak topraklarının az olması gelecekte Çin'in Rusya'yı hedef ülke olarak değerlendirmesine neden olabilecektir. Bu değerlendirmeden yola çıkarak bazı ülkelerin Çin ile Rusya'nın ittifakını engellemek maksadıyla Rusya ile bir uzlaşıya gitme arayışı içerisinde olabileceği düşünülebilir. Diğer taraftan bölgedeki güç dengesini sağlamak maksadıyla Hindistan'ın Çin'e karşı desteklendiğine yönelik kuvvetli emareler bulunmaktadır. Ancak Rusya-Ukrayna savaşında Hindistan'ın Rusya'ya yakın bir tutum izlemesi dikkat çekicidir.[74]

Bu gelişmeler sonucunda dünyada çok kutuplu, sürekli değişken bir yapı oluştuğu kabul edilmektedir. Bu küresel güçlerin birbirleri ile rekabet halinde olması, Birinci Dünya Savaşı sonrasında oluşan, realizmin hâkim olduğu bir büyük güçler yarışının yolunu açmıştır. Ancak bu dönemde yalnızca askeri açıdan güçlü olmak yeterli olmamakta, rekabet başta ekonomi, teknoloji olmak üzere diğer konularda da devam etmektedir. Yani realizm ve Kopenhag okulunun karışımı bir güvenlik anlayışından söz edilebilir.

Bu güvenlik anlayışında başta ekonomi olmak üzere diğer sektörlerdeki mücadelenin realist anlayış esas alınarak icra edildiği, askeri güvenlik anlayışının en azından diğerleri ile eşit konumda olduğu bir anlayış daha geçerli olmaya başlamıştır. Günümüzde barış ve savaşın aynı anda yaşandığı dikkate alındığında diğer güvenlik alanlarının da en az askeri güvenlik kadar önemli olduğu sonucuna varılabilir. Bu çerçevede, dijital çağda güvenlik stratejileri tasarımında, kapsamlı yaklaşım adı altında

[74]Tellis, Ashley J, *"What is in Our Interest": India and the Ukraine War*, 2022.

askeri güvenliğin yanında ekonomi, çevre, teknoloji gibi diğer konular da dikkate alınarak bütüncül bir yaklaşım gösterilmesi gerekmektedir.

Yeni Tehditler:

Günümüzde, dijital çağda dikkate alınması gereken diğer önemli bir tehdit ise iklim değişikliğidir. İklim değişikliği neticesinde tarımın olumsuz etkilenmesi, yağışların azalması, buzulların erimesi, doğal afetlerin artması gibi sonuçlar yaşanmaya devam etmektedir. Bu hususlar göçleri arttırırken ileride su ve tarım ürünleri savaşlarının gittikçe daha fazla gündeme gelmesi gibi güvenliği etkileyen önemli sonuçlar ortaya çıkabilecektir.

Bu çerçevede Kuzey Kutbundaki buzulların erimesinin güvenliğe önemli etkisinin olması beklenmektedir. Bu bölgedeki doğal kaynakların paylaşılmasının yanında, ulaşım hatlarının gittikçe kısalması jeopolitik ve jeostratejik açıdan önemli etkiler ortaya çıkarabilecektir. Ayrıca Rusya'nın ülkenin kuzey bölgesindeki limanları kullanmaya başlaması çevreleme stratejini boşa çıkartabilecek bir jeopolitik ve jeostratejik özelliğe sahiptir. Söz konusu bölgenin gelecekte daha yoğun olarak büyük güçler savaşına sahne olması beklenebilir.

Aynı paralelde ülkelerin hidrokarbon yataklarını kontrol etmeleri millî güç unsurları ve ekonomileri için önemli bir faktör olma özelliğini gittikçe arttırmaktadır. Bazı ülkelerin petrol ve doğal gaz ihraç eden ülke konumuna gelmesi günümüz güvenlik ortamında önemli bir parametre olarak karşımıza çıkmaktadır. Ortadoğu ve Hazar denizi bölgesinde bulunan enerji kaynaklarının AB ülkelerine sevki konusunda atılan adımlar ve bölgenin kontrol edilmesine yönelik gayretler önemli sonuçlara neden olabilmektedir. Almanya'nın Rusya-Ukrayna savaşından önce Rusya'dan doğal gaz almaya yönelik kuzey akım projesi ve bu bağlamda gelecekte, savaş sonrasında hammadde ihtiyacının giderilmesi çerçevesinde Rusya ile geliştirebileceği ilişkiler küresel anlamda önemli sonuçlar ortaya çıkarabilecektir.

Kovit-19 salgını sağlık konusunun yanında sosyal, ekonomik, güvenlik alanlarına önemli etkiler oluşturmuştur. Tarihte yer alan değişik savaşlar incelendiğinde askerler kadar salgınlar ile mücadele eden sağlık personeli de önemli olmuştur. Söz konusu salgının günümüzde savaşlardan daha etkin olacak şekilde gerek küresel gerek ulus-devletler çapında önemli sıkıntılara neden olduğu bilinmektedir. Sağlık alt yapısı zayıf olan ülkelerin beka konusunda karşılaştığı problemler dijital

çağda iç güvenliği tehdit eder mahiyete gelebilmektedir. Sosyal medyanın etkisiyle daha da vahim bir hal alabilmektedir. Kovit-19 salgını dijital çağda tehdit ortamının nasıl değişebileceğine güzel örneklerden birisini teşkil etmektedir.

Kovit-19 kadar önemli bir diğer gelişme ise ABD kongresinin 6 Ocak 2021 tarihinde göstericiler tarafından işgal edilmesidir. Göstericilerin aşırı sağcı unsurlara mensup olmasının yanında, bir anda ülkenin değişik bölgelerinde silahlı grupların ortaya çıkması, iktidar değişikliğinin tam olarak barışçıl şekilde yapılamaması, sivil bir darbeyi andıran olayların yaşanması, kolluk kuvvetlerinin olayları engelleyememesi, askerden yardım istenmesi gibi hususlar dijital çağda oldukça önemli küresel çapta mesajlar vermektedir. Demokrasinin beşiği olarak görülen bir ülkenin renkli devrimler ve hatta Arap Ayaklanması benzeri bir karışıklığa maruz kalması, yaygın şiddetin meydana gelmesi ABD'nin imajını küresel etkileri olacak şekilde olumsuz etkilemiştir.

Diğer taraftan birçok alanda insanın ve toplumların, dolayısıyla devletlerin teknolojiye olan bağımlılığının dijital çağda arttırdığı kabul edilen bir gerçektir. Metroların çalışmaması, elektriğin kesilmesi, internet bağlantısının olmaması, ulaşımın aksaması, para çekme makinalarının çalışmaması gibi olaylar insanın ve toplumların günlük hayatlarını güvenliği etkileyecek şekilde etkilemektedir. Dolayısıyla teknolojinin getirdiği bu imkânlar olan bağımlılığın emniyetle devam ettirilebilmesi, ulus-devletler için dijital çağın önemli bir güvenlik sorunu olarak ortaya çıkmaktadır.

Özet:

Özetle dijital çağda güvenlik ortamındaki belirsizlik, muğlaklık artarken; teknolojinin kullanımıyla tarihin akışı hızlanmış; stratejik şoklar, yeni tehditler, yeni aktörler ortaya çıkmıştır. Birey veya uluslararası kuruluşlar olarak ortaya çıkan yeni aktörlerin alışılmışın dışında, bazen ulus-devletlerden daha güçlü ve etkili olabildikleri görülmektedir. Arap Ayaklanmaları, salgın hastalıklar, iklim değişikliği, yeni tip terör saldırıları, teknolojiye bağımlılık dijital çağdaki tehditlere örnek teşkil ederken; özel askeri şirketler, devlet dışı aktörler, uluslararası şirketler yeni tip aktörlere örnek gösterilebilir. Neoliberal düzenin zayıflaması, mali krizlerin meydana gelmesi, uluslararası örgütlerin zayıflaması kural tabanlı küresel sistemi ve küresel işbirliğini olumsuz etkilemektedir. Rusya-Ukrayna savaşı ise dijital çağda ulus-devletlerin yıkıcı

etkisi olabilecek klasik savaşa ve hatta nükleer savaşa bile başvurabileceklerinin önemli bir örneğini teşkil etmektedir.

2.2. DİJİTAL ÇAĞDA GÜVENLİK ORTAMININ GÜVENLİK STRATEJİSİ TASARIMINA ETKİLERİNİN ANALİZİ

Bir önceki başlıkta açıklanan hususlardan istifade edilerek, tarihin çok kısa bir kesitini kapsayan durum tespitinden dijital çağdaki güvenlik ortamının güvenlik stratejisi tasarımına etkileri kısıtlı olarak analiz edilebilir. Daha önceki bölümde incelendiği gibi tarım toplumunda güvenlik anlayışı; krallığın ve kralın güvenliğinin ön planda tutulması, köylülerin tarımda rahat çalışmaları ve yeni topraklar ele geçirerek daha da güçlenilmesi ve zenginleşilmesi olarak özetlenebilir. Birey güvenliğinin ikinci planda tutulduğu, toprak kazanımının zenginliğin ve gücün temeli olduğu, toplum sözleşmesi kavramının oluşmaya başladığı, uluslararası sistemin güvenliğinin ve kuralların oluşturulmasının ise yeteri kadar göz önüne alınmadığı bir yaklaşım görülmektedir. Şehir devletlerinin, imparatorlukların, krallıkların ve derebeyliklerinin hâkimiyetleri tarım çağının belirgin özellikleri arasında yer almaktadır. Sanayi çağı ise özetle; ulus-devlet yapısı çerçevesinde bireyin ve kamu güvenliğinin sağlanması, toprak ele geçirmenin yanında, sanayinin güçlenmesi, bu maksatla hammadde için sömürgelerin kurulması, savaşların yıkıcılığının artmasından dolayı uluslararası sistemin güvenliğine ve kural tabanlı olmasına önem verilmeye başlanması; bu maksatla çalışmaların yapıldığı bir dönem olarak görülebilir. Hem tarım çağında hem de sanayi çağında güvenlik stratejileri tasarımında ekonominin temel bir parametre olarak alındığı unutulmamalıdır.

Dijital çağda ise artık ulus-devletlerin yanında terör örgütleri, uluslararası şirketler gibi yeni aktörlerin uluslararası güvenlik sisteminde dikkate alınmaya başlandığı ifade edilebilir. Yeni aktörlerin uluslararası hukuk kurallarını etkisiz hale getirmeye yönelik faaliyetlerinin kural tabanlı güvenlik sistemi anlayışına önemli derecede olumsuz etkilerinin olduğu belirtilebilir.

Neoliberal yaklaşım kural tabanlı sistemin temelini oluşturmaktadır. Ancak 2008 yılındaki ekonomik kriz, gelir dağılımdaki problemler gibi faktörler kural tabanlı sistemin zayıflamasına neden olmuştur. Yine de küresel ekonomik sistem bağlamında devletlerin birbirlerine olan bağımlılıklarının artarak devam ettiğini ifade etmek yanlış olmayacaktır. Ancak ekonomik gücün önemli bir silah olarak realist anlayışla

kullanılabildiği göz önünde tutulmalıdır. Tarım ve sanayi çağlarında olduğu gibi dijital çağda da ekonomi, güvenlik stratejilerinin tasarımında önemli bir parametre olarak karşımıza çıkmaktadır. Bununla beraber Avrupa Güvenlik Mimarisinin ve silahların kontrolü anlaşmalarının etkinliğinin azalması devletlerarasındaki güven ortamını olumsuz etkilerken, sıcak çatışma olasılığını yükseltmektedir. Bunun sonuçlarına Rusya-Ukrayna savaşında fazlasıyla şahit olunmuştur. Avrupa Güvenlik Mimarisi bağlamında silahların kontörlüne yönelik çalışmaların zayıflaması; Rusya'nın nükleer silahlarını kullanıma hazır hale getirmesiyle tehlikenin hangi boyutlara ulaşabileceğini göstermiştir.

Yukarıda vurgulanan hususları içeren bir güvenlik ortamında, Arap Ayaklanması, Kovit-19, Rusya'nın Kırım ve Ukrayna'yı işgali stratejik şoklar şeklinde uluslararası güvenlik ortamını etkilemektedir. Bu çerçevede dijital güvenlik ortamının değişken, belirsiz, karmaşık ve muğlâk bir yapıda olduğu ifade edilebilir. Değişim sürekli, süratli ve dikkate değer şekilde olmaktadır. Belirsizlik geleceğin tahmin edilmesini zorlaştırmaktadır. Karmaşık olması birçok konunun, faktörün, parametrenin gündeme gelmesine neden olmaktadır. Muğlaklık ise tam olarak durumun ve hatta gerçeklerin anlaşılmasını etkilemektedir. Bu hususların güvenlik stratejisi tasarımında dikkate alınması gerekmektedir. Diğer taraftan Rusya'nın uyguladığı savaş yöntemleri sanayi çağından kalma bir yapıya sahiptir. Buna karşın Ukrayna'nın diğer devletlerin ve aktörlerin desteği ile uyguladığı savaş yöntemi ise dijital çağ savaş yöntemlerinin bir başlangıcı olarak değerlendirilebilir.

Günümüzde Kovit-19 salgını ve hatta sel, yangın gibi diğer felaketler bizlere geçmişte yaşanan felaketlerin dijital çağda çok daha köklü, etkileri çok daha geniş alanlardan hissedilen sorunlara neden olabileceğini, bunun neticesinde ise güvenlik stratejileri tasarımına önemli etkilerinin olabileceğini hatırlatmaktadır. Bu çerçevede kamu güvenliği, vatandaşlara sağlık ve sosyal hizmetlerin ulaştırılması konuları ön plana çıkmaktadır. Maalesef başlangıçta uluslararası toplum salgın konusunda birlik ve beraberlik içerisinde başarılı bir mücadele verememiştir. Dolayısı ile bugüne kadar yapılanlar dikkate alındığında iklim değişikliği konusunda başarılı bir mücadele verilmesi beklenmemektedir. Bu çerçevede her iki konu da stratejik şoklar şeklinde iç ve dış güvenlik bağlamında güvenlik stratejisi tasarımını etkileme potansiyeline sahiptir.

Dijital çağda metropollerin ortaya çıkması ve metropollerde yaşayan insan sayısının gün geçtikçe artması güvenlik konusunda yeni kavramları da gündeme getirebilmektedir. Bu kavramlardan birisi yaşam alanı güvenliği olarak ifade edilebilir. "Yaşam alanı güvenliği ya da diğer bir ifade ile genel asayiş hizmetleri, bireylerin günlük yaşamlarını sürdürürken evlerinde, işyerlerinde, ulaşım araçlarında ya da günlük hayatın her evresinde çok daha üst özelliklere sahip, devletin güvenliği veya kamu düzeninin güvenliği gibi kavramların dışında kalan ama bireylerin bireylerle ve bireylerin temel kamu hizmetlerini veren yapılarla olan ilişkilerini şekillendiren, esaslarını belirleyen bir niteliği tarif eder."[75] Bu kavramın daha üstünde ise yaşam güvenliği tanımlanabilir. "Yaşam güvenliği ise bireylerin ve kamu düzeninin korunmasını ve kollanmasını hedefleyen yaşam güvenliği noktasındaki kamu güvenliği" olarak ifade edilebilir.[76] İkisinin arasındaki fark ise yaşam güvenliği devlet seviyesinde sağlanırken, yaşam alanı güvenliği yerel otoriteler tarafından sağlanması olarak belirtilebilir.

Dünya nüfusu artmaya devam ederken başta enerji kaynakları olmak üzere, kaynaklar gittikçe azalmaktadır. Bu nedenle enerji güvenliği konusu hem devlet hem de küresel ekonomi için önemli bir sorun kaynağı olabilecektir. Münhasır Ekonomik Bölge (MEB), deniz yolları üzerindeki önemli boğazlar ve geçiş bölgeleri enerji güvenliği yanında küresel ticaret ve jeopolitik mücadele için dikkate alınması gereken bölgeler olmaya devam edecektir.

Vestfalya Anlaşması ve Fransız İhtilalini müteakip ortaya çıkan ulus oluşturma süreci küreselleşme neticesinde zayıflamakta, çokkültürlülük ve göçler bu zayıflamayı daha da derinleştirmektedir. Buna ilave olarak müteakiben incelenecek olan teknolojik etkiler ulus-devlet açısından durumu daha tehlikeli hale getirebilmektedir. Hatta devletlerin seçimlerine müdahale edilerek müzahir iktidarların seçilmesinin sağlanması bile gündeme gelmektedir. Bu nedenle güvenlik stratejisi tasarımda iç güvenlik durumunun dikkate alınması ihtiyacı artmaktadır.

Bu anlamda dijital çağın bir yansıması olarak güvenlik stratejilerinin tasarımı ve uygulanması oldukça zor ve riskli olduğu kabul gören bir gerçek haline gelmiştir. Bir stratejinin tasarımı ve uygulanması için gelişmelerin tahmin edilebildiği, lineer

[75] Ayhan, Ufuk, *Metropoliten Alanlarda Güvenlik Sorunu ve Çözüm Önerileri Doktora Tezi*, Gazi Üniversitesi, Sosyal Bilimler Enstitüsü, 2006, s.115
[76] A.g.e., s.113

gelişmelerin olduğu bir güvenlik ortamının varlığı tasarımı kolaylaştıran en önemli parametrelerden birisidir. Ancak dijital çağda stratejik güvenlik ortamındaki istikrarsızlık, yeni aktörlerin ortaya çıkması, aktörlerin amaçları ve kimliklerindeki değişmeler, ülke içerisindeki politik ve güvenlik kuruluşlarının yapıları ve çalışma usulleri gibi hususlarda önemli belirsizlikler bulunmaktadır. Ayrıca çokkültürlülüğün ve popülist politikaların gittikçe artması güvenlik stratejisi tasarımını etkileyecek şekilde millî değerlerin ve kimliğin aşınmasına neden olmaktadır.

Dijital çağ güvenlik ortamında düşmanı, dostu ve tarafsızı doğru değerlendirmek, tehdidi doğru belirlemek oldukça zorlaşmıştır. Bu çerçevede içerisinde bulunan güvenlik durumunun parametrelerinin doğru tespit edilmesi önemli bir kuvvet çarpanı haline gelmiştir. Bunun yanında konjonktürde meydana gelen süratli değişiklikler neticesinde tasarımın başlangıcında ortaya konulan değerlendirmeler beklenenden daha hızlı değişebilecek, bu nedenle de başlangıçta ortaya konulan stratejik parametreler değişerek tasarımı etkisiz ve hatta geçersiz hale getirebilecektir. Benzer şekilde aktörlerin kuvvet kullanma yöntemleri, kuvvet kullanma amaçları da değişmiştir. Özetle Soğuk Savaş zamanında olduğu gibi belirgin bir ortamda güvenlik stratejisi geliştirilmesi için kullanılan teknikler geçerliliğini yitirmiştir.

Bununla beraber hâlâ ulus-devletler uluslararası sistemin en önemli aktörü olmaya devam etmekte, toprak kazanmak, önemli su yollarının ve enerji kaynaklarının kontrol edilmesi, bölgesel nüfuz sağlanması stratejik amaçlar/hedefler olarak belirlenebilmektedir. Ancak günümüzde artık toprak ele geçirmek, ülke işgal etmek maliyet etkinliği dikkate alındığında geçmişteki kadar kabul görmemektedir. Bu anlamda devletlerin iki konuya ağırlık verdiği ifade edilebilir. Bunlar millî refahın artırılması ve ekonomik bir şekilde en az kaynak kullanarak millî menfaatlerin gerçekleştirilmesi olarak özetlenebilir. Her devlet için farklı olabilmekle birlikte, genel olarak devletler; iyi bir ekonomiye, teknolojik üstünlük sağlayabilecek bir altyapıya sahip olmayı ve küresel ağlar (network) ile iletişim halinde olarak durumsal farkındalıklarını üst seviyede tutmayı hedefledikleri görülmektedir.

Diğer taraftan askeri yöntemler kullanılarak millî hedeflerin gerçekleştirilmesi veya problemlerin çözülebilmesi gittikçe zorlaşmaktadır. Hatta Afganistan ve Irak'ta da görüldüğü gibi askeri müdahalelerin, durumun daha iyiye gitmesinin aksine daha da kötüleşmesine neden olduğu görülmektedir. Bu çerçevede küresel veya büyük güçlerin askeri güç kullanımını nispeten sınırladıklarını ve daha küçük, uygun

kabiliyetteki kuvvetlerle muharebe sahasında bulunmayı tercih ettiklerini ifade etmek yanlış olmayacaktır. Aslında bu dijital çağda yeni askeri yöntemlerinin, güç unsurlarının kullanılmaya başlandığını gösteren önemli bir emare olarak algılanabilir. Çağımızın diğer önemli bir özelliği ise yeni aktörlerin küresel güvenlik ortamında etkin rol oynamak için gayret sarf etmeleridir. Yeni aktörlerden bazıları; bölgesel gruplar, terör örgütleri, savaş ağaları, devlet dışı aktörler, özel askeri şirketler, büyük küresel şirketler olarak listelenebilir.

Özetle yeni aktörler, askeri güç kullanmadaki sorunlar, yeni güç kullanma yöntemleri, teknolojideki gelişmeler, küreselleşmenin etkileri, göçler sonucunda ulus-devletlerin çokkültürlülük çerçevesinde yaşadığı sorunlar gibi sınamalar küresel güvenlik ortamını çok karmaşık hale getirmiştir. Doğal olarak bu ortama yönelik olarak güvenlik stratejisi tasarlanması ve yönetimi zorlaştırmıştır. Böyle bir ortamda ulus-devletlerin millî menfaatleri çerçevesinde istediklerini klasik, sanayi çağından kalma alışıla gelmiş yöntemler ile elde etmeleri zorlaşmıştır. Aktörler, neoliberalizme dayalı küresel düzenin ve işbirliği mekanizmalarının etkisinin zayıfladığı bir ortamın içerisinde yaşamakta olduklarını güvenlik strateji tasarım ve yönetimde dikkate almak zorundadırlar.

Askeri yöntemlerin kullanıldığı savaşların büyük maliyetler ve ekonomiye önemli bir yük getirmesi; bunun diplomatik yöntemler kullanılarak bulunabilecek çözümleri de etkilemesi küresel güvenlik ortamını daha da karmaşık hale getirmektedir.

Böyle bir karmaşık küresel güvenlik ortamında klasik veya lineer bir düşünce sistemiyle güvenlik stratejileri tasarımı ve bu sayede millî menfaatlerin gerçekleştirilmesinin imkânsız hale geldiği kabul gören bir gerçektir. Diğer taraftan böyle bir karmaşık ortamda güvenlik stratejisi olmadan millî menfaatlerin gerçekleştirilmesinin de mümkün olamayacağını kabul etmemiz gerekmektedir. Bu nedenle güvenlik stratejileri tasarımının ve yönetiminin günümüz koşullarına uyarlanması gerekmektedir. Uyarlama çalışmalarının başında âdemi merkeziyetçi bir karar alma sistemi ve daha kısa zaman aralıkları ile değerlendirmelerin yapılması, ara hedeflerin belirlenmesi gibi yöntemlerin kullanılması düşünülebilir.

Sonuç olarak, Arthur F. Lykke Jr tarafından 1989 yılında ortaya konulan; Strateji = Hedef + Konsept + Kaynak ;şeklinde denklem olarak da ifade edilen klasik strateji tasarımının çerçevesi dijital çağda, güvenlik ortamında meydana gelen değişiklikler dikkate alındığında etkinliğini, belki de geçerliliğini yitirmiştir. Tezin sorusunun

cevaplandırılabilmesi kapsamında en azından dijital çağdaki güvenlik ortamının şartlarına uyum sağlaması için gerekli tedbirlerin alınması gerektiği açık olarak ortaya çıkmaktadır.

2.3. DİJİTAL ÇAĞDA GÜVENLİK STRATEJİSİ TASARIMINI ETKİLEYEN TEKNOLOJİK GELİŞMELER

Tarım çağındaki en önemli buluş kara saban, sanayi çağında ise en önemli buluş buharlı makine olarak kabul edilebilir. Bu buluşlar veya teknolojilerin genellikle insanın kas gücünün yerini aldığı ifade edilebilir. Dijital çağda ise en önemli buluş bilgisayarların daha etkin kullanılmaya başlanması ve hızla bilgisayar teknolojisinin gelişmesidir. Bu çerçevede bilgisayarların kullanılmaya başlanmasıyla artık insan beyninin fonksiyonlarının bazılarını yerine getirebilecek çalışmalar başlamıştır. Bu çalışmalar 2000'li yıllarının başında bilgisayar teknolojisindeki ve yazılım konusundaki baş döndürücü gelişmeler ile süratlenmiştir.

Dijital çağdaki güvenlik stratejileri tasarımını etkileyebilecek en önemli teknolojik buluş bilgisayar teknolojisindeki gelişme olarak kabul edilmesine rağmen, diğer teknolojik gelişmeler de tasarımı önemli ölçüde etkileme potansiyeline sahiptir. Güvenlik stratejisi tasarımını etkileme potansiyeli olan teknoloji ve buluşlardan bazıları; Büyük Veri (BV), Yapay Zekâ (YZ), internet, nesnelerin interneti (Internet of Things, IOT), sosyal medya, metaverse, cep telefonları, yeni sensör teknolojileri, otonom sistemler, kuantum bilgisayarlar, siber savaş yöntemleri, uzay teknolojileri olarak özetlenebilir. Bunun yanında medya kuruluşlarının, televizyon ve radyo gibi haberleşme araçlarının da etkinliği teknoloji sayesinde artmıştır. Bu teknolojilerden özellikle BV, YZ, internet ve otonom sistemler güvenlik stratejisi tasarımını önemli ölçüde etkileme potansiyeline sahiptir. Güvenlik stratejisi tasarımına önemli etkisi olanlar müteakip maddelerde incelenmiştir.

2.3.1. Büyük Veri

Dünya nüfusunun yaklaşık % 62,5'nin internet, yaklaşık % 58,4'nün sosyal medya[77],% 67,1'nin[78] cep telefonu kullandığı ve bu oranların çok süratli bir şekilde arttığı ifade edilebilir. Bunun yanında güvenlik kameraları, meteoroloji sensörleri, medya kuruluşlarının yayımları, uydu fotoğrafları, İnsansız Hava Aracı (İHA) kameralarının görüntüleri gibi birçok veri kaynağı bulunmakta ve bunların sayısı gittikçe artmaktadır. Bu çerçevede dijital çağın en önemli özelliklerinden birisinin veri üretimi olduğu belirtilebilir. BV olarak nitelendirdiğimiz bu veri üretiminin üç önemli özelliği bulunmaktadır. Bunlar hacim, hız, çeşitliliktir.

İnsanların sürekli internet, cep telefonu gibi araçlar ile sürekli çevrim içi olmaları; sensörlerin, kameraların ve medyanın da sürekli çevrim içi olması neticesinde çok büyük hacimde veri üretilebilmektedir. İnsanın bu kadar büyük miktardaki veriyi gözden geçirip kullanabilmesi imkânsızdır.

İnsanların, sensörler ve medya kuruluşları gibi unsurların sürekli çevrim içi olması büyük hacimli olan verinin sürekli, hızla akmasına neden olmaktadır. Bu nedenle veri sürekli değişime uğramaktadır. Verinin sürekli değişime uğraması yapılacak stratejik değerlendirmeleri ve buna bağlı olarak alınacak kararları olumsuz etkilemektedir. Bu çerçevede gündeme gelebilecek en önemli tehlike ise karar vericilerin gereksiz bilgiler ile meşgul edilmesi, esas dikkate almaları gereken verilerin zamanında sunulamamasıdır. Doğal olarak BV'nin kullanışlı hale getirilmesi oldukça önemli bir kuvvet çarpanı oluşturmaktadır.

Büyük hacimli, akan veri değişik ve çeşitli şekillerde ortaya çıkabilmektedir. Veri metin, fotoğraf, video, ses, sinyal olarak yapılandırılmış veya yapılandırılmamış olarak karşımıza çıkabilmektedir. Yapılandırılmış veri daha önceden uygun şekilde depolanmış ve istenildiği zaman kullanıma hazır olan veridir. Elde edilen verilerin çoğu, yaklaşık % 80'ni yapılandırılmamış olduğu ifade edilebilir[79]. Yapılandırılmamış verilerin depolanması, bilgi haline getirilebilmesi mevcut teknolojik imkânlarla oldukça zor bir süreci içermektedir.

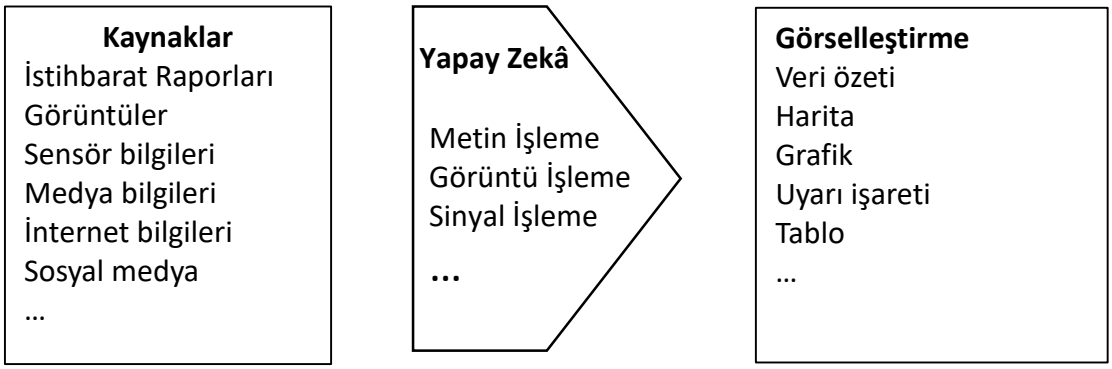
[77]Digital 2022, *Global Overview Report* (bigumigu.com), 13 Mayıs 2022.
[78]Digital 2022, *WeAreSocial 2022: Dünyada ve Türkiye'de İnternet-Sosyal Medya Kullanımı* (recrodigital.com), 13 Mayıs 2022.
[79] Taylor, Christine, *Structured vs. Unstructured Data* (datamation.com), 21 May 2021.

Bu kadar büyük hacimli, hızlı akan, çeşitli formlardaki verinin yönetiminin sağlanması, doğruluğunun kontrol edilmesi, insanın anlayacağı şekle sokulması oldukça zordur. Bu çerçevede veri analizi, veri bilimciliği gibi yeni uzmanlık alanları gündeme gelmektedir. Veri bilimcisinin BV'nin yönetilebilmesi ve istenen amaçlar için kullanılabilmesi için bir dizi işlem yapması gerekmektedir. Bunlar özetle; problemin tanımlanması, veri toplama, verinin temizlenmesi, verinin kullanım modelinin belirlenmesi, kullanıma sunulmasıdır. Konuya güvenlik stratejisi tasarımı ve yönetimi açısından baktığımızda üç temel alanda BV'nin kullanımının yapılabileceği düşünülebilir. Bunlar stratejik istihbarat, durumsal farkındalık stratejik planlamanın yapılmasıdır.

Bilindiği gibi istihbarat çarkı; ihtiyaçların tespiti ve yönlendirilmesi, toplama, işlem ve yayım ve kullanma olmak üzere süreklilik arz eden dört safhalı bir süreçtir. İhtiyaçların tespiti veri bilimci için toplama amacını ve problemin tanımlanmasına yardımcı olabilecektir. Toplama safhasında ise sinyal istihbaratı (signal intelligence, SIGINT), görüntü istihbaratı (image intelligence, IMINT), açık kaynak istihbaratı (open source intelligence, OSINT), insan istihbaratı (human intelligence HUMINT), coğrafi konum istihbaratı (geospatial intelligence, GEOINT),yayılım istihbaratı (measurement and signature intelligence, MASINT) çerçevesinde ham veri toplanmaktadır. Bu veriler kurum içi ve dış kaynak olarak ikiye ayrılabilir. Genel olarak bu veriler metin, sinyal ve görüntü olarak gelecektir. Ham olan BV'nin süratle işleme tabi tutulabilmesi için metin, sinyal ve görüntü işleme gibi teknikleri kullanılarak ham veri bilgi haline, yani istenen bir formata dönüştürülebilir.

Bu verilerden bazıları durumsal farkındalık için bir pano/harita üzerine yerleştirilebilir. Örneğin dünya üzerindeki kriz bölgeleri bu şekilde gösterilebilir. Bunun yanında değişik tablolar veya grafikler oluşturulabilir. Erken ikaz sistemi kurulabilir. Hedef ülkenin millî güç unsurlarının durumları incelenerek tehdit değerlendirmesi yapılabilir. Bu çerçevede Şekil 2.2'de BV'nin istihbarat haline getirilmesi gösterilmektedir. Bu çalışmada BV'nin istihbarat haline getirilmesi bir katkı olarak sunulmaktadır.

Şekil 2.2: Büyük Verinin İstihbarat Haline Gelmesi.



Kaynak: Yazar tarafından oluşturulmuştur.

Stratejik planlama için stratejik seviyede elde edilen BV, aktörlerin çalışma yöntemlerinin belirlenmesi, stratejik karar verme kültürlerinin tespit edilmesi, davranışlarındaki anomalitenin tespit edilmesi gibi konularda kullanılabilir. Bunun yanında ekonomi, nüfusun durumu, askeri gücün hazırlık durumu gibi millî güç unsurlarının durumunun tespit edilmesi için de BV'den faydalanılabilir. Bu veriler kullanılarak stratejik planlamaların daha etkin yapılmasında kullanılan varsayımlar, faktörler daha fazla bir doğrulukla tespit edilebilir. Ayrıca planlamanın sürati ve doğruluğu artabilir.

2.3.2. Yapay Zekâ

YZ özet olarak insanın zihinsel olarak yaptığı işlemlerin bilgisayara yaptırılması olarak ifade edilebilir. Bu sayede BV'nin işlenebilmesi ve faydalı hale getirilmesi sağlanabilmektedir. Üç çeşit YZ'den bahsedilebilir. Bunlar dar, geniş ve süper YZ'dir. Kısaca dar YZ insanın yerine getirdiği bazı fonksiyonların yerine getirilmesi, geniş YZ ise insan gibi bilgisayarın davranabilmesi, süper YZ ise insandan daha kabiliyetli bir yapının oluşturulabilmesidir. Bilim adamları halen ağırlıklı olarak dar YZ üzerinde çalışmaya devam etmektedirler.

YZ'nin alt kolu olarak makine ve derin öğrenme teknikleri sayılabilir. Makine öğrenmesi bilgisayara ağırlıklı olarak istatistiki yöntemler kullanarak insan gibi düşünmesini öğretmek olarak tanımlanabilir. Makine öğrenmesinde üç ana yöntem kullanılmaktadır. Bunlar denetimli, denetimsiz ve pekiştirmeli öğrenmedir. Denetimli

öğrenmede bilgisayara verilen veri seti ile kuralların tanımlanması, bu kurallara uygun olarak sonuçlar üretmesi hedeflenmektedir. Denetimsiz öğrenme ise kural tanımlanmadan verinin gruplara ayrılması hedeflenmektedir. Pekiştirmeli öğrenmede ise belirli bir mükâfat tanımlaması çerçevesinde kararların verilmesi hedeflenmektedir. Derin öğrenme ise insan beynindeki nöronların yapıları taklit edilerek matematik fonksiyonlardan oluşan katmanlar ve denklemler kullanılarak bilgisayarın insan gibi düşünmesinin sağlanmasıdır. YZ'nin başarılı sonuçlar verebilmesi için mümkün olduğu kadar fazla veri ile eğitilmesi gerekmektedir.

Değişik YZ yöntemleri bulunmaktadır. Doğal Dil İşleme (Natural Language Process, NLP) metin halindeki veriyi alıp özet çıkartma, metindeki duygu analizi gibi işlemleri yapabilir. Görüntü İşleme (Image Process, IP) ise bir görüntünün sınıflandırması, yüz tanıma, duygu analizi gibi fonksiyonları yerine getirebilir. YZ yöntemleri kullanarak güvenlik değerlendirmesi maksadıyla bir aktörün istikrar durumu, eğilimleri, izlediği patern, eylemlerindeki farklılık (anomaly detection) gibi hususlar ortaya konulabilir. Ayrıca dünya üzerinde meydana gelen olayların tespit edilebilmesi ve bu olaylardan önemli olanlar belirlenerek daha önce ifade edildiği gibi erken uyarı sisteminde kullanılması gerçekleştirilebilir.[80] Ancak YZ kullanarak, özellikle hedef olarak belirlenen aktörün yanlış verilerden faydalanması sağlanarak aldatma yapılabileceği de her zaman akılda tutulmalıdır. Önümüzdeki süreçte teknolojinin gelişmesiyle bu imkân ve kabiliyetlere yenileri eklenecektir. Ancak YZ'nin her sorunu çözebileceği, her soruya cevap verebileceğini düşünmek yanlış sonuçlar verebilecektir.

2.3.3. İnternet, Sosyal Medya, Metaverse, Nesnelerin İnterneti

Dijital çağın en belirgin özelliklerinden birisi internettir. Başlangıçta sadece mesaj gönderme ve okuma yapılan bir sistem olan internet günümüzde internet 2.0 olarak adlandırılan insanların birbirleri ile etkileşime geçebildikleri, bloklar ve uygulamalar ile veri üretebildikleri bir yapıya evirilmiştir. İnsanlar Facebook, Twitter gibi uygulamalar kullanarak bu etkileşimi gerçekleştirmektedirler. Hatta belirlenmiş kişiler tarafından katkı sağlanabilen, yazı yazılabilen, tek merkezden yönetilen, belirli kişiler tarafından katkı yapılabilen Wikipedia gibi uygulamalar insanların algısını önemli

[80]Babak, Akhgar vd., *Application of Big Data for National Security*, 2015.

ölçüde yönlendirebilmektedir. Kullanıma başlanabileceği öngörülen internet 3.0'da bu sorunun ortadan kaldırılabileceği, daha dağıtık bir yapının ortaya çıkabileceği ifade edilebilir. Yani her şeyde olduğu gibi güvenlik stratejilerini önemli ölçüde etkileme potansiyeli olan internetin de sürekli değişim halinde olduğu dikkate alınmalıdır. İnsanlar internetten yalnızca bilgi almakla kalmamakta, kendi düşüncelerini de paylaşabilmektedir. Bu nedenle internet önemli bir BV kaynağı, dolayısıyla açık istihbarat kaynağı haline gelmiştir.

İnsanlar internette birçok işlem gerçekleştirmektedir. Bunlardan bazıları; bankacılık, alışveriş, medya takibi, mesajlaşma, sosyal medya ile arkadaşlarıyla iletişim kurmak, eğlence, eğitim, değişik sensörlerden gelen bilginin takibi gibi işlemlerdir. Bu işlemlerin her biri BV üretimine önemli katkılar sunmaktadır. Bu internet çoğu insanın erişebildiği ve işlemler gerçekleştirdiği yüzeysel internettir. Bunun yanında internetin derin ve karanlık internet olmak üzere iki katmanı daha bulunmaktadır. Derin internet özel cihaz ve yöntemler ile girilebilen devletlerin, değişik kurumların bilgilerinin saklı olduğu, işlemler yapılabilen bir internet katmanı olarak tanımlanabilir. Karanlık internet ise yine farklı, özel yöntemler ile girilebilen internetin çok daha karanlık ve kanunsuz katmanıdır. Bu internet ortamlarında çok daha fazla bilgi bulunmaktadır.

Sosyal medya, Facebook'un 2004 yılında kuruluşundan itibaren, insanların internetteki en fazla kullandıkları alanlarından birisini oluşturmuştur. Müteakiben başka sosyal medya uygulamaları ortaya çıkmıştır. Sosyal medya şirketlerinin de dâhil olduğu büyük bilgisayar şirketleri GAFAM (Google, Amazon, Facebook, Apple, Microsoft) olarak adlandırılmaktadır. Bu şirketlerin dijital sektördeki hâkimiyetleri çok daha önemli sonuçlara yol açmaya başlamıştır. Bu şirketler birçok konuda kendi kurallarını koyabilmekte, ulus-devletlerin egemenliklerine meydan okumaktadırlar. Kişilere verilen dijital vatandaşlık benzeri uygulamalar ulus-devletlerin daha fazla sorgulanmasına neden olmaktadır.

Ulus-devletlerin egemenliklerini zayıflatabilecek diğer bir konu ise kripto para kullanımıdır. İnternet aracılığı ile blokchain ve buna bağlı olarak kripto para kullanımı; bankacılık ve küresel finans sistemi üzerinde yıkıcı (disruptive) etkiler oluşturma kapasitesine sahiptir. Blockchain anlayışı ile oluşturulmuş düğüm noktalarında verilerin depolanması, belirli protokoller kullanılarak işlem yapılabilmesi gerçekleştirilebilmektedir. Bu çerçevede bazı işlemlerin bu konsept kullanılarak

emniyetli olarak yapılması, sanal kuruluşlar, hatta sanal polis karakolları (özel şirketlere ait olabilir) gibi güvenlik kuruluşları oluşturulması da gündeme gelebilecektir. Ancak bu etkilerin sonucunda devletlerin merkez bankalarının etkinliklerinin azalması ve hatta ortadan kalkması ulus-devletler için oldukça önemli sonuçlar doğurabilecektir. Bunun yanında kripto para kullanımı bazı aktörlerin güçlenmesi, yasa dışı faaliyetlerin hızlanması gibi başka sonuçlara da neden olabilecektir. Kripto para ve dijital çağdaki diğer teknolojik gelişmelerin sonuçları; şehir devletleri, krallıklar, ulus-devletler gibi tarihi süreçteki devlet yapılanmalarından sonra devlet sonrası (post-state) yapıların oluşabileceğini işaret etmektedir. Diğer taraftan ulus-devletlerin dijital paraya ilgilerinin ve bu yapıyı kontrol etme gayretlerinin artmaya devam ettiği ve dijital para kullanımına geçilmeye başlandığı bilinmektedir.

Önümüzdeki dönemde metaversin gündeme gelmesi çok daha ilginç güvenlik sorunlarına neden olabilecektir. Metaverse internette yapabildiğiniz birçok işlemi beraber yapabildiğiniz, oluşturacağınız avatar ile alışveriş yapabileceğiniz, ödeme yapabileceğiniz, gezebileceğiniz, oyun oynayabileceğiniz, konsere gidebileceğiniz kısacası sanal bir dünyada üç boyutlu olarak hareket edebileceğiniz bir dijital ortam oluşmaktadır. Yani sanal evrenler oluşturulacaktır. Güvenlik çerçevesinde metaverste mülk edinmek, sanat eseri yaratmak, bitcoin ile para ödemek, katılımcıların uyması gereken kuralları belirlemek, kişilerin kurallara uymadığı takdirde verilecek cezaları belirlemek önemli tartışma konuları olarak gündeme gelmektedir. Daha şimdiden NFT (Non Fungible Token), yani değiştirilemez varlık olarak adlandırılan, sanat eserleri dolandırıcılığı başlamıştır.

İnternet konusunda bilinmesi gereken diğer önemli bir konu ise verilen bilgilerin hepsinin doğru olmamasıdır. Bu bilgiler çoğunlukla belirli kaynaklar tarafından kasıtlı olarak yayılmaktadır. Bu çerçevede insanlara kimlik suikastı dâhil birçok iftiraların atılması, imajların zedelenmesi, algı yönetimi ile yanlış yönlendirmelerin yapılması gibi sonuçlar doğurmaktadır. Dolayısıyla internetin faydalarının olduğu kadar zararlı taraflarının olduğu bilinmelidir.

Başta cep telefonları olmak üzere birçok cihaz ve sensör internet ortamını kullanarak haberleşmektedir. Çok yakın bir zamanda 5G teknolojisiyle birçok sistemin, cihazın, sensörün internet aracılığı ile yönetimi çok daha kolay hale gelebilecektir. Bu sistem nesnelerin interneti olarak adlandırılmaktadır.

2.3.4. Medya

Dijital çağın en belirgin özelliklerinden birisi de medyanın gücünü arttırmış olmasıdır. Medya kuruluşları uydu antenleri, internet, cep telefonları ve diğer cihazlar sayesinde dünyanın birçok yerinde insanlara çok süratli olarak ulaşabilmektedir. Bu konu o kadar ileri gitmiştir ki savaşlar bile artık naklen, gerçek zamanlı olarak medya kuruluşlarından yayımlanabilmektedir. Bu sayede medya önemli bir güç unsuru olarak karşımıza çıkmaktadır. Medyanın yönlendirilmesi ve yönetilmesi aktörler için önemli avantajlar sağlamaktadır. Bunun farkında olan aktörler medyayı güç haline getirmek ve hedef kitlelere en süratli, etkin bir şekilde ulaşabilmek maksadıyla değişik yöntemler kullanmaktadırlar.

Medya kuruluşlarının haberleri veya verdikleri bilgiler internet ortamında elde edilen bilgiler ile mukayese edildiğinde; haberlerinin kaynakları belirli olmasından dolayı nispeten daha güvenilir olduğu sonucuna varılabilir. Bununla beraber bazı aktörler çok değişik yöntemler kullanarak millî menfaatleri doğrultusunda medyayı kullanarak algı yönetimi yapabilir, bilgi harekâtı icra edebilir.

Dijital çağ medyası BV ve YZ uygulamalarını ağırlıklı olarak kullanmaya başlamıştır. Başta "The New York Times", Reuters, BBC, Bloomberg, "The Washington Post" gibi medya kuruluşları olmak üzere birçok medya kuruluşu YZ uygulamalarını kullanmaktadır.[81]Medya kuruluşları YZ sayesinde çok süratli olarak haber toplayabilir, değerlendirebilir ve belirli adreslere yayımlayabilir. Mevcut teknoloji ile belirli sınırlar çerçevesinde haber üretimi bile yapılabilir. Dünyanın değişik bölgelerindeki olaylar söz konusu bölgede muhabir olmadan süratle tespit edilebilir. Doğal Dil İşleme yöntemleri kullanılarak özetler çıkarılabilir. Teknolojinin gelişmesiyle birlikte bu konuda gelişmeler önümüzdeki dönemde daha hızlı gündeme gelebilecektir.

2.3.5. İnsansız ve Otonom Sistemler

BV ve YZ alanındaki gelişmeler insansız ve otonom sistemler alanında önemli gelişmelere neden olmuştur. Bu sistemler genel olarak üçe ayrılabilir. Bunlar uzaktan

[81]Underwood, Corinna, *Automated Journalism-AI Application at New York Times, Reuters, and Other Media Giants*, 2019.

komutalı sistemler, yarı otonom ve tam otonom sistemler olarak ifade edilebilir. Günümüzde söz konusu sistemlerin çoğu şimdilik uzaktan komuta edilebilen sistemler olarak ortaya çıkmaktadır. Bazı sistemler yarı otonom olarak da tasarlanabilmektedir. Tam otonom sistemlerin geliştirilmeye ihtiyacı bulunmakla birlikte yakın gelecekte bu konuda da önemli gelişmelerin olması beklenmektedir. Otonom sistemlerin kullanımı konusunda hukuk ve etik konularında çalışmalar başlatılmıştır.

Söz konusu sistemleri hava, deniz, kara platformu olarak görebileceğimiz gibi uzay ve siber ortamlarda da otonom sistemlerin kullanılmaya başlandığına şahit olunmaktadır. Bu sistemlerin özellikle bilgi toplama konusunda karar vericilere önemli katkılar sağladığı bilinmektedir. Söz konusu sistemler sayesinde ulaşım, haberleşme, muharebe sahasında manevra veya hassa vuruş gibi imkân kabiliyetler gelişmektedir. Ancak insan hayatı söz konusu olduğunda mutlaka son kararın insan tarafından verilmesi konusunda bir uzlaşı bulunmaktadır.

2.3.6. Uzay Teknolojileri

Yaklaşık son 70 yıllık bir süreçte uzay çalışmaları oldukça ileriye gitmiştir. Roket teknolojisinin ilerlemesiyle her gün onlarca uydu uzaya atılmakta, aktörler uzayı hâkimiyetleri altına almak için mücadele etmektedir. Uydular, haberleşme, internet hizmeti, gözlem, meteoroloji, seyrüsefer gibi amaçlar ile günümüzde yaygın olarak kullanılmaktadır. Turizm konusunda gelinen aşama uzay teknolojisinin ulaştığı seviyeyi göstermesi açısından önem taşımaktadır. Atmosferde hareket edebilen hava araçlarının benzeri olan yeni uzay araçları hem atmosferde hem uzayda hareket edebilecek şekilde süratle geliştirilmeye devam edilmektedir. Bu nedenle önümüzdeki dönemde uzay turizminin daha ucuzlayabileceği ve artabileceği öngörülebilir. Doğal olarak uzayın çok daha süratli keşfedilmesi dijital çağın önemli bir sonucu olarak karşımıza çıkabilecektir.

Uzay çalışmaları kapsamında başka gezegenlerin keşfedilmeye devam edilmesi, gelecekte, dünya üzerindeki keşif faaliyetlerine benzer etkiler yapabilecektir. Bugün için oldukça yavaş ilerleyen bu husus insanların gelecekte uzayda koloniler kurmaları ile sonuçlanabilecektir.[82]

[82]Tillman, Taylor Nola, *Space Colonies Will Start Out Like the Wild West*, Grow Family-Friendly, 2016.

Tüm bu hususlar aktörlerin uzayın hâkimiyeti ve kullanımı konusunda mücadele etmesine neden olmaktadır. Bu nedenle uzay kara, deniz ve havaya ilave olarak önemli bir mücadele alanı olarak karşımıza çıkmaktadır.

2.4. TEKNOLOJİK GELİŞMELERİN GÜVENLİK STRATEJİSİ TASARIMINA ETKİLERİ

Tarih boyunca yaşanan teknolojik gelişmelerin güvenlik ve güvenlik stratejisi tasarımına önemli etkileri olmuştur. Kara sabanın icadı tarımın gelişmesine neden olurken, toprakların ve köylülerin korunması gibi güvenlik ihtiyaçlarını da gündeme getirmiştir. Bu maksatla kalelerin tasarımında bu ihtiyaç göz önüne alınmış ve kaleler bu konsept dikkate alınarak inşa edilmiştir. Buhar makinesinin bulunması ise çok daha fazla güvenlik ve güvenlik stratejisi tasarımına etkisi olmuştur. Bu anlamda sanayi çağında silahların öldürücülüğünün artması neticesinde, uluslararası güvenlik sistemine, barışın sağlanmasına daha fazla önem verildiği; ulus-devletlerin millî güvenliklerinin ön plana çıktığı ifade edilebilir.

Bilgisayarın kullanılmaya başlamasıyla dijitalleşme; kara saban, buharlı makineler gibi toplum, ekonomi, günlük hayatımız ve benzeri alanlarda önemli değişiklikler yaratmaya başlamıştır. Bu değişiklikler güvenlik alanında tarım ve sanayi çağı ile mukayese edildiğinde çok daha değişik, önemli farklılıklar meydana getirmiştir. Dijitalleşme ile daha önce ifade edildiği gibi insanın beyin fonksiyonlarının, düşünme sisteminin takviye edilmesi çerçevesinde; insan hayatının her alanında güvenliliği de kapsayan çok daha etkili, önemli değişiklikler meydana gelmiştir. Bu çerçevede bilimsel çalışmalar, buluşlar, haberleşme ve ulaşım gibi insan hayatındaki önemli fonksiyonların tamamı hızlanmıştır. Doğal olarak güvenlik alanında verilen kararlar ve bu kararların icrası ve icra neticesinde ortaya çıkan durumlara geçmişe nazaran daha hızlı tepki gösterilmesi, güvenlik stratejilerinin tasarımını önemli ölçüde zorlaştırmıştır. Hatta yeni yaklaşımların kullanılmasını zaruri hale getirmiştir.

Dijitalleşme ile teknolojinin neredeyse bütün alanlarında meydana gelen baş döndürücü ve süratli gelişmeler teknolojinin güvenlik tasarımlarında önemli bir parametre olarak dikkate alınmasını gerektirmektedir. Rakip aktörler tarafından kullanılan teknolojiler tehdit olarak ortaya çıkarken, teknolojinin güvenlik stratejisi

tasarımında ve yönetiminde kullanılabilmesi çok önemli avantajlar sağlamaktadır. Yukarıda açıklanmaya çalışılan dijital çağ teknolojilerinden bazılarının güvenlik stratejisi tasarımına olabilecek etkileri; tasarım süreci çerçevesinde müteakip maddelerde incelenmiştir.

2.4.1.BV ve YZ'nin Güvenlik Stratejilerinin Tasarımına Etkisi

Gelişmiş veya gelişmekte olan ulus-devletlerin birçoğu BV ve YZ konusunu millî güvenliğin bir parçası olarak görmektedir. İlk bakışta BV ve YZ insan hayatını kolaylaştıracak, medeniyetimizin gelişmesini sağlayacak önemli bir teknolojik gelişme olarak görülmektedir. Ancak rakip aktörlerin elinde BV ve YZ önemli bir tehdit kaynağı da oluşturabilir. Buna karşın ulus-devletler tarafından iyi kullanıldığında millî güvenliğin sağlanmasında önemli bir millî güç unsuru da olabilir.

Üretilen BV'nin, YZ ile kullanılabilir, faydalı hale getirilmesinin güvenlik açısından önemli sonuçları olmaktadır. Veri üretiminin 5G ve ortaya çıkacak iletişim teknolojileri ve sensör yapıları ile daha da artabileceği dikkate alındığında konunun önemi daha iyi anlaşılabilir. Devletler bu konuyu millî güvenlik meselesi olarak gördüklerinden dolayı 5G alt yapı çalışmalarına Çin'in bir şirketi olan Huawei'nin katılmasını engellemeye çalışmaktadırlar. Bu husus ilk bakışta ticari bir kaygı olarak görülebilir. Ancak 5G otobanında bir ülkenin ürettiği verinin bir merkeze depolanması ve YZ teknolojisi ile değerlendirilebilmesinin çok önemli bir bilgi ve istihbarat kaynağı haline gelebileceği dikkate alındığında konunun önemi ortaya çıkmaktadır.

Bu çerçevede herhangi bir aktör, ulus-devlet olabilir veya bir terörist örgüt, elde edilen bu BV'nin uygun YZ algoritması kullanarak rakiplere göre çok daha hızlı durumsal farkındalığı oluşturabilir, geleceğe yönelik isabetli tahminde bulunabilir, netice olarak çok daha iyi karar verebilir. BV ve YZ teknolojisi insan gözünün çok daha uzakları görmesini sağlayan dürbüne benzetilebilir. Dürbün gözümüzü kuvvetlendirirken, BV ve YZ teknolojisi beynimizi çok daha güçlendirdiği ifade edilebilir. Beynimizin çok daha hızlı çalışması her konuda çok daha etkin olmamızı sağlayacaktır. Bu imkân ve kabiliyetin rakip veya terörist örgütün elinde olması, hedef aldığı kitlelere sızmasını, verileri çalmasını ve zayıf tarafları istismar etmesini sağlayacaktır. Birey, toplum, kritik altyapı gibi kritik hususların hassas taraflarının tespit edilmesi ve istismar edilmesinin güvenlik açısından önemli sonuçları olacaktır.

Doğal olarak bu imkân ve kabiliyet güvenlik stratejisi tasarımında ve icrasında çok büyük bir avantaj olarak karşımıza çıkmaktadır.

Toplanan BV'nin nasıl değerlendirilebileceğinin en iyi örnekleri şirketlerin pazarlama stratejilerinde çok belirgin olarak ortaya çıkmaktadır. Vatandaşların internet aracılığı ile satın aldıkları veya arama yaptıkları malların kayıtlarının tutulması, bu kayıtlara göre stokların ve imalatın yönlendirilmesi, hatta hedef kişinin önüne sürekli söz konusu malın reklamının getirilmesi şirket için önemli bir ticari avantaj sağlayabilmektedir. Benzer yaklaşım güvenlik açısından değerlendirildiğinde sosyal medyada tartışılan konular, hizipleşmeler, kutuplaşmalar, vatandaşların yakındıkları konular tespit edilerek; uzaktan, hedef ülkede bulunmaya gerek olmadan istismar edilebilir. Rusya'nın ABD seçimlerini, hatta Brexit'i etkilediği yönündeki iddialar unutulmamalıdır. Bu nedenle bir ülkenin ürettiği veriler günümüzde hayati önemi sahiptir. Bu çerçevede bir ülkenin vatandaşlarının verilerinin depolandığı bilgisayarlar millî güvenlik açısından önemli bir hassasiyet arz etmektedir. Diğer taraftan güvenlik kuvvetlerinin terörist bir örgütün eleman temin sistemini çözmesi ve çökertmesi yine BV ve YZ sayesinde gerçekleşebilir. BV artık dijital çağda petrol kadar değerli bir konuma gelmiştir.

Yalnızca internet değil çeşitli sensörlerden üretilen veriler de oldukça değerlidir. Ülke içerisindeki kameraların görüntüleri, üretilen sinyaller, haberleşme ve benzer şekilde üretilen veriler çok değerli hale gelmiştir. Örneğin görüntülerden vatandaşların, taşıtların nerede oldukları, nereye gittikleri nesne tanıma, yüz tanıma ve davranış tanıma algoritmaları ile tespit edilebilir. Ukrayna tarafından yüz tanıma sisteminin şehirlere sızan Rus askerlerini tespit etmek maksadıyla savaşta kullanıldığını vurgulamakta fayda vardır. Bu millî güvenlik açısından çok iyi sonuçlar verebilirken, özgürlük-güvenlik dengesinin dikkate alınması hayati önemi haizdir.

BV ve YZ konusunu iyi kullanan bir ulus-devlet ekonomi, bilim, sağlık, eğitim, kısacası hayatın her alanında rakiplerine göre çok süratli ilerleyebilecektir. Toplanan verilerin diğer aktörlere göre çok daha süratli değerlendirilebilmesi bilimsel anlamda normalden daha erken sonuçların elde edilmesini sağlayabilecektir. Doğal olarak söz konusu ulus-devletin halkının refahını sağlaması çok daha kolay ve hızlı olabilecektir.

Halen dar YZ üzerinde çalışılabilmektedir. Gelişen teknoloji sayesinde genel ve hatta süper YZ'nin her alanda çok daha önemli sonuçları ve avantajları olabilecektir. Bu nedenle günümüzde teknolojik üstünlük önemli bir kuvvet çarpanı haline gelmiştir.

Her alanda kullanılan bu imkân ve kabiliyetin silah sistemlerinde de kullanılabileceği unutulmamalıdır. Örnek olarak YZ, topçunun çok daha sıhhatli ve isabetli atış yapmasını sağlarken, güdüm sistemlerinin etkinliğini artırabilir. Elektronik harp ve siber saldırıların icrasını ve tespitini çok daha yüksek doğruluk ve etkinlikle yapabilir. Bu nedenle eskiden orduların güçleri personel, silah sayısı gibi parametreler ile ölçülürken; dijital çağda orduların gücü BV toplama, analiz etme, ağ oluşturma, algoritma kullanma gibi yeni parametreler ile ölçülmek zorunda kalacaktır. Benzer yaklaşım, ekonomi, sağlık, bilim gibi alanlar için de geçerli olabilecektir.

Buraya kadar örnek verilen hususlar ülkelerin niçin BV ve YZ konusunu bir millî güvenlik meselesi olarak gördüklerini açıklamaktadır. Bu nedenle ülkelerin YZ stratejisi hazırlayıp uygulamaya koydukları, çok ciddi bir şekilde takip ettikleri, bir YZ eko sistemi oluşturmaya çalıştıkları görülmektedir. Özet olarak BV ve YZ konusundaki gelişmeler yeni bir dünya düzenini, güvenlik sistemini işaret etmektedir.

BV ve YZ'nin hayatın her alanında olduğu gibi güvenlik stratejisi tasarımına önemli etkileri bulunmaktadır. Diğer teknolojik gelişmelere göre BV ve YZ'nin güvenlik stratejisi tasarımı sürecinin her safhasını etkileme özelliği bulunmaktadır. Söz konusu etkilerin Şekil 1.3'te belirtilen klasik güvenlik strateji sürecinin yanında; tasarlanan stratejinin yönetilmesine de etki etmesi doğaldır. Bu çerçevede süreç analizi esas alınarak sürecin her bir safhasında ve stratejinin yönetilmesine olan etkiler incelenmeye çalışılacaktır. İncelemeyi müteakip ortaya çıkacak sonuçlar; dijital çağa uygun bir süreç, tasarım ve yönetim modeli önerilmesinde kullanılabilecektir.

2.4.1.1. Durum Tespitinde BV ve YZ

Strateji uzmanları etkin bir güvenlik stratejisi tasarlayabilmek amacıyla durum tespitinde kullanabilmek maksadıyla stratejik seviye veriye ve istihbarata ihtiyaç duyacaklardır. Bu veriyi üç başlık altında toplayabiliriz. Bunlar genel veri bankası, cari durum veri bankası, konuya özel veri bankasıdır. Dijital çağda üç veri bankasındaki bilgilerin stratejik seviyede, BV ve YZ kullanılarak hazırlanması gerekmektedir. Stratejik seviye bilgilerin oldukça uzun bir zamanda hazırlandığı, değerlendirilebildiği, kullanılabilir hale getirilebildiği sürekli göz önünde bulundurulmalıdır. Dünya, bir dizi gerçek olayın yer aldığı bir ortam olarak algılanabilir. Her üç veri bankasında dünya üzerindeki gerçek olaylar dijital hale

dönüştürülerek bir anlamda dijital veya sanal bir dünya yaratılması söz konusu olabilecektir. Böyle bir ortamda veriler uygun şekilde oluşturulmalı, depolanmalı, ulaşılabilmeli, paylaşılabilmeli, filtre edilebilmeli ve güncellenmelidir. En önemli sorun kaynağı, bu sanal dünyanın veya dünyaların temelini oluşturan BV'nin zamanında doğru olarak güncellenmesi olacaktır. Bunun yanında siber saldırılardan bu veri bankalarının korunması gerekmektedir.

Genel veri bankası ilgi ve etki sahamızdaki coğrafi bölgeler ve konulara yönelik olarak hazırlanabilirler. Burada depolanacak bilgiler değişik kaynaklardan elde edilebilir. Bunlar gelen değişik istihbarat raporları, açık kaynak istihbaratı, internet ve medya analizleri gibi kaynaklardan gelebilir. Bu raporların veya dokümanların hazırlanabilmesi maksadıyla amacımızın ve ilgi alanımızın belirlenmesi gerekmektedir. Bu veri bankasının güvenlik stratejisi tasarlanabilecek bilgilerin süratle elde edilebilmesi maksadıyla sürekli güncel tutulması, istenildiği zaman faydalı bilginin elde edilebilecek şekilde tasarlanması gerekmektedir. Bu veri bankasındaki verilerin bir genel stratejik durum haritası veya dashboard haline dönüştürülmesi oldukça faydalı olabilecektir. Genel veri bankasında yalnızca hedef aktörlere veya coğrafi bölgeye yönelik bilgiler değil aynı zamanda kendi durumumuza yönelik bilgiler de olmalıdır. Bu çerçevede millî güç unsurlarının durumlarını kapsayan bilgilerin uygun şekilde depolanması gerekmektedir. Güvenlik strateji tasarımı ve yönetimi maksadıyla kullanılabilecek bir genel veri bankası modeli bu çalışmada Şekil 2.3'te önerilmektedir. Geçici veya cari durum veri bankası bir haftalık veya ihtiyaca göre ayarlanabilir. Bu veri bankasındaki bilgilerin cari durumu yansıtacak şekilde dashboard olarak görselleştirmesi yapılabilir. Elde edilen verilerin terörizm, EYP, siber güvenlik, bilgi harekâtı gibi konulara göre sınıflandırılması ile konuya özel veri bankaları oluşturulabilir. Elde mevcut teknolojilerle akan verinin temizlenmesi, kontrol edilebilmesi, sınıflandırılabilmesi ve bunun sürekli yapılabilmesi önemli bir problem alanını teşkil etmektedir. Teknolojinin gelişmesiyle önemli bir ilerleme olabilecektir.

Durum tespitindeki en önemli hususlardan birisi millî menfaatlerin referansında tehdit, fırsat, zayıf ve kuvvetli taraflarımızın belirlenebilmesi olduğunu tekrar vurgulamak gerekir. Millî menfaatlerin önem derecesine göre sınıflandırılmasını müteakip, millî menfaatlere tehdit veya geliştirilmesi için fırsat olup olmadığına karar verilmesi gerekmektedir. Daha önceki bölümde tehdit = niyet x imkân ve kabiliyet

olarak belirtilmiştir. Herhangi bir aktörün niyetinin belirlenebilmesi için liderlerinin güvenlikleştirmeye yönelik söylemlerinin analizi, millî güç unsurlarını konumlandırma ve kullanma durumu gibi parametreler dikkate alınabilir. Liderlerin basındaki beyanatları, gelen istihbarat Doğal Dil İşleme yöntemi ile YZ'den faydalanılarak incelenebilir ve kullanışlı bilgi haline getirilebilir. Ayrıca güvenirliği ispatlanmış bazı kuruluşların yayımladıkları sayısal veriler kullanılarak imkân ve kabiliyetlerin sayısal olarak belirlenmesi gerçekleştirilebilir. Hem niyetin hem de imkân ve kabiliyetlerin bu şekilde sayısal hale getirilmesi neticesinde karar vericilere tehdit değerlendirmesi olarak sayısal bir ölçü sunulabilir.

Durum tespitinde kullanılan diğer bir yöntem ise sistem analizidir. Mühendisler BV ve YZ kullanarak tasarlayacakları sistemin dijital ikizini yaratmakta ve tasarımı bu çerçevede yönlendirebilmektedir. Akıllı şehirlerin komuta kontrol odalarında benzer yöntem kullanılmaktadır. Bir uçak tasarlanacaksa uçağın alt sistemlerinin davranışları YZ algoritmaları ile modellenebilmekte, alt sistemlerin bir araya getirilmesiyle sanal olarak, dijital ortamda uçak oluşturulabilmektedir. Yine akıllı şehirlerde trafik, hava durumu, hastanelerin durumu gibi veriler sensörler vasıtasıyla toplanabilmekte ve şehir modeli yaratılmaktadır. Benzer şekilde güvenlik stratejisinin hedef aldığı aktörün bir sanal modeli oluşturulabilir. Eğer hedef aktör bir devlet ise millî güç unsurları dikkate alınarak bir sanal model oluşturulabilir. Bu çerçevede Şekil 1.4'te belirtildiği gibi ekonomi, politika, altyapı, bilgi altyapısı gibi alt sistemler ve bu sistemler arasındaki ilişkiler esas alınarak bir sanal model geliştirilebilir. Bu maksatla toplanacak BV, YZ ile işleme tabi tutularak hangi durumlarda ne tepkiler verilmekte tespit edilebilir. Benzer yaklaşımın davranış bilimcileri tarafından kullanıldığı unutulmamalıdır. Artık insanların davranışları hakkında bilgi toplamak çok daha kolaydır. Birçok firma, bu yöntemle pazarlama stratejilerini çok daha etkin hale getirebilmektedir.

2.4.1.2. Nihai Hedefin Belirlenmesinde BV ve YZ

Durum tespitinden elde edilen en önemli hususlardan birisi millî hak ve menfaatler çerçevesinde tehdit veya fırsatların zamanında, doğru olarak belirlenebilmesidir. Müteakiben tehdidin ortadan kaldırılması ve fırsatın kullanılabilmesi maksadıyla nihai hedefin veya hedeflerin belirlenebilmesidir. Bu çerçevede BV ve YZ nihai hedefin doğru belirlenmesine yardımcı olabilir.

Nihai hedefin doğru belirlenmesinde dikkate alınması gereken faktörlerden bazıları; tehdidi etkisiz hale getirebilmesi, fırsatın kullanılması ve millî menfaatin pekiştirilmesini veya geliştirilmesini sağlaması, millîi güç unsurları tarafından etki altına alınabilmesi gibi hususlardır. Burada önemli olan hususlardan birisi tehdit veya fırsatın BV ve YZ kullanılarak zamanında hissedilebilmesi ve somut olarak ortaya konulmasıdır.

Bazı kriterler kullanılarak hedef seçimine karar verilebilir. Ancak doğru hedefin seçilip seçilmediğine karar vermek oldukça zordur. Bu maksatla stratejik seviye oyunlama, modelleme, masa başı tatbikatı gibi yöntemlere başvurulabilir. BV ve YZ kullanarak bilgisayar destekli olarak veya dijital ikizler (sanal modeller) oluşturularak karar vericilerin daha sağlıklı kararlar vermesi sağlanabilir. Bu çerçevede kullanılabilecek önemli bir yaklaşım sistem dinamikleri yaklaşımı olabilir. Sistem dinamikleri yaklaşımının BV ve YZ ile birlikte kullanılarak etkinliği arttırılabilir. Sistem dinamikleri yaklaşımı ile güvenlik stratejisi tasarımında üzerinde çalışılan aktör, aktörler veya sistem sanal olarak modellenebilir. Modelin oluşturulması aşamasında bile tasarımcılar üzerinde çalışılan sistem üzerinde çok önemli bilgiler elde edebilir. Oluşturulan model yalnızca tasarım esnasında değil icra esnasında da bir durum haritası, satranç tahtası olarak kullanılabilir. Bu sayede gelişmelere ve elde edilen verilere göre sistemin yenilenmesi, mevcut duruma uyarlanabilmesi sağlanabilir. Ancak kurulan sistemin oldukça basit, yönetiminin kolay olmasına özel dikkat sarf edilmelidir. Aksi takdirde güvenlik stratejisi tasarımının başarıya ulaşması, hedeflere ulaşılması yerine model üzerinde gereksiz emek sarfı tasarımın başarısını engelleyebilecektir. Aslında dijital çağda bu yalnızca nihai hedefin tespiti için değil güvenlik stratejisi tasarımının başından sonuna kadar kullanılması gereken bir yöntemdir. Bu hususa güvenlik stratejisi tasarım sürecine yeni bir model önerilmesi safhasında tekrar geriye dönülecektir.

Nihai hedefin başlangıçta doğru tespit edilmesinin yanında, hedefe ulaşılıp ulaşılmadığına karar verilmesi de oldukça zordur. Dijital çağda belirsizliklerin artması neticesinde bu konu daha da önem kazanmıştır. Bunun yanında hedefe ulaşılsa bile istenen sonucu veya etkiyi üretmesinde, yani tehdidi etkisiz hale getirmede, fırsatı değerlendirmede beklenen olmayabilir. Bu nedenle nihai hedefe ulaşıldığının ve istenen sonucun veya etkinin ortaya çıktığının sayısal olarak değerlendirmesini sağlayacak rakamsal değerler belirlenebilir. Bu rakamsal değerlerin zamanında rapor

olarak, yani BV olarak elde edilmesi ve YZ ile değerlendirilebilmesi maksadıyla bir model oluşturulabilmelidir.

2.4.1.3. Millî Güç Unsurları, Araç ve Kaynakların Kullanımında BV ve YZ

Yalnızca hedef aktörün veya devletin durumunun takip edilmesi güvenlik stratejisinin başarısı için yeterli değildir. Aynı zamanda kendi millî güç unsurlarımızın durumlarının da sürekli takip edilmesi ve değerlendirilmesi başarı için şarttır. Daha önce belirtildiği gibi bunun rakamsal değerler çerçevesinde BV ve YZ kullanılarak takip edilmesi sağlanabilir.

Ancak bu yeterli değildir. BV ve YZ'den en iyi şekilde faydalanabilmek maksadıyla dijital çağa uygun, gerekli kurumların ve teşkillerin kurulması, eko sisteminin oluşturulması uygun olacaktır. Bu maksatla Dijital Dönüşüm Başkanlığı, Veri Yönetim Başkanlığı gibi kuruluşlar oluşturulabilir. Eğitim alanında da gerekli tedbirlerin alınması insan kaynağının oluşturulması ve demografik güç unsurunun şekillendirilmesi için hayati önemi haizdir. Dijital çağda farkına tam olarak varılmasa bile bu kurum ve kuruluşlar millî güç unsurlarının etkinliğinin arttırılmasında bir kuvvet çarpanı olmasının yanında, yeni ve etkin bir millî güç unsuru olarak karşımıza çıkacaktır.

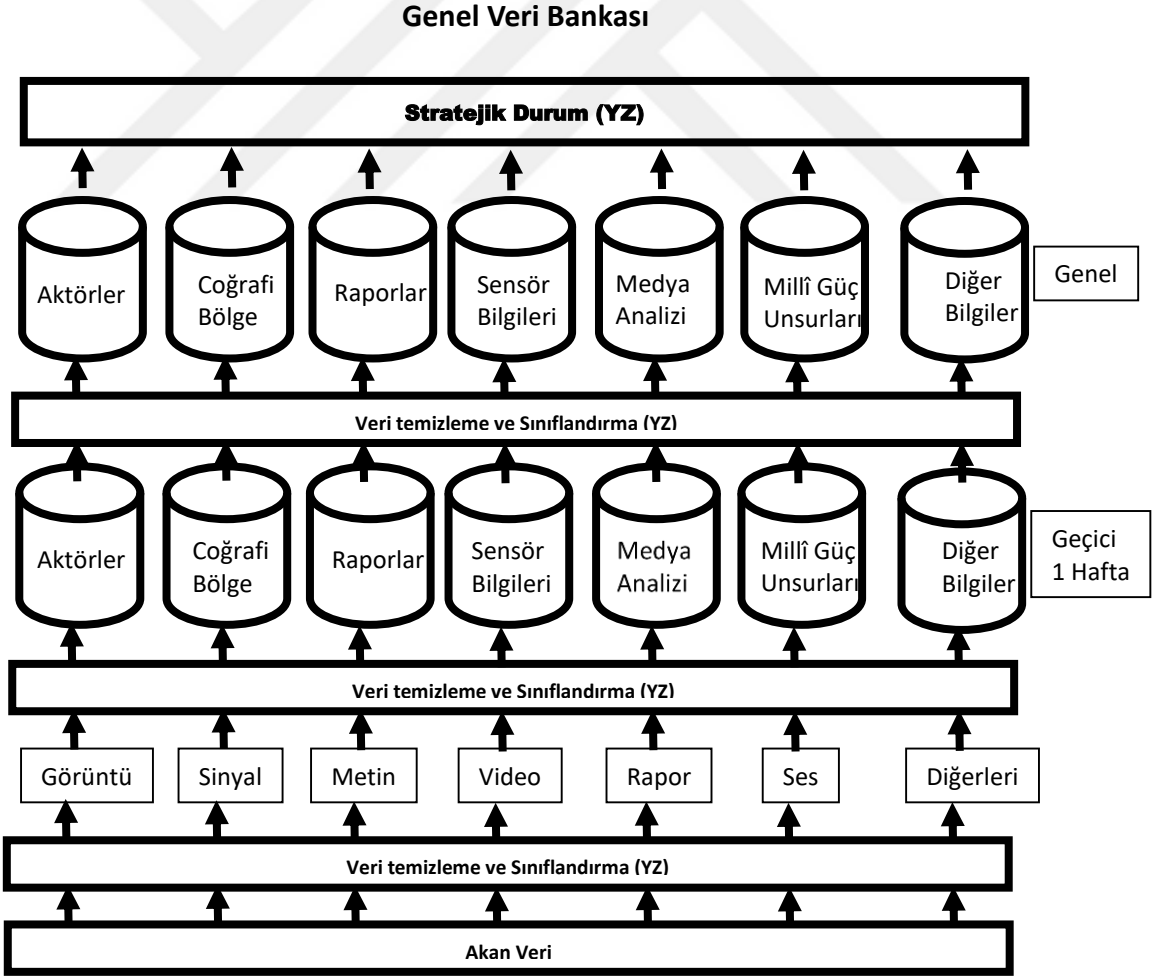
Bu modeldeki en önemli hususlardan birisi elde edilen verilerin stratejik durumu yansıtacak hale getirilmesi veya verinin görselleştirilmesidir. Akan verinin değişik YZ modelleri kullanılarak stratejik durum haritası haline getirilmesi, yani verinin görselleştirilmesi, karar vericiler tarafından anlaşılır hale getirilmesi bir örnek olarak Şekil 2.4'te gösterilmiştir. Şekil 2.4'te önemli örgütlere ayrı bir bölüm açılabilir veya açılmayabilir. Bunu mevcut stratejik durum belirleyebilecektir. BM, NATO, AB gibi örgütlerin küresel ve bölgesel anlamda stratejik etkileri olabilmektedir. Örneğin BM'nin aldığı kararların göz önünde bulundurulması, takip edilmesi stratejik faaliyetlerin uluslararası ortamda meşruiyeti sağlamada önemli bir etkisi olabilecektir. Benzer yaklaşım diğer örgütler için farklı şekillerde göz önüne alınabilir.

2.4.1.4. Konsept Oluşturulmasında BV ve YZ

Daha önce incelendiği gibi konsept oluşturmanın temel amacı nihai hedefe ulaşmak maksadıyla millî güç unsurlarının nasıl kullanılabileceğinin ortaya konulmasıdır. Konsept oluşturma aşamasında hangi hedefe hangi millî güç unsurunun tahsis edileceği, hedeflere öncelik verilmesi, safhaların belirlenmesi gibi bazı önemli kararların verilmesi gerekmektedir. Bunun yanında direkt mi dolaylı mı bir yaklaşım sergileneceği gibi değişik hal tarzlarına yönelik kararların verilmesi gerekmektedir.

Bu kararların verilmesinde yine sanal bir model yaratılması ve bu model üzerinde bu kararların verilmesi çok faydalı olabilir. Ancak güvenlik stratejisi bağlamında sanal bir modelin yaratılmasının mühendislik alanında kullanılan diğer sanal modellere göre oldukça zor olduğu unutulmamalıdır.

Şekil 2.3: Genel Veri Bankası



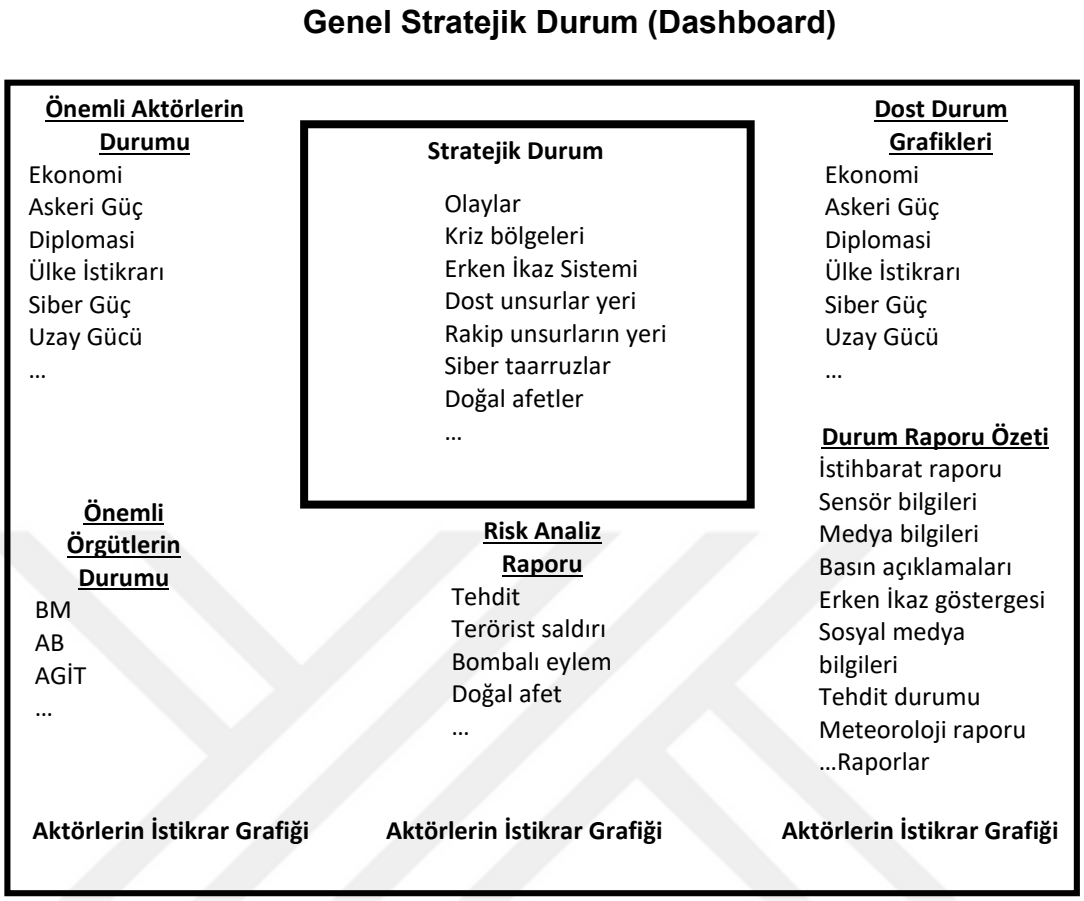
Kaynak: Yazar tarafından oluşturulmuştur.

2.4.1.5. Risk Yönetiminde BV ve YZ

Daha önce incelendiği gibi güvenlik stratejisi tasarlamada kullanılan risk yönetimindeki en önemli hususlardan birisi nihai hedef, millî güç unsurları ve konsept arasında bir uyum olup olmadığının belirlenmesi, takip edilmesi ve gerekli tedbirlerin alınmasıdır (Şekil 1.8). Sanal modelleme yine burada fayda sağlayabilir. Bu maksatla müteakip bölümlerde ayrı bir inceleme yapılacaktır.

Maliyet risk yönetiminde diğer önemli bir konudur. İnsan kaynağı, mali kaynaklar gibi kaynakların harcanması ile elde edilen faydanın sürekli sorgulanması gerekmektedir. Diğer bir ifadeyle elde edilen nihai hedef ile harcanan kaynak arasındaki sorgulamanın yapılması hayati önemi haizdir. Bu anlamda kaynakların harcanma seviyesinin tespiti BV kullanarak yapılabilirken, faydanın belirlenebilmesi için matematiki modeller kullanabilir. Bu matematiki modellerin YZ aracılığı ile BV ile birlikte kullanımı sağlanabilir.

Şekil 2.4: Genel Stratejik Durum (Dashboard).



Kaynak: Yazar tarafından oluşturulmuştur.

2.4.2. İnternet, Sosyal Medya, Metaverse, Nesnelerin İnternetinin Güvenlik Stratejilerinin Tasarımına Etkisi

2.4.2.1. Genel

Dijital çağda BV ve YZ'den sonra güvenlik stratejisi tasarımına etkisi olabilecek en önemli teknolojik gelişmelerden birisi internet ve internete bağlı olarak ortaya çıkmış olan teknolojilerdir. Hayatımızın bir parçası haline gelmiş olan internetin güvenlik alanına yansımalarının olması oldukça doğaldır. Bu yansımaların tespit edilip zamanında tedbir alınabilmesi millî güvenliğin sağlanmasında önemli bir rol oynayabilecektir.

İnternetin sayısız faydası olmakla birlikte, güvenlik açısından bakıldığında önemli tehditleri barındırdığı da unutulmamalıdır. Yasadışı veya terörist örgütlerin interneti eleman temin etmek, yasa dışı faaliyetlerinin etkinliğini arttırmak ve

ideolojilerini yaymak gibi maksatlarla kullandıkları bilinmektedir. Bu örgütler özellikle sosyal medya sitelerini kullanarak internet aracılığı ile sempatizan yaratabilmekte ve bu sempatizanlardan bazılarını kendi saflarına katabilmektedir. Yine bu örgütlerin elemanlarına internet aracılığı ile talimatlar gönderdikleri, hatta başta bomba imali olmak üzere değişik konularda eğitim verdikleri bilinmektedir. Bu sayede Afganistan'da konuşlu bir örgüt ABD'de yaşayan bir elemanına talimatlar gönderebilmekte, tek başına eylem yaptırabilmektedir. Terör örgütleri yaptıkları eylemin videolarını internette yayımlayarak çok daha geniş kitlelere şiddeti, terörü yayabilmektedirler.

Ulus-devletler açısından bakıldığında ise dijital çağda internet aracılığı ile hedef ülkenin halkına çok kolay erişilebildiği, algının yönetilebildiği görülmektedir. Bir savaşın nihai hedefi, hedef ülkenin halkının savaşma azim ve kararlılığını yok etmek olduğunda, internet paha biçilmez bir imkân sağlamaktadır. Hatta bunun için devletlerin birbirlerine savaş ilan etmelerine bile gerek kalmamıştır. Dolayısı ile hedef devletlerin kendilerine yönelik internet ortamında savaş başlatıldığını tespit edebilmesi de oldukça zordur. Bu çerçevede hedef ülkenin kültür kodlarını değiştirmeye yönelik bir çalışma başlatıldığında, kültür kodlarının temel unsuru olan memikleri değiştirmeye yönelik bir faaliyet bu çerçevede değerlendirilebilir. Bu faaliyete memik savaşı da denilmektedir. Memik jenerasyondan jenerasyona iletilen, bir toplumun kültür kodunu veya DNA'sını oluşturan birimlerdir. Bunların değiştirilmesi toplumun kültürü üzerinde önemli değişikliklere neden olabilmektedir. İnternet bu maksatla önemli bir ortam sunmaktadır.

Ülkelerin vatandaşlarının dijital çağda internette ikinci bir kimlikleri veya dijital vatandaşlıkları oluşturulmaktadır. Örneğin Twittera üye olan bir kişinin, şirket tarafından bir profili veya vatandaşlığı oluşturulmaktadır. Bu kimlikle söz konusu hesaba ulaşabilmekte, tanınmakta, işlem yapabilmektedir. Daha da önemlisi vatandaş bu ortamda kendi devletinin değil şirketin koyduğu kurallara tabidir. Sosyal medya ortamında iftiralar, asılsız haberler yayılabilmekte, planlı olarak kişiler hedef alınarak kimlik suikastları yapılabilmektedir. Bu maksatla hedef olarak belirlenen kişi hakkında hazırlanan bir iftira aynı anda birçok hesaptan veya bot (robot hesap) kullanarak yayılmaktadır. Bilinçsiz insanlar farklı hesaplardan aynı bilgi geldiği için, sorgulama gereği hissetmeden iftiraları bile doğru olarak kabul etmektedirler. Kişilik hakları çiğnenmekte, ulus-devletin egemenliği bu ortamda geçerli olmamaktadır. Bu

hem birey güvenliğine hem de ulus-devletin güvenliğine olumsuz yansımakta, devletin otoritesi sorgulanmaktadır. Kişilerin bu ortamlarda kullandıkları kişisel bilgilerinin çalınması ise birey güvenliği için çok daha vahim sonuçlar doğurabilmektedir.

İnternetin insan hayatının bir parçası olmasıyla kara, deniz ve havaya ilave olarak siber alan bir savaş ortamı olarak nitelendirilmeye başlanmıştır. Hackerlerin bankalar, devletin değişik hizmetleri gibi alanlara internet ortamında saldırılar yapmaları siber savunmayı gündeme getirmiştir. Siber saldırılar yalnızca internet ile kalmamış, bütün dijital sistemleri hedef almaya başlamıştır. Ulus-devletler siber savunma komutanlıkları ve stratejileri oluşturmak zorunda kalmışlardır. NATO tarafından siber alanda icra edilen bir saldırının savaş nedeni olabileceği ve topyekûn savunma kararı alınabileceğini kabul etmiştir. Ulus-devletlerin toplumlarının internete bağımlılığının artması, birçok hizmetin internet ortamında verilmesi, elektrik, bankacılık gibi kritik alt yapıların siber ortamda saldırıya açık hale gelmesi devletler için önemli bir güvenlik problemi oluşturmaktadır. Siber savunmayı dikkate almadan dijital çağda güvenlik sağlanamayacağı kabul edilen bir gerçek haline gelmiştir.

İnternet yalnızca haberleşme değil aynı zamanda değişik algılayıcılardan gelen bilgilerin iletilmesi, akıllı evler, şehirler gibi ortamlarda kullanılan cihazların kontrol edilebildiği bir ortam da sunmaktadır. Bu ortama genel olarak nesnelerin interneti adı verilirken, siber saldırılar aracılığı ile bu ortamın hedef alınması önemli bir tehdit oluşmasına neden olmaktadır. Güvenliğin nasıl sağlanacağı önemli bir sorun olarak karşımıza çıkmaktadır.

Güvenlik yaklaşımlarında en önemli konulardan birisi bir önceki bölümde açıklandığı gibi mülkün korunması olduğu bilinmektedir. Dijital çağda sosyal medyada gönderilen mesajlar, oluşturulan web sayfaları birer mülk olarak değerlendirilerek korunması gerekmektedir. Ancak bu korunmanın devlet yerine şirketler aracılığı ile yapılması yine ulus-devletlerin egemenliklerini olumsuz etkileyen hususlardan birisi olmaktadır. İnternette oluşan bu varlıkların miras bırakılması konusunun gündeme gelmesi ise durumu daha da karmaşık hale getirmektedir.

Metaverse sayesinde sanal dünyaların yaratılması internet kullanımı nedeniyle ortaya çıkan problem sahalarının daha derinleşmesine neden olabilecektir. Metaverse sayesinde insanlar oluşturdukları avatarları ile sanal dünyada alışveriş yapabilecek, varlık satın alabilecek, ziyaretler yapabilecek, konserler gibi eğlencelere katılabilecek,

sanal para veya bitcoin ile ödeme yapabilecektir. Yaratılan sanal dünyanın kanunlarını ise söz konusu dünyayı yaratan şirketler koyabilecektir. Örneğin dolandırıcılık, taciz, terör gibi suçlar oluştuğunda nasıl müdahale edilip adaletin sağlanacağı oldukça önemli soru işaretleri oluşturmaktadır. Ulus-devletlerin sanal arsalar gibi varlıkları nasıl koruyabilecekleri veya oluşturulan sanal dünyaya teröristler tarafından sızılmasını nasıl engelleyebilecekleri, hangi teröristlerin özgürlük savaşçısı olarak kabul edilebileceği konuları ise bu soru işaretlerini daha da zorlaştırmaktadır. Sanal ortam ile gerçek yaşama veya tam tersi olan suç geçişlerinin nasıl değerlendirileceği ise önemli bir sınama oluşturabilecektir.

İnternette oluşturulan sanal dünyada yaratılan yeni gerçekliklerin dünyadaki gerçek hayata yansımaları oldukça olumsuz olabilecektir. Para kullanımı, kanunlar, kurallar gibi yeryüzünde yaratılmış olan gerçekliklerin etkinlikleri internette oluşturulan sanal gerçeklikler ile sınamaya tabi tutulmaktadır. Metaverse bunu daha da derinleştirebilecektir. Metaverse çerçevesinde oluşturulan yeryüzünde toprağı olmayan, sınırları belirli olmayan, ancak belirli bir topluma hitap edebilen, dijital vatandaşlık verebilen, bazı simgeleri kullanarak sivil bir din oluşturabilen sanal ortamlar ulus-devlet anlayışını olumsuz etkileyebilecektir. Bu ortamlarda sanal gerçeklik, artırılmış gerçeklik ve karma gerçeklik teknolojileri ile oluşturulan sanal ortamlarda yeryüzündeki gibi hareket etmek, olumsuzluğun boyutlarını çok daha derinleştirebilecektir. Bu sanal ortamın dış ve iç güvenliği nasıl sağlanabilecektir? Kolluk kuvvetleri nasıl çalışacaktır? Adalet nasıl sağlanabilecektir? Diğer sanal âlemlerden gelen saldırılar nasıl engellenebilecektir? Bu ve benzeri sorular gelecekte güvenlik kurumlarının karşılaşması muhtemel potansiyel sorunlar olarak karşımıza çıkacaktır.

İnsanların sanal ortamlardan yeryüzündeki gerçek şartlara uyum sağlaması ve tekrar sanal ortama uyum sağlaması insan beynini, duygularını, psikolojisini olukça fazla etkileyecektir. Bu çerçevede gerçek dünyada yansımaları olabilecek yeni sağlık sorunları, tehditler, güvenlik sorunları gibi önemli konular üzerinde ulus-devletler çalışmak zorunda kalacaklardır.

Aslında günümüzde dijital çağda benzer sıkıntılar yaşanmaya başlamıştır. İnternet kullanımı nedeniyle “post truth” ortamın yaratıldığı bilinmektedir. “post truth” terimi ilk olarak 2016 yılında ABD seçimleriyle birlikte gündeme gelmiştir. “post truth” basit olarak sahte haber veya bilgi olarak açıklanabilir. Ancak sosyolojik

açıdan çok daha köklü bir sorun olarak karşımıza çıkmaktadır. İnsanlar dijital çağda gerçeği bilmelerine rağmen manipüle edilmiş, çarpıtılmış bilgiyi duymak istemektedirler. Buna en güzel örnek futbol takımları veya siyasal partilerin taraftarlarının gerçek farklı olmasına rağmen kendi takımlarının veya partilerinin söylemlerini kabul etmeleri ve kutuplaşmaları verilebilir. Küme düşmek üzere olan bir takımın taraftarlarının hala iyi bir takım olduklarını ifade etmeleri örneği daha da pekiştirebilir. Diğer bir ifadeyle insanlar yalanla, yani sanal bir gerçeklikte yaşamayı tercih etmektedirler. Gelinen aşamada dijital çağda insanlar ilk gördüklerine inanmakta, oluşan önyargı nedeniyle sorgulama ihtiyacı hissetmemektedir. Böyle bir ortamda bilginin doğruluğunu ispat etmek okuyucuya düşmektedir. "Deepfake" (derin sahte), "voice cloning" (ses klonlama) gibi yöntemler ile çok daha büyük sahtekârlıklar "post truth" ortamın çok daha etkin olmasına neden olmaktadır.

Terörist örgütlerin böyle bir ortamdan etkilenmemeleri imkânsızdır. Bu çerçevede teröristlerin elde ettikleri verileri "post truth" ortamın bilinçaltındaki önyargıları ile değerlendirmeleri ve bu çerçevede terör eylemleri gerçekleştirmeleri mümkündür. Örnek olarak terör örgütünün hedef kişiye veya topluma yönelik, davranışlar ve söylemleri esas alan verileri "post truth" ortamın önyargısı ile değerlendirmesi; gerçek farklı olmasına rağmen, davranışların veya söylemlerin kendileri açısından olumsuz olduğu sonucuna varması ve masum insanları öldürmesi yeni bir terör motivasyonu şekli olan, veri terörü (data terrorism, data abuse) olarak, yeni bir ifadeyle kavramsal olarak açıklanabilir.

Böyle bir ortamda kolluk kuvvetleri yeni yöntemlere başvurmak durumunda kalmışlardır. "Computer Forensics" (adli bilişim) bu yöntemlerden birisidir. Yapılan bütün işlemlerin bilgisayar ortamında iz bıraktığı bilindiğinden bu izlerin tespit edilip adli yargılamalarda kullanılması için hazırlanması yeni bir meslek olarak karşımıza çıkmaktadır. Yine kolluk kuvvetleri tarafından sanal devriyelerin oluşturulması, sosyal medyada yapılan hakaretler konusunda bilgi toplamaları dijital çağın güvenliğin sağlanması çerçevesinde ortaya çıkarttığı kolluk hizmetleridir.

Dış güvenlik açısından ise diğer ulus-devletler veya teröristler tarafından yapılan değişik şekillerdeki saldırılara karşı tedbir alınması gerekmektedir. Bu saldırılar kültürel saldırılar, bilgi harekâtı çerçevesinde yapılan saldırılar veya siber saldırılar gibi değişik şekillerde olabilir. Bunların tespiti ve bu tehditler ile mücadele oldukça

zordur. Bu maksatla özel birimler kurulmalı ve başta YZ olmak üzere teknolojik yöntemler kullanılmalıdır.

Kolluk kuvvetleri internetin güvenliğe olumsuz etkilerini azaltmak için daha değişik ve yaratıcı yöntemlere de başvurmaktadır. Bu çerçevede kolluk kuvvetleri dijital çağda yalnızca şehirlerin sokaklarında, caddelerinde değil aynı zamanda siber ortamda da devriye gezmeye başlamışlardır. Aynı şekilde terör örgütlerinin faaliyetlerini takip etmek için internet ve sosyal medya ortamının izlenmesi, terör örgütlerine bu ortamlar kullanılarak sızılabilmesi, eleman temin etme sistemlerinin tespit edilmesi yeni taktikler olarak karşımıza çıkmaktadır. Kolluk kuvvetlerinin dijital çağın farkına varılması zor olan tehditlerini tespit etmeleri ve yaratıcı yöntemler ile çözümler üretmeleri güvenliğin sağlanmasında önemli bir faktör olarak karşımıza çıkmaktadır.

İnternetin ortaya çıkarttığı diğer bir husus ise ülkelerin vatandaşlarına ulaşabilmek, iletişim kurmak, ticaret yapmak için sınırları ortadan kaldırmış olmasıdır. Daha önce belirtildiği gibi savaşların sonlandırılması için kullanılan nihai hedeflerden en etkili olanı hedef ülkenin halkının savaşma azim ve iradesinin kırılmasıdır. Bu maksatla ülkeye bizzat gidilmesine gerek kalmamıştır. İnternet aracılığı ile bunun kolaylıkla yapılabilmesinin, savaşların ve mücadelelerin gidişatlarının belirlenebilmesinin önü açılmıştır. Aynı çerçevede ülkenin işgal edilmesi için bizzat ülkenin fiziksel olarak işgal edilmesi yerine internet ve sosyal medya sayesinde hedef ülkenin halkının etki altına alınması, kamuoyunun düşüncelerinin yönlendirilmesi, liderlerin kararlarının istenen istikamette verilmesinin sağlanması yeterli olmaktadır. Sistemlerin heklenmesi yanında bizzat insan beyninin heklenmesi gerçekleşebilmektedir. Bu savaşların ve mücadelelerin yürütülmesinde kullanılan bu yeni yöntemler siber vatan ve siber vatanın güvenliğinin sağlanması konusunu gittikçe daha ağırlıklı olarak gündeme getirmektedir.

Buraya kadar belirtilen konular dikkate alınarak internetin güvenlik açısından uluslararası sistem, ulus-devlet ve birey analiz düzeylerinde ortaya çıkarttığı sonuçlar ortaya konulabilir. Uluslararası sistemi küreselleşme açısından güçlendirdiği, ancak internet şirketlerinin yeni, güçlü aktörler olarak uluslararası sisteme dâhil oldukları ifade edilebilir. Ekonomik açıdan ise küresel sistemin çok daha hızlı işlediği, ülkelerin birbirlerine olan bağımlılıklarının arttığı görülebilir. Ulus-devlet açısından ise egemenliği ve dolayısı ile devleti zayıflattığı belirtilebilir. Bunun tam tersi olarak siber

ortamı iyi anlayan ve değerlendiren ulus-devletlerin bu dezavantajı avantaja çevirebilecekleri dikkate alınmalıdır. Ulus-devletlerin bu mahzurları ortadan kaldırmak maksadıyla yaratıcı tedbirler aldıkları görülmektedir. Birey açısından ise oldukça sıkıntılı sonuçlar ortaya çıkabilir. Bireylerin kişisel verilerinin ele geçirilmesi ve kullanılması birey güvenliğini tehlikeye düşüren önemli bir parametre olarak karşımıza çıkmaktadır. Yine sosyal medya uygulamaları gibi araçlar kullanarak kimlik suikastları yapıldığına çok sık şahit olunmaktadır.

İnternetin ve internet kaynaklı uygulamaları hayatın her alanında olduğu gibi güvenlik stratejisi tasarımına önemli etkileri bulunmaktadır. Söz konusu etkilerin Şekil 1.3'te belirtilen klasik güvenlik strateji sürecinin yanında; tasarlanan stratejinin yönetilmesine de etki etmesi doğaldır. Bu çerçevede yapılan inceleme müteakip maddelerde belirtilmektedir.

2.4.2.2. İnternet ve Diğer Uygulamaların Güvenlik Stratejilerinin Tasarımına ve Yönetimine Olan Etkisi

Bilindiği gibi internet iyi bir açık kaynak istihbarat ortamı sağlamaktadır. Zaten günümüzde istihbaratın önemli bir bölümü açık kaynaktan sağlanabilmektedir. Sosyal medyadaki bir fotoğraf, konum bilgisi, yazılan bir yorum diğer kaynaklar ile teyit edilerek çok şey ifade edebilmektedir. Bu özellikleri ile güvenlik stratejisi tasarım sürecinde durum tespiti safhasından başlamak üzere her safhada, değişik oranlarda internetten istifade edilebilir. Yalnızca durum tespiti değil durumun herkes tarafından aynı şekilde algılanmasını sağlayacak bilgilerin yayımı için de internet gerekli siber güvenlik tedbirleri alınarak kullanılabilir.

Durum tespiti safhasında sosyal medya, değişik web sayfalarından alınan veya sensörlerden gelen bilgiler belirli YZ algoritmaları ile işleme tabi tutularak faydalı bilgi haline getirilebilir. İlave olarak elde edilen bilgiler kullanılarak erken ikaz sistemi kurulabilir. Bu sayede dünyanın değişik yerlerindeki mevcut veya potansiyel güvenlik olayları tespit edilebilir. Ancak stratejik seviyede uzun vadeli olarak olayların veya gelişmelerin tahmin edilmesinde bazı sorunlar yaşanabilir. İnternetten elde edilen bilgilerin tanımlı kaynaklardan gelen istihbarat raporları ve İHA'lar, uydular gibi sensörlerden elde edilen bilgiler ile beraber değerlendirilmesi oldukça kuvvetli bir bilgi kaynağı elde edilmesine neden olabilir. Birleşmiş Milletler, Avrupa Birliği,

Dünya Bankası, Uluslararası Para Fonu, Küresel Ateş gücü gibi değişik kaynaklardan elde edilen bilgiler önemli bilgi kaynakları olarak kullanılabilir. Bununla beraber internette yukarıda belirtildiği gibi kasıtlı veya doğal nedenlerden dolayı doğru bilgiye ulaşmak oldukça güç olabilir. Bu olumsuzluk dikkate alınarak gerekli çalışmaların yapılması gerekmektedir. Ayrıca internetteki bilgilerin daha önce belirtildiği gibi yaklaşık % 80'den fazlasının, süratle kullanımı engelleyecek şekilde yapılandırılmamış olması ayrı bir sorun kaynağı olabilecektir. Buna karşın güncel ve süratle bilginin elde edilebilmesi, karar mekanizmalarının hızlı çalışmasına neden olabilecek ve rakiplere göre önemli bir kuvvet çarpanı olabilecektir.

Güvenlik stratejilerinde nihai hedefin belirlenmesinde tehdit tanımı oldukça önemlidir. Bu aşamada da iyi bir analizci interneti kullanarak herhangi bir konunun tehdit olup olmadığını erkenden tespit edebilir veya teyit edebilir. Nihai hedefe ulaşılıp ulaşılmadığı konusunda yapılacak değerlendirmelerde bilgilerin doğruluğu dikkate alınarak kontrollü olarak internetten faydalanılabilir.

Dijital çağda BV ve YZ ile desteklenen, internet ortamında çalışan, bilgi temin etmeyi amaçlayan programlar kullanılmaya başlanmıştır. Söz konusu programlardan güvenlikle ilgilenen kuruluşların yanında birçok özel firma tarafından da faydalanılmaktadır .Özel şirketler tarafından hazırlanan, BV ve YZ'nin de etkin olarak kullanıldığı bilgisayar programları ve uygulamaları ile internetten etkin olarak açık kaynak istihbaratı toplanabilmektedir. Söz konusu programlar incelendiğinde dünyanın herhangi bir yerinde meydana gelen bir olay tespit edilebilmekte, coğrafi olarak bir harita üzerinde gösterilebilmektedir. Bu olaylardan ilgi alanında olup dikkatimizi çekmesi gerekenler ise erken ikaz sistemi ile bildirilmektedir. Açık kaynak istihbaratı elde etme programları günlük olarak sosyal medyayı, haber ajanslarını, değişik medya kuruluşlarını ve diğer kaynakları takip etmekte, dikkat çekici bilgileri derleyerek kullanıma sunmaktadırlar. Bu kaynaklardan istenen bir dile tercüme yapılabilmekte, farklı dillerde yayımlanan kaynaklardan faydalanılması gerçekleşebilmektedir. Belirli bir süre geçmişe yönelik olaylar kullanılarak eğilim ve pattern analizlerinin yanında belirli bir bölgenin tansiyonunu veya duygu analizini de yapabilmektedir. Herhangi bir ülkenin, şehrin mevcut durumunun değerlendirmesi, gerginlik durumu raporlanabilir. Bu programların teknolojinin gelişmesiyle çok daha etkili olabileceği öngörülebilir. Ancak dezenformasyon ve aldatmaya karşı gerekli tedbirlerin alınması gerekmektedir.

İnternet kullanımı tasarım sürecinin konsept safhasında oldukça önemli bir ortam sağlayabilir. Bu safhada siber savunma ve bilgi harekâtı konsept çalışmalarında kullanılabilecek önemli bir başlık olarak karşımıza çıkmaktadır. Değişik tanımları olmakla beraber siber savunma bilgisayar sistemleri üzerinde etkili olurken, bilgi harekâtı insanların düşüncelerini değiştirmede kullanılan yöntemlerdir. Buna ilave olarak psikolojik harekât ise insanların davranışlarının değiştirilmesi için önem arz etmektedir. Bütün bu savaş yöntemleri için internet çok uygun bir ortam sunmaktadır. Daha önce belirtildiği gibi internetin kuralları, insanların interneti nasıl kullandıkları, internetin algıyı nasıl yönlendirdiği gibi hususlar iyi değerlendirilerek internet ortamı çok iyi kullanılabilir. Bu maksatla daha önce de ifade edildiği gibi hedef ülkeye gidilmesine gerek kalmamıştır.[83]

Siber savaş, bilgi harekâtı, psikolojik savaş gibi yöntemlerin kullanılabilmesi için yeni organizasyonlara, hatta askeri birliklere ihtiyaç duyulmaktadır. Askeri birlik olarak İngiltere'nin 77. Tugayı[84], Çin'in 50 Cent[85] Ordusu örnek verilebilir. Bu birliklerin kuruluşu ve görevleri dijital çağın güvenlik yapılanmasının en iyi örneklerini vermektedir. Ayrıca bu maksatla, değişik ülkeler tarafından troll çiftliklerinin de kullanıldığı bilinmektedir. Aslında bu konu millî güç unsurlarının geliştirilmesi çerçevesinde ele alınabilir. Dijital çağın ihtiyaçlarına göre bu yeni askeri birlikler ve organizasyonlar verilen hedeflere ulaşabilmek maksadıyla etkin bir şekilde kullanılmakta, geliştirilmektedir.[86]

Millî güç unsurlarından dijital çağda en etkin olarak kullanılabilecek güç unsurları siber ve bilgi harekâtı icra edebilen organizasyonlardır. Bu kabiliyetler güvenlik stratejisi tasarımında her zaman dikkate alınması gereken, özel önem verilmesi gereken, sürekli geliştirilmesi gereken bir millî güç unsurudur. Hatta daha da ileriye gidilerek devamlı bir faaliyet olarak icra edilecek şekilde siber savaş stratejisi, bilgi harekâtı stratejisi gibi ayrı stratejilerin hazırlanmasına ihtiyaç duyulmaktadır.

[83]Singer, P.W. ve Brooking, Emerson T, *LikeWar, Weaponization of Social Media*, 2018.
[84]Army.mod.uk, *77th Brigade, Influence and outreach*, 1 Temmuz 2022.
[85]Lau, Joyce, *Who Are the ChineseTrolls of the "50 Cent Army"?,* 2016.
[86]Patrikarakos, David, *War in 140 Characters, How Social Media is Reshaping Conflict in the Twenty-First Century*, 2017.

En son aşamada risk analizi ise yine durum tespit safhasında olduğu gibi internetin, resmi istihbarat raporları, sensör bilgileri gibi veriler beraber kullanarak yapılabilir.

2.4.3. Medyanın Güvenlik Stratejilerinin Tasarımına Etkisi

2.4.3.1. Genel

Medyanın güvenlik konusuna olan önemli etkisi bilinmektedir. Bu çerçevede internet ile mukayese edildiğinde en önemli özellik, verilerin, bilginin kaynağının belirli olmasıdır. Medya bu özelliği ile aktörlerin kendi tutumlarını, değişik konulardaki düşüncelerini paylaşabildikleri, kitleleri kendi görüşleri doğrultusunda ikna edebildikleri önemli bir güç unsuru olarak karşımıza çıkmaktadır.

Medyanın genellikle tarafsız olması beklenmekle birlikte bunun aksine bazı medya kuruluşlarının tarafsızlıklarını yitirdikleri bilinmektedir. Aslında tarafsızlığını kanıtlamış bir medya kuruluşu "post truth" ortamın olumsuzluklarını giderebilecek en önemli unsurlardan birisi olabilmektedir. Ancak değişik aktörlerin medya kuruluşuna sahip olmalarının gerisinde kendi gerçeklerini veya seçilmiş gerçekleri iç ve dış kamuoyu ile paylaşabilmeleri bulunmaktadır. Paylaşımlar ne kadar inandırıcı olursa söz konusu aktörün etkinliği o kadar artabilmektedir.

Reklamlardan elde edilebilen gelirin düşüklüğü dikkate alındığında medya dünyasının reklamlar ile kendisini finansa etmesi neredeyse imkânsızdır. Değişik aktörler değişik nedenlerden dolayı medya kuruluşlarını satın almaya veya medya kuruluşlarına ortak olmaya çalışabilirler. Bu aktörler, devletler, değişik şirketler veya hatta terörist örgütler dahi olabilirler. Dolayısı ile medya kuruluşlarının bazıları bir amaca ulaşmak maksadıyla tasarlanmış, şirketler haline gelmiştir. Bu şirketlerin gelirlerinin büyük bölümünü hangi haberi hangi maksatla yaptıklarına bağlı olabilmektedir. Haberlerde verilen ana mesajlar tespit edilip analiz edildiğinde amaç açığa çıkarılabilmektedir. Hatta bu yöntemle hangi aktörün söz konusu medya kuruluşunu finansa ettiği ortaya çıkarılabilmektedir.

Medyanın özellikle terör örgütleri tarafından kullanılması güvenlik açısından olumsuz sonuçlara neden olabilmektedir. Bazı medya kuruluşlarının terör saldırılarının sonuçlarını bilinçsiz şekilde yayması, hedef kitle veya halk üzerinde terör örgütünün istediğinden çok daha fazla olumsuz etki yaratabilmektedir. Bu çerçevede

etkisi bölgesel çerçevede kalabilecek bir terör eylemi medya aracılığı ile çok süratli olarak küresel olarak yayılabilmektedir. Terör örgütlerinin terör eylemleri yapmalarının gerisinde de zaten asıl düşünce budur. Medya terör örgütünün halkı sindirmek, korkutmak, baskı ve etki altına almak maksadıyla yaptığı bir eylemi tam terör örgütünün istediği şekilde çok daha geniş kitlelere yayabilmektedir. DEAŞ'ın medyayı en iyi kullanan terör örgütlerinden birisi olduğu bilinmektedir.

Buna karşın kolluk kuvvetlerinin terör örgütüne karşı halkı doğru ve zamanında bilgilendirebilmeleri terör örgütlerinin medyayı istismar etmelerinin önemli ölçüde önüne geçebilmektedir. Aynı paralelde güvenlikleştirme çerçevesinde ulus-devlet liderlerinin medyayı kullandıkları, bu sayede halkın söz konusu tehdit konusunda ikna edildiği, bilgilendirilebildiği bilinmektedir.

Medya kuruluşlarının değişik bölgelerdeki temsilcileri vasıtasıyla tarafsız haberler elde ederek yayımlamaları beklenmektedir. Bu bilgiler oldukça değerli veriler olarak ilgili aktörler tarafından açık kaynak bilgisi olarak değerlendirilmektedir. Dolayısı ile medya kuruluşları yalnızca doğru, tarafsız veya belirli amaçla haberler vermekle kalmamakta, aynı zamanda değişik bölgelerden aynı çerçevede açık kaynak bilgilerini sahadan bizzat toplayabilmektedir.

Müteakip maddede medyanın güvenlik stratejisi tasarım sürecine ve yönetimine olan etkileri incelenmektedir.

2.4.3.2.Medyanın Güvenlik Stratejilerinin Tasarımına ve Yönetimine Olan Etkisi

Yukarıda belirtildiği gibi medya internete göre nispeten bilgi kaynağının belirgin olması nedeniyle durum tespiti safhasında kullanılabilecek önemli bir açık veri kaynağıdır. Verinin alındığı kaynağın güvenilir olması verinin kalitesini artırabilecektir. Medyadan gelen bilgilerin oldukça fazla olduğu dikkate alındığında bu bilgilerin belirli algoritmalar kullanarak günlük, haftalık, aylık, yıllık olarak özetlenmesi; özetlenen bu bilgilerin medya bilgisi olarak depolanması sayesinde önemli bir veri kaynağı oluşturulabilir. Bu veri kaynağındaki bilgilerin diğer kaynaklar ile teyit edilmesi çok kaliteli sonuçlara ulaşılmasına neden olabilir. Liderlerin medyadaki söylem ve davranış analizinin iyi bir şekilde yapılabilmesi önemli bilgiler verebilmektedir. Aktörlerin veya liderlerin söylem ve davranışlarda tespit edilen değişiklikler yine değerli olabilmektedir. Bununla birlikte aldatma amaçlı oluşturulan

söylemler ve davranışlara dikkat edilmesi gerekmektedir. Bu nedenle söylemle gerçek icraatların beraber değerlendirmesi gerekmektedir.

Medyanın diğer veri kaynaklarına göre daha süratli olması nedeniyle elde edilen bilgiler erken ikaz anlamında kullanılabilmektedir. Olayların medyada yer alması, koordinatlarının belirli olması en azından konunun daha detaylı incelenebilmesi için zemin oluşturabilmektedir. Ayrıca bazı medya organları stratejik olaylara yönelik kronolojik olayları listeleyebilmekte, bu da yine değerlendirme maksadıyla önemli bir veri kaynağı oluşturabilmektedir. Bu çerçevede oluşturulacak bir medya izleme merkezi veya durum merkezi önemli faydalar sağlayabilecektir.

Güvenlik stratejisi tasarımı sürecinde ikinci safha olan nihai hedefin belirlenmesinde özellikle yukarıda açıklandığı şekilde aktörlerin veya liderlerin söylem ve davranış analizleri tehdit konusunda önemli ipuçları verebilir. Bu anlamda liderlerin belirli bir konuyu güvenlikleştirmesi veya güvenliksizleştirmesi yine bu çerçevede tespit edilebilir. Daha da önemlisi liderlerin söylemlerinin halk tarafından kabul görüp görmediği yönünde önemli ipuçlarına ulaşılabilir. Müteakiben tehdidin etkisiz hale getirilmesine yönelik nihai hedefin belirlenmesi daha etkin yapılabilir.

Millî güç unsurlarının belirlenmesi safhasında ise gerekli bilgilendirmenin yapılabilmesi maksadıyla bir medya yapılanmasına ihtiyaç vardır. Bu medya yapılanması bütün millî güç unsurlarının etkinliğine önemli katkılar sunabilir. Ancak medya yapılanmasının millî güç unsuru haline gelebilmesi için kurulması yeterli değildir. Söz konusu medya kuruluşunun yerine getirdiği uygulamalarda etkin olması ve kuruluşunun bu husus dikkate alınarak oluşturulması gerekmektedir.

Bu çerçevede stratejik iletişim (Strategic Communication, STRATCOM) olarak adlandırılan yeni bir fonksiyon alanı oluşturulmuştur. Stratejik iletişimin değişik tanımları bulunmaktadır. Özet olarak; belirli bir amaçla medya faaliyetlerinin, bilgi harekâtının ve psikolojik harekâtın beraber koordineli olarak kullanıldığı bir fonksiyon alanı olduğu ifade edilebilir. Bu maksatla yeni organizasyonların oluşturulduğu görülmektedir.

Konsept safhasında güvenlik stratejisi tasarımı ve icrası esnasında sürekli kullanılabilecek medya bilgilendirme konseptinin oluşturulması gerekmektedir. Ancak bu konseptin oluşturulması kolay anlaşılan bir konu değildir. Değişik konsept oluşturma teknikleri olabilir. Bir örnek olması maksadıyla güvenlik stratejisi genel

tasarımı dikkate alınarak medya konseptinin ana amacı ortaya konulmayı müteakip, bu amaca ulaşabilmek için ana mesajların belirlenmesi ve bu mesajların ne zaman, nerede, kim veya hangi araç tarafından verileceğinin belirtilmesi yeterli olabilir. Bu mesajların sürekli gözden geçirilmesi ve sahadaki gerçeklik ile uyum içerisinde olması önem arz etmektedir. Ayrıca bu mesajların hedef kitle tarafından anlaşılıp, kabul edilip edilmediği de etkinlik göstergeleri ve anket şirketlerinin yaptıkları araştırmalar ile ölçülebilir.

Risk safhasında ise durum tespiti safhasında olduğu gibi medyadan faydalanılabilir. Tespit edilen risklerin medyadan alınan veriler ile değerlendirilmesi faydalı olabilir.

2.4.4. Otonom Sistemlerin Güvenlik Stratejilerinin Tasarımına Etkisi

2.4.4.1. Genel

Son teknolojik gelişmeler sonucu otonom sistemler süratle günlük hayatımızda artan bir şekilde yer almaya devam etmektedirler. Otonom araçlar, robotik cerrahi cihazları, otonom ev süpürgeleri, otonom silahlar gibi sistemler gündeme gelen otonom sistemlerden bazılarıdır. Otonom sistemler güvenlik açısından önemli katkılarda bulunurken, hukuksal veya etki yönü ile bazı sorunların tartışılmasına da neden olmaktadır.

Silahlı kuvvetlerin ve kolluk kuvvetlerinin süratle otonom sistemleri kullanmaya çalıştığı, deneyler ve tatbikatlar yaptığı bilinmektedir. Silahlı kuvvetler açısından bakıldığında; hassas güdümlü mermiler, mayın tarlalarından geçit açılmasına yardımcı olan araçlar, dronlar, İHA'lar (İnsansız Hava Araçları) ve SİHA'lar (Silahlı İnsansız Hava Araçları), İKA'lar (İnsansız Kara Araçları), İDA'lar (İnsansız Deniz Araçları) gibi sistemler savaşın karakterini değiştirebilecek yeni taktiklerin kullanılmasına neden olmaktadır. Bu silah sistemlerinin kullanılması taktik, operatif, stratejik seviyelerde önemli değişikliklere neden olmasının yanında, orduların kuvvet yapılarının da dijital çağa uygun şekilde değişmesine neden olabilecektir. Bu değişimin farkında olan ulus-devletler şimdiden dijital çağ silahlı kuvvetlerini oluşturmak için çalışmaya başlamışlardır. Kolluk kuvvetleri açısından bakıldığında silahlı kuvvetlerle mukayese edildiğinde daha hafif otonom sistemlerin kullanıldığını görmek mümkündür. Bomba imha robotları, keşif ve gözetleme sistemleri, yetkisiz

kişilerin girişlerini tespit eden akıllı cihazlar gibi otonom sistemlerin kullanılmasının gittikçe yaygınlaştığı görülmektedir.[87] Silahlı kuvvetlere benzer şekilde kolluk kuvvetlerinin de aynı çerçevede taktiklerini ve kuvvet yapılarını değiştirdikleri görülmektedir.

Terörist örgütler, organize suç örgütleri gibi topluma zarar vermeye çalışan unsurların otonom sistemlerin avantajını fark ederek kullanmaya başladıkları bilinmektedir. DEAŞ'ın maket uçaklara basit bir mekanizma ile bomba bırakma kabiliyetini monte etmesi ve yine basit bir bilgisayar programı ile yönlendirebilmesi en güzel örneklerden birisini teşkil etmektedir.[88] Yine maket uçaklar kamikaze saldırıları, liderlere suikast gibi otonom sistemlerin suç örgütleri tarafından kullanılması kolluk kuvvetlerinin teknolojiyi kullanarak tedbir almasını gerektirmektedir.

Otonom sistemlerin kullanılmasıyla yaşanan sorunlara yönelik çalışmalar devam etmektedir. Örnek olarak otonom bir aracın kaza yapması sonucunda hukuksal olarak kim suçlu olacağı konusunda yapılan tartışmalar verilmektedir. Otonom araç kaza yaptığında; araç sahibi, sistemi tasarlayan mühendis, bilgisayar programını yazan mı? suçlu olacaktır. Benzer şekilde otonom bir silah sisteminin insan öldürmesinden kim sorumlu olacaktır. Bu konudaki hukuki çalışmalar adalet ve güvenlik açısından yeni düzenlemelerin gündeme gelmesine neden olabilecektir.

2.4.4.2.Otonom Sistemlerin Güvenlik Stratejilerinin Tasarımına ve Yönetimine Olan Etkisi

Güvenlik stratejileri tasarımı açısından bakıldığında durum tespiti safhasında otonom gözetleme sistemlerin gerçek zamanlı olarak oldukça faydalı sonuçlar ürettikleri ifade edilebilir. Dijital çağda elde edilen BV'den çıkarılan sonuçların otonom sistemler üzerindeki sensörlerden elde edilen veriler ile teyit edilmesi durum tespitinin kalitesini ve güvenirliğini artırabilir. Durum tespitinin otonom sistemler sayesinde daha güvenilir yapılabilmesi, tehdidin ve neticede nihai hedefin YZ kullanılarak daha iyi belirlenebilmesini sağlayabilecektir.

[87]Fleming, M. H.; Brannan, S.J.; Mosher, A. G.; Altmire, B.; Metrick, A.; Boyle, M.; Say, R, *Unmanned Systems in Homeland Security*, Homeland Security Studies and Analysis Institute, Ocak 2015.
[88]Balkan, Serkan, *DAESH Drone Strategy Technology and The Rise of Innovative Terrorism*, İstanbul 2017.

Otonom sistemlerin önemli bir millî güç unsuru olarak, oyun değiştirici bir şekilde karşımıza çıkmaya başladığı görülmektedir. İHA'lar kullanılarak Karabağ savaşında (2021) başarılı sonuçlar alınması buna iyi bir örnek teşkil etmektedir. Mevcut teknolojik gelişmeler neticesinde gelecekte iki ulus-devletin savaşında önce robotlarla robotların, müteakiben robotlarla insanların, eğer sonuç alınamaz ise insanlarla insanların savaşmak zorunda kalabileceği hayal ürünü olarak görülmemelidir. Millî güç unsurlarındaki bu değişiklik doğal olarak konseptlerin etkilenmesine de neden olabilecektir. Otonom sistemlerin veya bu sistemlere karşı sistemlerin kullanılmasına yönelik yeni taktikler geliştirilmeye devam edilmektedir.

2.4.5. Uzay Teknolojisinin Güvenlik Stratejilerinin Tasarımına Etkisi

2.4.5.1. Genel

Son yıllarda meydana gelen gelişmeler uzayın güvenlik açısından iyi incelenmesini gerektirmektedir. Dünyanın yörüngesindeki uydu sayısının 2022 yılında 4500'den fazla olduğu belirtilmektedir[89]. Bu uyduların ağırlıklı olarak ABD, Çin, İngiltere, Rusya ve Japonya'ya ait olduğu görülmektedir. Bu uyduların her birinin belirli yörüngesi, ömürleri, fonksiyonları gibi uzayda dikkate alınması gereken özellikleri bulunmaktadır. Bu durum çerçevesinde dünyada yaşanan aktörler arası mücadelenin uzaya yansımalarının olması kaçınılmazdır. SpaceX firmasının Rusya-Ukrayna savaşında "starlink" sistemini Ukrayna'nın faydalanacağı şekilde konumlandırması savaşın gidişatını belirleyen önemli bir kuvvet çarpanı olmuştur.[90]Ayrıca başta SpaceX olmak üzere belirli firmaların uyduların önemli bir bölümüne sahip oldukları görülmektedir. Yani uluslararası şirketleri uzay güvenliği açısından yeni aktörler olarak daha fazla gündeme gelmektedirler. Bunun hem uzayda hem de yeryüzünde güvenlik açısından yansımaları olması kaçınılmazdır.

Bu durum dikkate alındığında küresel rekabetin ve güç mücadelesinin benzerinin değişik yöntemlerle uzayda da yaşandığını değerlendirmek zor değildir. Rusya'nın savaş çerçevesinde Ukrayna'ya internet maksadıyla tahsis edilen uyduları etkisiz hale getirmeyi gözden geçirdiği tahmin edilebilir. Yine uyduların yeryüzü ve birbirleri ile olan etkileşimlerinin takip edildiği, hatta elektronik harp ve siber güvenlik kapsamında

[89]Whitt, Kelly Kizer, WhoOwnsAllTheSatellites?, 8 Şubat 2022.
[90]Miller, Christopher; Scott, Mark; Bender, Bryan, *UkraineX: How Elon Musk's Space Satellites Changed the War on the Ground*, 2022.

mücadelenin devam ettiği değerlendirilebilir. Uzaya hâkim olan küresel mücadelede önemli bir üstünlük sağlayabilecektir.

2.4.5.2. Uzayın Güvenlik Stratejilerinin Tasarımına ve Yönetimine Olan Etkisi

Uzayın güvenlik stratejisi tasarımı ve yönetimine internet, medya benzeri bir etkisi olduğu ve uyduların yarısının haberleşme uydusu olduğu bilinmektedir. Doğal olarak haberleşme uydularından oldukça fazla miktarda BV üretilmektedir. Bunun yanında casus uydular, diğer sensör yapısında olan görüntü alabilen uydular da dikkate alındığında BV miktarı daha da artmaktadır. Uzaydan elde edilen BV'nin yeryüzünden elde edilen diğer sensör verileri ile beraber kullanıma sokulması önemli bir kuvvet çarpanı olabilmektedir. Bu veri durum tespiti safhasında önemli bir kaynak teşkil edecek, durum tespitinin daha sağlıklı yapılmasını sağlayabilecektir.

Millî güç unsuru olarak uzayın kullanılabilmesi için ise yeni ve uzaya özel bir yapılanmaya ihtiyaç duyulacaktır. Özel şirketlerin başlattığı uzay turizminin yansımaları devam etmektedir. Turizmi müteakip uzayda maden işletmeciliği, kolonilerin kurulması, sonuç olarak da mülkiyetin oluşması ve mülkiyetin korunması ihtiyacının gündeme gelmesi kaçınılmaz olacaktır. Bilindiği gibi birçok aktör bunun bilincinde olarak uzay komutanlıkları oluşturmuştur. Aktörler bu komutanlıkları ve kuruluşları kullanarak uzaydaki gelişmeleri takip ederek, millî menfaatleri çerçevesinde yönlendirmeye başlamışlardır.

Konsept safhasında ise uzayın diğer millî güç unsurlarına olan etkisi ile kendi başına yapabileceği etkiler göz önüne alınmalıdır. Ancak konsept üretiminde uzayın şartlarının iyi değerlendirilmesi, uzmanlar vasıtasıyla konseptlerin hazırlanması gerekmektedir. Bu maksatla barış zamanından itibaren birçok devletin yaptığı gibi siber güvenlik stratejisine benzer uzay stratejisinin hazırlanması uygun olacaktır.

2.5. DİJİTAL ÇAĞDA GÜVENLİK STRATEJİSİ TASARIMI VE YÖNETİMİNE ETKİ EDEBİLECEK FAKTÖRLERİN VE PARAMETRELERİN TESPİT EDİLMESİ

Çalışmada buraya kadar dijital çağda güvenlik ortamının ve teknolojik gelişmelerin güvenlik stratejisi tasarımına olan etkileri ortaya konulmaya çalışılmıştır. İnceleme sonucunda elde edilen değerlendirmeler ile tezin sorusunun cevaplandırılabileceği düşünülmektedir.

Ayrıntılı olarak incelenen dijital çağda güvenlik ortamındaki süratli ve sürekli değişim, krizlerin stratejik şoklara dönüşmüş olması, belirsizliklerin artmış olması gibi güvenliğe yönelik faktörlerin yanında; BV, YZ, internet, siber ve uzay gibi teknolojilerdeki baş döndürücü gelişmelerin güvenlik stratejisi tasarımına önemli etkilerinin olması kaçınılmazdır. Dijitalleşme ile insanın düşünme sisteminin takviye edilmesi; iletişim, ulaşım, araştırma gibi insanların bazı kabiliyetlerinin geliştirilmesi ve hızlanması sağlamıştır. Dolayısıyla insan hayatı hızlanmıştır. Bu bölümün başından buraya kadar yapılan tüm incelemeler dikkate alındığında; birinci bölümde kavramsal olarak ortaya konulmuş olan klasik güvenlik stratejisi tasarımı ve yöntemi modelinin dijital çağın şartlarına cevap veremeyeceği ifade edilebilir.

Klasik güvenlik stratejisi tasarımının etkinliğini kaybetmiş olması demek stratejiye olan ihtiyacın ortadan kalktığı anlamına gelmemelidir. Belirli bir strateji olmadığı takdirde, herhangi bir organizasyonda kargaşa ortamının oluşması, fırsatların değerlendirilememesi, tehditlere zamanında cevap verilememesi, koordinasyonun sağlanamaması, gayretlerin boşa gitmesi gibi hayati sorunlarla karşılaşma ihtimali, dijital çağın yukarıda ortaya konulan özellikleri nedeniyle daha da artabilecektir. Hatta bu sınamalar nedeniyle dijital çağda stratejiye olan ihtiyacın daha da artmış olduğu ifade edilebilir. Bu nedenle dijital çağın şartlarına uyarlanmış bir güvenlik stratejisi tasarımı ve yönetimi modeli önemli bir kuvvet çarpanı olabilecektir.

Bu değerlendirmeler ışığında yeni bir model oluşturulmasına yardımcı olabilecek olan faktörlerden bazılarının bu aşamada incelenmesi uygun olacaktır. Bu çerçevede müteakip maddelerde bir inceleme yapılmıştır.

2.5.1. Süratli Değişim

Yukarıda incelendiği gibi dijital çağ güvenlik ortamı ve teknolojik gelişmeler günümüzde olayları çok hızlandırmıştır. Buna ilave olarak meydana gelen bir olayın etkileri çok daha derin yaşanabilmektedir. ABD'deki 11 Eylül saldırısı, Arap Ayaklanması, Kovit-19 gibi olaylar stratejik şok olarak nitelendirilmektedir. Bu şoklar neticesinde güvenlik stratejisinin tasarlandığı gibi icra edilebilmesi neredeyse imkânsızdır. Küçük değişikliklerle stratejinin tekrar icraya konulması mümkün olmamakta, bazen yeniden tasarımın yapılması gerekebilmektedir. Yeniden tasarlanan stratejinin benzer şekilde süratli değişim neticesinde etkisiz kalmayacağı, aynı akıbete uğramayacağına yönelik bir garanti bulunmamaktadır. Neticede strateji tasarlanmasına olan inanç sarsılmakta, strateji kâğıt üzerinde kalmaya mahkûm olmaktadır. Stratejik şoklar olmasa bile olayların akış hızı, değişim hızı stratejik tasarımın en azından etkinliğini azaltabilecek önemli sonuçlara neden olmaktadır.

Değişim süratinden stratejik tasarımın etkilenmemesi için alınabilecek tedbirlerden birisi stratejinin oldukça genel hatları ile yazılmasıdır. Bu özellikle bir önceki bölümde tasarım sürecinin konsept safhasında belirtilen yöntemlerden birisi kullanılarak aşılabilir. Diğer bir çözüm ise yalnızca hedeflerin ve alt hedeflerin verilmesi ve genel amacı ortaya koyabilecek bir niyet metninin oluşturulmasıdır. Strateji tasarımının daha kısa süreleri kapsayacak şekilde yapılması diğer bir çözüm tarzı olabilir. Bu çözümlerin hepsi tasarımın kalitesini düşürebilecektir.

Strateji ve strateji tasarımının özelliklerini muhafaza ederek başlangıçtan itibaren değerlendirmenin daha sık aralıklarla ve nasıl yapılacağının ortaya konulması kaliteyi ve uygulanabilirliği arttırabilecektir. Yönetim esnasında yalnızca bilgi aktarımı veya durumsal farkındalığın oluşturulması yeterli olmayacaktır. Bunun yanında her stratejinin bir değerlendirme planı ve değerlendirme periyodu oluşturulmalı, tasarım sürecinin başından itibaren değerlendirmenin nasıl yapılacağı açık olarak ortaya konulmalıdır.

Değerlendirmenin süratle, etkin olarak yapılabilmesi maksadıyla bazı nirengi noktalarının tasarımda yer alması uygun olabilecektir. Bunlar ara hedefler, muhtemel kriz noktaları, karar noktaları, sıklet merkezi yapılacak noktalar veya kritik hat, değerlendirme periyotları gibi hususlar olabilir.

Süratli değişim, kriz yönetimi ve stratejik şoklar güvenlik stratejisi yönetiminde karşımıza çıkması kaçınılmaz problem sahalarıdır. Bu problemlere tasarım safhasında hem tasarım sürecinde hem de problemler meydana geldiğinde etkin olarak müdahale edebilmek maksadıyla teşkilat kurulması ve önceden tedbir alınması gerekmektedir.

Süratle gelişen durumda diğer bir önemli konu karar vericilerin zamanında stratejik seviye kararları verebilmeleridir. Stratejik seviyede kararların verilmesi operatif ve taktik seviye kararlara göre çok daha zordur. Öncelikle bir karara ihtiyaç olup olmadığına karar vermek gerekmektedir. Çoğu zaman bu konuda hata yapılmakta, karar verilmesi gereken bir safhada zamanında karar verilememekte, tespit edilemeyen problem kartopunun çığa dönüşmesi gibi bir etki yaratarak stratejinin yönetilmesini önemli ölçüde etkilemektedir. Problem tespit edilse bile karar vericilere karar verdirmek gerektiğinde zamanında, karar verilmesi için ihtiyaç duyulan veriler sunulamamaktadır. Karar verilmesi için ihtiyaç duyulan yöntem ve seçilecek veriler ayrıca önem taşımaktadır. Yöntemin karışık olması veya gereğinden fazla bilginin sunulması karar vericinin kafasını karıştıracak, zamanında karar verememesine neden olabilecek, neticede karar zamanı geçebilecektir. Bu mahzurun giderilmesi için tasarımda, teşkilatta ve stratejinin yönetiminde gerekli tedbirlerin alınması gerekmektedir. Alınabilecek tedbirlerden birisi stratejik karar vericinin önemli kararları zamanında verebilmesi için ihtiyaç duyacağı bilgilerin daha tasarım aşamasında belirlenmesi ve sürekli gözden geçirilmesidir. Buna Stratejik Lider Kritik Bilgi İhtiyacı (SLBİ) adı verilebilir. SLBİ yalnızca hedef veya rakip aktörü kapsamamalı, kendi durumunu gösteren millî güç unsurlarının durumu, küresel güvenlik ortamı, jeopolitik durum gibi ihtiyaç duyulan bütün bilgiler bulunmalıdır.

Stratejik seviyede yönetimin başarılı olması için millî güvenlik konusunda görevlendirilen kuruluşun bir çalışma temposu veya programı olmalıdır. Bu kuruluşun değişik alt birimleri kendi aralarında ve diğer paydaşlar ile koordinasyon toplantısı yapabilmeli, zamanı gelince elde edilen sonuçlar stratejik karar vericiye sunularak karar vermesi sağlanabilmelidir. Bu program genel anlamda; gözlem, odaklanma, karar, icra döngüsünü kapsayabilir. Döngünün temposu olayların akış hızına göre yavaşlatılıp arttırılabilir.

Değişmeyen tek şeyin değişimin kendisi olduğu düşüncesinden hareketle; dijital çağdaki süratli değişime ayak uydurulabilmesi, rakip aktörlerden daha ileriye geçilebilmesi için stratejik yönetim için teşkilatlanma çok daha önem kazanmıştır. Bu

çerçevede yukarıda belirtilen dört fonksiyon alanı ayrı birimler tarafından icra edilirken, planlama konusuna özel önem verilmelidir. Bu anlamda icranın hemen yanında kısa vadeli planlama birimi oluştururken, gelecek planlaması için tedbir alınması uygun olabilecektir.

2.5.2.Belirsizlik ve Muğlaklık

Belirsizliğin etkisinin azaltılmasının en iyi yöntemlerinden birisi proaktif planlamadır. Proaktif planlamada en önemli husus geleceğin şekillendirilmesinden geçmektedir. Buna rağmen tam olarak geleceğin tahmin edilmesi ve belirsizliğin giderilmesi gerçekleşmeyebilecektir.

Belirsizlik ile beraber muğlaklık durumu daha da zorlaştırmaktadır. "Post-truth" bir ortamda gerçeklerin tespit edilmesi ve muğlaklığın giderilmesi oldukça zordur. Bu çerçevede BV ve YZ oldukça faydalı olabilecektir. Ancak burada dikkat edilmesi gereken önemli husus BV'nin veri kaynaklarının güvenilir olması, güvenirliklerinin sürekli gözden geçirilmesidir. Diğer bir tedbir ise veri kaynaklarının birbirleri ile çapraz kontrole tabi tutulmasıdır. Bu hususları veri bilimciler tasarımlarında dikkate almak zorundadırlar. Elde edilen BV'nin gerçek zamanlı olarak İHA'lar, uydular gibi sensörlerden teyit edilmesi daha kaliteli sonuçların elde edilmesine neden olabilecektir. Bir önceki bölümde üzerinde durulan bir bakışta kritik noktanın veya noktaların tespit edilebilmesi olarak nitelendirilen "coup d'oeil" özelliği BV ve YZ sayesinde artık bilgisayarlar tarafından gerçekleştirilebilmesi gündemdedir. Bu doğal olarak oldukça önemli bir kuvvet çarpanı olarak karşımıza çıkabilecektir. İnsanın olayları veya diğer gerçekleri doğru olarak algılayabilmesi bu kuvvet çarpanının çok daha etkili olmasına neden olabilecektir.

2.5.3.Yeni Aktörler

Yukarıda belirtildiği gibi DEAŞ gibi terör örgütleri, önde gelen dijital şirketler, güçlü enerji şirketleri gibi uluslararası organizasyonlar dijital çağda dikkate alınması gereken aktörler olarak karşımıza çıkmaktadır. Aktörlerin sayısının ve çeşidinin artmış olması millî menfaatlere tehdit oluşturabilecek unsurların yeni bir anlayışla incelenmesi gerektiğini ortaya koymaktadır. Bu anlayışla söz konusu olan aktörlerin takip edilebilmesi ve faaliyetlerinin amaçlarının anlaşılabilmesi için özel birimler kurulması

gerekebilir. Dolayısı ile tasarım ve değerlendirme sürecinde ilave birimlere ihtiyaç olup olmadığı, millî güç unsurlarının performansının yeterli olup olmadığı, ilave güç unsuru ihtiyacı sürekli sorgulanmalıdır.

Dijital çağın şartları çerçevesinde bilgi teknolojileri alanında çalışan sosyal medya şirketleri, e-ticaret şirketleri gibi organizasyonlar önemli aktörler olarak karşımıza çıkmaktadır. Gelecekte de önemleri artabilecektir.

Dolayısıyla durum tespiti safhasında tehdit değerlendirmesi yaparken dijital çağın şartları dikkate alınarak yeni aktörlerin hesaba katılması gerekmektedir. Bu aktörler tehdit olarak karşımıza çıkabilecektir. Tehdidin içeriği yine dijital çağın gereklerine uygun yapılmalıdır. Günümüzde aktörlerin yanında salgın hastalıklar, iklim değişikliği sonucunda oluşan problemler, göçler, doğal afetler de önemli tehdit sahalarıdır. Özet olarak basmakalıp bir anlayışla klasik aktör veya tehdit tanımlaması yapılmamalı, geniş bir perspektif ile düşünülmelidir.

2.5.4.Siber ve Uzay Ortamları

Bilindiği gibi stratejinin üç temel faktörü; kuvvet, zaman, mekân olarak ifade edilmektedir. Eskiden kara, deniz, hava olarak belirtilen mekân faktörüne daha önce de ifade edildiği gibi artık siber alan ve uzay eklenmiştir. Yani dijital çağda strateji tasarımı üç boyutlu değil beş boyutlu olarak düşünülmek zorundadır. Bunun yanında kuvvet yani millî güç unsuru ve hatta konsept yazılımında yine siberin ve uzayın dikkate alınması gerekmektedir.

Burada sibere ayrı bir yer verilmesi uygun olacaktır. Siber denilince hem siber savaş hem de bilgi harekâtı akla gelmelidir. İnsanların sürekli çevrim halinde olduğu düşünüldüğünde strateji tasarımında bu iki hususun sürekli bir faaliyet olarak dikkate alınması gerekmektedir. Bu çerçevede dost, tarafsız ve rakip aktörlerin gerektiği şekilde bilgilendirilmesi, gerekirse siber yöntemler ile mücadele edilmesi tasarlanabilir. Bu maksatla stratejik iletişim biriminin kurulması ve stratejik seviye faaliyette bulunması önemli bir yumuşak güç unsuru olarak karşımıza çıkabilecektir.

Stratejik iletişim birimi her bir stratejiye göre farklı bir stratejik iletişim stratejisi oluşturmak zorundadır. Strateji tasarım sürecine paralel olarak stratejik iletişim stratejisi tasarlanmalıdır. Bu anlamda iletişime yönelik bir durum tespiti, iletişimin nihai hedefi, kullanılacak güç unsurları ve kullanım konsepti, risk unsuru incelenmeli

bir strateji oluşturulmalıdır. Stratejik iletişimin her safhasında BV ve YZ kullanımı dikkate alınmalıdır. Bunun en temel nedeni dijital çağın süratli ve sürekli değişim ortamına ayak uydurulabilmesidir. Dijital çağ stratejik tasarımı konusunda ihtiyaç duyulan neredeyse her şey stratejik iletişim tasarımına da eklenebilir. Stratejik iletişimde medya, bilgi harekâtı, bilgi destek harekâtı farklı teknikler ve uzmanlıklar gerektirmesi nedeniyle farklı birimler ve uzmanlar tarafından yönlendirilmesi gerekmektedir. Bu nedenle aralarındaki koordinasyon hayati önemi haizdir. Söz konusu birimlerin birbirlerinin faaliyetlerinin etkisini azaltmasına müsaade edilmemelidir.

Siber boyutun önemi Rusya-Ukrayna savaşında açık bir şekilde ortaya çıkmıştır. Dijital çağda neredeyse bütün medya batılı ülkelerin elinde bulunmaktadır. Rusya'nın elinde nispeten daha az medya ve internet kuruluşu bulunmaktadır. Netice olarak batının anlatısı veya mesajları çok daha etkili olmaktadır. Rusya başlangıçta Ukrayna'nın iletişim alt yapısını etkisiz kılarak bu üstünlüğü kırmaya çalışmıştır. SpaceX firması tarafından "starlink" sisteminin uzaydan Ukrayna'ya hizmet verecek şekilde konuşlandırılması önemli bir oyun değiştirici olmuştur. Görüldüğü gibi sivil bir şirket siber ortam ve uzayı kullanarak savaşın gidişatında önemi bir rol oynamıştır.

Belirli ülkelere ait uzaya yerleştirilmiş GPS, Galilo gibi seyir sistemleri yukarıda açıklanan şekilde savaşın veya güvenlik stratejilerinin tasarımını önemli bir şekilde etkilemektedir. Bu sistemler millî güç unsurları arasında önemli bir yer kaplamaktadır. Doğal olarak bu ve haberleşme, görüntü alma gibi benzeri sistemlerin barıştan itibaren uzaya yerleştirilmiş olmalıdır.

Siber ortamda yapılan saldırıların tespit edilmesi oldukça zordur. Bu nedenle saldırı olup olmadığını belirleyebilen teknolojinin yanında sorumlu bir organizasyon da kurulmalıdır. Bu organizasyon 7/24 siber ortamı izleyebilmeli, değerlendirmeler yapabilmeli, kararlar verebilmeli ve kararları icra edilebilmelidir. Bu kuruluş aynen normal bir harekât merkezinin klasik bir savaşı sevk ve idare ettiği gibi faaliyetleri icra edebilmelidir. Siber ortam klasik mücadelelerde olduğu gibi kinetik faaliyetleri içermediği için sevk ve idaresi, bu maksatla konsept üretilebilmesi oldukça zordur. Bunun en güzel örneklerinden birisi siber casusluk ve karşı casusluk faaliyetleri olarak gösterilebilir. Doğal olarak tehdit değerlendirmesi de özel yöntemler ve uzman personel tarafından yapılmalıdır. Verilmesi gereken en zor kararlardan birisi siber saldırıların eşik değerini aştığı ve savaş boyutunu geldiği veya bu saldırıların kimin

tarafından yapıldığıdır. Bunun yanında kinetik olmayan faaliyetler ile kinetik olan faaliyetlerin koordineli olarak yürütülmesi ise çok daha zordur. Ancak bu imkân ve kabiliyetin kazanılması önemli bir millî güç unsuru olabilecektir.

2.5.5. Dijital Çağ Teknolojisi

Tarım ve sanayi çağı ile mukayese edildiğinde dijital çağ teknolojilerinin keşfedilmesi, kullanılması daha zordur. Bunun yanında teknolojik gelişmeler çok hızla meydana gelmekte; millî güvenlik açısından etkilerini değerlendirmek, karşı tedbir almak, millî menfaatlerin gerçekleşmesi için kullanabilmek önemli sınamaları içermektedir. Dolayısı ile balistik füzeler, nükleer silahlar gibi başta BV ve YZ olmak üzere dijital çağ teknolojilerinin çok iyi takip edilmesi, uzman yetiştirilmesi mili güvenlik açısından hayati önemi haizi bir duruma gelmiştir. Hatta yapılan bazı değerlendirmelerin[91] dijital çağ teknolojilerinin nükleer silahlardan daha fazla yıkıcı etkisinin olabileceği yönündedir. Bu şartlarda dijital çağ teknolojileri stratejik tasarım sürecinin etkinliğini artırabilecek özelliklere sahipken aynı zamanda tehdit olma özelliğini içerebilmektedir. Teknolojik gelişmelerin gerisinde kalan bir ulus-devlet BV ve YZ gibi teknolojileri çok iyi kullanan diğer ulus-devletlerin hatta devlet dışı aktörlerin sömürüsü durumuna gelebilecektir. Önümüzdeki süreçte bu teknolojilerin daha gelişmesi bu anlamda çok daha etkin sonuçlar üretebilecektir.

Bu nedenlerden dolayı teknoloji hazırlık seviyesi, daha önceki bölümde belirtilen yedi millî güç unsuruna ilave sekizinci millî güç unsuru olarak değerlendirilmelidir. Teknoloji hazırlık seviyesi yalnızca savunma değil bütün millî güç unsurlarını etkileyebilecek bir kuvvet çarpanı olacaktır. Bunun bilincinde olan ülkeler diğer ülkelerden kritik teknolojilerin üretilmesini sağlayabilecek eğitimi almak isteyen bazı ülkelerin öğrencilerinin eğitim almasını bile engellemektedir.

Bir önceki bölümde savunma planlaması kapsamında örnek olarak askeri güç unsurunun nasıl geliştirilebileceği açıklanmıştır. Savunma teknolojilerinin geliştirilmesi konusunda uluslararası ortamda benzer yaklaşımlar olduğu vurgulanmıştır. Bu çerçevede yapılacak stratejik bir planlama sayesinde teknolojik

[91]Ullman, Harlan, *Is Artificial Intelligence More Formidable Than Nuclear Weapons*, 2021.

hazırlık seviyesi arttırılarak güç unsurunun sürekli geliştirilmesinin hedeflenmesi uygun olacaktır.

Güvenlik stratejisi tasarlama ve yönetim süreçleri açısından konu değerlendirildiğinde teknolojinin etkin kullanılabilmesi, gelişen stratejik teknolojilere yönelik tedbir geliştirilebilmesi için teşkilat anlamında yenilikler yapılması gerekmektedir. Bu anlamda dijital çağın yeni meslek branşlarından olan veri bilimci, veri analizci, veri üretimci, YZ uzmanları gibi bazı uzmanların kullanılması ve yeni birimlerin oluşturulması kaçınılmaz hale gelmiştir. Önümüzdeki süreçte bu ihtiyaç çok daha fazla artabilecektir.

Tasarım ve yönetim sürecinde üzerinde durulması gereken diğer bir konu ise süreçteki unsurların her birinin mümkün olduğu kadar dijital çağın gereklerine uygun tertiplenebilmesidir. Bu maksatla gelen raporların formatları değiştirilebilir, millî güvenlik ile sorumlu olan kuruluşun kullandığı süreçlerin dijital çağa uygun hale getirilmesi, süratin artması sağlanabilir. Bu hususta verilecek direktif doğrultusunda kurum bilişim uzmanı ile beraber diğer uzmanlar karar verebilecektir.

Özetle başta BV ve YZ olmak üzere dijital çağın getirdiği teknolojik gelişmeler dikkate alınmadan artık güvenlik stratejilerinin tasarlanması ve yönetilmesi imkânsız hale gelmiştir.

2.5.6. Dijital Çağda Karar Verme

Güvenlik stratejisi kapsamında öncelikle tasarım aşamasında, sonrasında stratejinin yönetimi veya icrası esnasında karar süreçlerinin işletilmesi oldukça önemlidir. Tasarım aşamasında verilecek kararlar ile ilgili bir önceki bölümde "1.4.Güvenlik Stratejisi Tasarımının İncelenmesi" başlığı altında cevap verilmesi gereken sorular çerçevesinde bazı öneriler yapılmıştır. Bu liste daha uzatılabilir veya kısaltılabilir. Tasarım aşamasında verilecek kararlar nispeten statik bir çerçevede verildiği için zaman baskısı kısmen daha azdır. Paydaş kuruluşlar ile uzlaşıya gidilebilmesi için zaman ve fırsat bulunabilir. Ancak güvenlik stratejisinin icrasına başlandığında benzer süreçler için yeterli zamana sahip olunamayabilir.

Bilindiği gibi stratejinin; bir yol haritası, politik seviye ile taktik seviye (operatif seviye) arasında bir köprü, mevcut durum ile ulaşılması istenen nihai hedef (vizyon) için planlama, eldeki kaynaklar ile nihai hedefe ulaşılması için yapılan çalışma gibi

değişik tanımları bulunmaktadır. Bu nedenle karar vericilerin hem politik hem de icrayı esas alacak bir bilgi seviyesine sahip olması gerekmektedir. Dolayısıyla karar vericiler politik ve icraya yönelik olarak operatif ve taktik faktörleri aynı anda dikkate almak durumunda kalabileceklerdir. İcranın daha ağır bastığı operatif ve taktik seviyelerde de kararlar alınmaktadır. Ancak alınan bu kararlar stratejik seviye tarafından bilinmeyen hususlar bilinir hale getirilerek oluşturulan daha belirgin bir ortamda alınmaktadır. Dolayısıyla öncelikle havada kalmış, belirgin olmayan birçok konu icranın sağlıklı yapılabilmesi için stratejik seviyede bilinir veya somut hale dönüştürülmesi gerekmektedir. Bir önceki bölümde "Stratejinin Özellikleri" başlığı altında incelenen hususlar da dikkate alındığında stratejik seviye kararların verilmesi operatif ve taktik seviyeye göre daha zordur.

Birçok lider stratejik kararlar yerine daha görünür olabilen taktik seviye kararlar vermeyi tercih eder. Hatta bu liderler stratejik seviyede bir karar vermeleri gerektiğini bile hissedemezler veya anlayamazlar. Dijital çağın getirdiği teknolojik imkânlar, haberleşme olanakları da dikkate alınarak bu liderler ast seviyedeki taktik, yani daha somut olayları daha kolay anlayabilir ve maalesef kendi vermeleri gereken kritik karaları göz ardı ederek astlarının vermeleri gereken kararları kendileri vermeye başlayabilirler. Ancak burada doğru bilginin zamanında elde edilebilmesine özel önem verilmesi gerekmektedir. Bu nedenle ast seviye unsurlardan, ilgili kurumlardan gerekli bilgilerin raporlar aracılığı ile veya doğru soruların sorulduğu bilgi istek formları gönderilerek talep edilmesine özel önem verilmesi uygun olacaktır. Stratejik seviyede yeterli zaman varken, zamanında kararlar verilemediği ve göz ardı edildiği için taktik seviyede başlangıçta kartopu halinde olan problemler birikerek çığ haline dönüşebilir. Buna ilave olarak stratejik seviyede yapılan hatalar taktik seviyede düzeltilemez. Bununla beraber yine dijital çağdaki teknolojik gelişmeler neticesinde taktik seviyede meydana gelen olayların çok önemli stratejik sonuçları da olabilmektedir. Dijital çağdaki karar vericilerin bu hususu sürekli akılda tutmaları gerekmektedir.

Diğer taraftan "Süratli Değişim" başlığı altında incelendiği gibi değişmeyen tek şey değişimin kendisidir. Bu nedenle dijital çağda hem tasarım sürecinde hem de icra esnasında verilen birçok karar çok kısa sürede geçerliliğini kaybedebilecektir. Bu husus dikkate alınarak özellikle icra esnasında kararların zamanında ve süratle verilmesi, süratle gelişen durumlar karşısında karar verilme ihtiyacının hissedilebilmesi veya anlaşılabilmesi, yeni karşılaşılan duruma adapte olunabilmesi

için gerekli tedbirlerin alınması, zamanında kararların verilmesi gerekmektedir. Dijital çağdaki değişim süratinden dolayı tasarım sürecinde verilen kararlar ile tasarımın dayandığı; hedef, kaynak, konsept gibi stratejinin temel hususlarının da incelenmeye alınması ihtiyacı ortaya çıkmaktadır. Dolayısıyla icra esnasında eleştirel bir yaklaşımla sadece icraya yönelik bir değerlendirme değil güvenlik stratejisinin dayandığı temel hususların da değerlendirilmeye alınması, yani değerlendirmede kapsamlı yaklaşımın benimsenmesi önem taşımaktadır.

İcra esnasında kararların verilme süreci çok daha dinamik bir yapıya sahiptir. Genel olarak karar süreçleri; verinin üretilmesi, verinin bilgi, faydalı bilgi ve hatta erdem haline getirilmesi, rakiplerin veya aktörlerin uygulayabilecekleri hal tarzlarının ve/veya güvenlik ortamının gelecekte alabileceği şeklin tahayyül edilmesi, bu çerçevede hal tarzlarının belirlenmesi ve bu hal tarazlarının arasından karara esas olan hal tarzının seçilmesi şeklinde özetlenebilir. Bu maksatla Şekil 2.5'te gösterilen karar verme süreci bu çalışmada önerilmektedir.

Karar verme sürecinde verinin üretilmesini müteakip güvenlik stratejisinin amacına göre verilerin faydalı hale getirilmesi gerekmektedir. Örneğin terörle mücadele konusunda bir güvenlik stratejisi oluşturulması gerekiyorsa; örgütün eylem yöntemleri, zayıf ve kuvvetli tarafları, liderlerinin özellikleri, geçmişte önem taşıyan eylemleri gibi veriler önem kazanmaktadır. Bu verilerle terör örgütünün önümüzdeki dönemde uygulayabileceği hal tarzları ortaya konulabilir. Bu hal tarzlarından bazıları; şehirlerde eylem arayışı, halkın kolluk kuvvetlerine yardım etmesinin engellenmesi, sınır birliklerine saldırması olarak belirlenebilir. Bu hal tarzlarından uygulama ihtimali en yüksek olanı tespit edilerek hal tarzı üretilebilir. Bunun yanında daha tehlikeli hal tarzları için de tedbir alınabilecek stratejik seviye ihtimalat planları oluşturulabilir. Bunun yanında iyi, kötü ve muhtemel senaryoların ortaya konulması da düşünülebilir. Bunların yerine sadece meydana gelen olayların ham şekilde karar vericinin önüne konulması ve karar vermesinin beklenmesi oldukça önemli bir hata oluşturacaktır. Ayrıca stratejik seviyedeki bir karar vericinin önüne taktik seviye bir bilginin konulması da sadece zaman kaybına neden olacak gerekli kararların alınması zorlaşacaktır. Taktik seviyedeki bilgiler genellikle münferit olaylar şeklinde rapor edilmektedir. Bu bilgilerin direkt olarak karar sürecinde kullanılması faydalı olmamaktadır. Ancak stratejik seviyede sonuçları olabilecek bazı kritik olayların dikkate alınması karar sürecini olumlu etkileyebileceği hususu akılda tutulmalıdır.

Taktik seviyedeki olayların birleştirilmesi ve değerlendirilmesinden elde edilen, stratejik yansımaları olan, nihai hedefe ulaşılmasına katkı sağlayan analizler stratejik seviye karar vericinin işine yarayabilecektir. Stratejik karar verici de doğru karar verebilmesi için ilave stratejik seviye bilgiler elde edebilmek maksadıyla sorular sormalıdır.

Karar verme sürecinde veriler toplanırken en önemli hususlardan birisi gerekli veya ilgili verilerin toplanması, bilgi enflasyonuna izin verilmemesidir. Dijital çağda veri enflasyonu ve gereksiz bilgiler hem karar vericinin odaklanmasına hem de ilgisiz istikametlere yönelmesine, işin özünü kaçırmasına neden olabilecektir. Sonuç olarak karar vericinin yanlış karar vermesine neden olabilecektir. Stratejik seviyede verilen bu kararların olumsuz etkileri uzun bir süre sonra ortaya çıkabilecek, düzeltilmesi için fırsat olmayacaktır. Bununla beraber sensör ve iletişim teknolojisi sayesinde karar vericiler gerçek zamanlı, hatta naklen bazı gelişmeleri takip edebileceklerdir. Bilinçli olmayan bir lider yalnızca gerçek zamanlı konulara yönelerek genel stratejik resmi kaçırabilecek, stratejik seviye karar alma zorlaşabilecektir.

Taktik seviyede imkân kabiliyetlerin ve gayretlerin toplanmasını sağlayabilecek yöntemlerden birisi sıklet merkezi veya kuvvet çoğunluğu bölgesi oluşturmaktır. Bu sayede kararların verilmesi, gayretlerin hedefin ele geçirilmesini sağlayacak bir bölgeye toplanması, rakibe göre üstün bir konuma geçilmesi sağlanabilmektedir. Stratejik seviye daha uzun bir süreci kapsadığı için bu yöntemin kullanılması zor olmaktadır. Bunun yerine nihai hedefe ulaşılmasını sağlayacak alt hedeflerin belirlenmesi ve bu alt hedeflerden stratejinin başarıya ulaşmasını sağlayacak bir kritik hat oluşturulması bu çalışmada önerilmektedir. Bu kritik hattın müteakip bölümde bir model önerilirken açıklaması yapılacaktır.

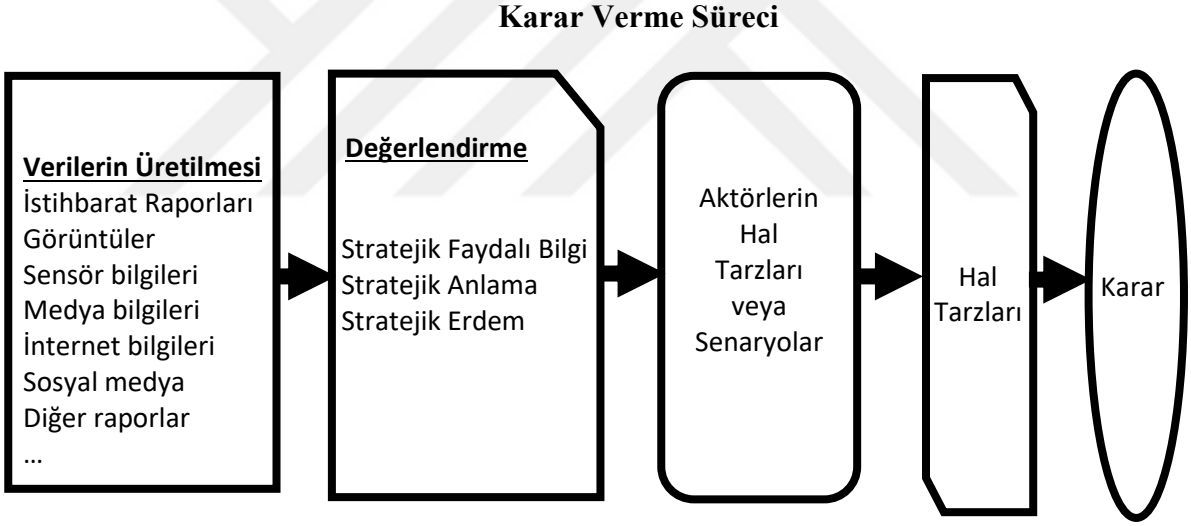
Diğer taraftan stratejik seviye karar vericiler aynı anda birçok kararı vermek zorunda kalabilmektedirler. Bu kararların aynı anda verilebilmesi oldukça zordur. Bu nedenle mümkün olan her durumda önceliklendirme yapılması, en yakın tehlikenin öncelikle ele alınması uygun olabilecektir. Doğal olarak stratejik seviyede verilen kararların uygulanması zaman alacaktır. Bu nedenle verilen kararın icrası için geçebilecek ve ortaya çıkacak sonuçların etkilerinin görülmesi için ihtiyaç duyulacak süre kadar önce stratejik kararların verilmesi uygun olacaktır.

Güvenlik stratejisinin icrası esnasında dikkat edilmesi gereken en önemli hususlardan birisi icra çerçevesinde alınan stratejik kararların nihai hedefe veya

ulaşılmak istenen ideal durum referans alınarak verilmesidir. Bu hususun tasarım aşamasında dikkate alınması uygun olabilecektir. Ancak eğer herhangi bir strateji, ortaya konulmamış, tasarlanmamışsa böyle bir yaklaşım gerçekleşmeyecek, nihai hedef olmadan icra esnasında gayret birliği sağlanamayacaktır.

Stratejik seviyede kararsız kalınması dijital çağda çok daha önemli sorunlara neden olabilecektir. Karar verilememesi neticesinde zincirleme olarak ast kademelerde, yani operatif ve stratejik seviyelerde de kararlar verilemeyecek; rakiplerin inisiyatifi ele geçirmeleri, bizim karar verme sürecimizin içerisine girmeleri gerçekleşecek, sonuç olarak karar verme süreçlerimiz etkisiz hale veya rakiplerin verdiği kararlara tabi olacak şekilde olumsuz etkilenecektir. Stratejik komuta kontrolün kaybedilmesi güvenlik stratejinin tamamını etkileyebilecektir.

Şekil 2.5: Karar Verme Süreci



Kaynak: Yazar tarafından oluşturulmuştur.

Stratejik seviyede, dijital çağda karar verme süreçlerinin yanında kriz yönetimi konusu üzerinde de çalışmalar yapılması gerekmektedir. Kriz durumu; çok özet olarak planlanandan farklı veya hayatın normal akışının dışında olayların gelişmesi, amaçlara ulaşılabilmesi maksadıyla ilave tedbir alınması gerekmesi olarak ifade edilebilir. Dijital çağda krizlerin önceden hissedilmesi, kapsamının anlaşılması maksadıyla tedbirler alınması uygun olacaktır. Krizlerin stratejik şoklara dönüşmesi ile tedbir alınması, sonuçların yönetilmesi çok daha sıkıntılı olabilir. Stratejik şokların ve

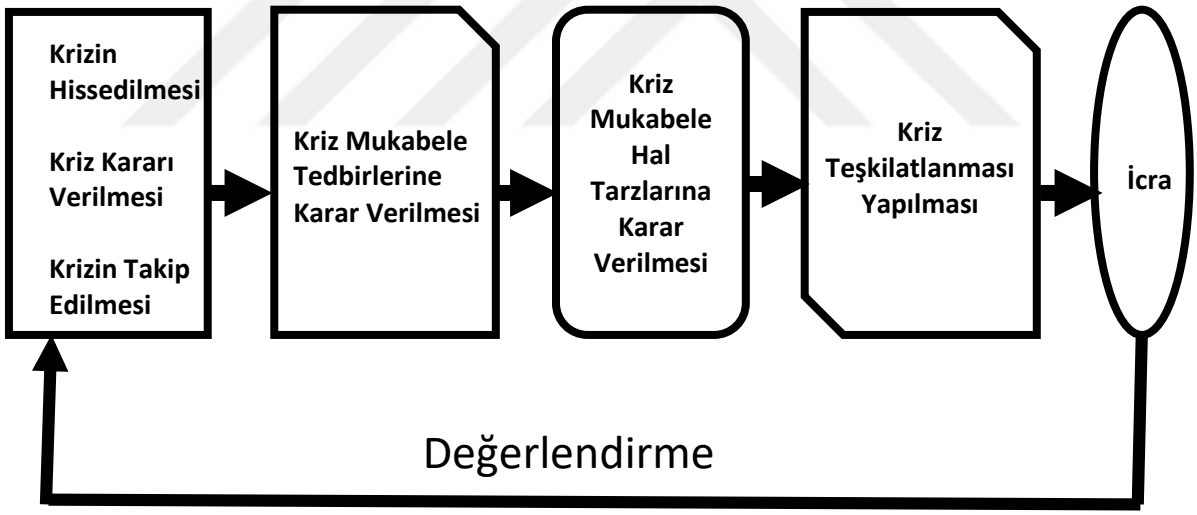
krizlerin etkin yönetilebilmesi için tasarımda gerekli tedbirlerin alınması gerekmektedir. Aksi takdirde güvenlik stratejisi tasarımı etkinliğini kaybedebilecektir. Güvenlik stratejisi açısından kriz yönetiminin aşamaları Şekil 2.6'da bu çalışmada önerilmektedir.

Stratejik şokların meydana geldiği bir güvenlik ortamında, güvenlik stratejisi tasarımında karar verme süreçlerinin yanında kriz tespit ve yönetim sistemleri üzerinde muhakkak durulması gerekmektedir. Hatta ihtiyaç duyulduğu zaman kriz yönetiminin en etkin şekilde yapılabilmesini sağlayabilecek bir anlayışla strateji tasarımının yapılması hayati önemi haizdir. Aksi takdirde krizlerin veya stratejik şokların fazla olduğu dijital çağda her krizle karşılaşıldığı tasarım boşa çıkacak, yeniden bir strateji tasarımı yapılmak zorunda kalınacaktır. Kriz yönetiminin ilk aşaması erken uyarı sistemi sayesinde bir krizin varlığının hissedilmesi veya anlaşılmasıdır. Kriz ne kadar erken anlaşılırsa tedbir almak maksadıyla zaman o kadar fazla olacaktır. Krizin hissedilmesinin yanında söz konusu kurumun veya organizasyonun krizle kurumsal olarak etkin mücadele edebilmesi maksadıyla kriz kararının alınması ve krizin daha yakından takip edilmesine başlanması gerekmektedir. Krizin ilk etaptaki olumsuz etkilerini azaltmak veya zarar vermesini engellemek maksadıyla süratle kriz mukabele tedbirleri yürürlüğe konulabilir. Bu tedbirlerden bazıları, rakip aktörün baskın etkisi yaratmasını veya etkili olmasını engelleyici, hazırlıkları arttırıcı tedbirler olabilir. Genellikle bu tedbirler daha önce planlanmış tedbirler olabilir. Bir sonraki aşama krize mukabele edebilmek için tedbirlerin belirlenebilmesidir. Bunun için bir analiz, değerlendirme yapılmalıdır. Bu değerlendirme bütün millî güç unsurlarımız ve hatta bütün imkânlarımız, kaynaklarımız dikkate alınarak icra edilmelidir. Ulus-devletler bu maksatla sivil-asker durum muhakemesi yaparlar ve hem sivil hem askeri seçenekleri ortaya koyarlar. Bu safha genellikle ihmal edilen, iyi bir değerlendirme yapılmadan, akla gelen ilk tedbirlerin alınmaya başladığı bir süreç olarak icra edilir. Kriz yönetimi ile ilgili yeterli bilgisi ve deneyimi olmayan devletler, aktörler paydaşlar arasında yalnızca durumun paylaşılmasının veya mesajlaşmanın yeterli olduğunu düşünürler. Herkesin durumdan haberdar olması, ancak tedbir alınması için değerlendirme yapılmaması kriz yönetimi olarak nitelendirilemez. Normal olarak ulus-devletler kriz tedbiri olarak, hiçbir şey yapmadan beklemek ile savaş ilan etmek arasında geniş bir spektrumda seçenekler oluşturabilirler. Sadece krizin izlenmesi veya kontrollü olarak tırmandırılması üzerinde de çalışılabilir. Tabi tırmandırma için gerekli hazırlıkların

yapılmış olması gerekir. Bir sonraki adım krizin izlenmesi ve gerekli çalışmaların yapılabilmesi için bir kriz teşkilatlanmasına gidilmedir. Son olarak tedbirlerin icrasına ve geri besleme için değerlendirmeler yapılabilir. Krizin sona ermekte olduğu da tespit edilip, kriz teşkilatının ve tedbirlerinin yürürlükten kaldırılması ve normale dönülmesi için karar verilmesi gerektiği unutulmamalıdır.

Dijital çağda süratle ve etkin olarak karar verilmesine yardımcı olabilecek YZ çerçevesinde bazı yeni yaklaşımlar ortaya çıkmaktadır. Bunlardan bazıları; uzman sistemler, karar ağaçları, sürü zekâsı, dijital modelleme gibi teknolojik yöntemlerdir. Uzman sistemler yaklaşımında değişik durumlara göre daha önce belirlenen kararların alınabilmesi için hazırlanan bilgisayar programları bulunmaktadır. Karar ağacı ise belirli bir gurup alternatifin elenerek doğru sonuca ulaşılmasını sağlayan yöntem olarak özetlenebilir.

Şekil 2.6: Kriz Yönetim Süreci



Kaynak: Yazar tarafından oluşturulmuştur.

Dijital çağda karar verme yöntemlerinden gittikçe gelişme sağlayan iki yöntem; sürü zekâsı ve dijital modellemedir. Sürü zekâsı her ne kadar balıkların, kuşların veya arıların sürü halinde karar vermelerini sağlarken, bu yöntem sosyal ağlarda da kullanılabilir. Bu çerçevede gerçek zamanlı olarak elde edilen veya depolanmış BV, YZ kullanılarak işleme tabi tutulabilir. Uzmanların örtük veya açık bilgisini kullanarak, ayrıca duygusal boyut da dikkate alınarak insanların veya paydaşların

verdiği kararlar ile bu verilerin beraber harmanlanması oldukça doğru sonuçların ortaya çıkmasına neden olabilmektedir. Bu anlamda borsada, finansal tahminlerde, bahis oyunlarında benzer yaklaşımların kullanıldığı bilinmektedir. Bu çerçevede güvenlik stratejisi kapsamında bir örnek verilebilir. Uzmanların herhangi bir ülkenin komşularının tehdit olup olmadığını değerlendirmeye çalıştıkları ve bu anlamda sürü zekâsı kullanmaya çalıştıklarını farz edelim. Komşuların sırayla ele alındığı; savunma harcamalarının, ekonomilerinin, askeri birliklerinin yaptıkları tatbikatların, kritik silah sistemi mukayesesinin, liderlerinin güvenlikleştirme bağlamındaki konuşmaları, sosyal medyada halkın duygu analizi gibi parametreler dikkate alınarak bir sonuç elde edilebilir. Daha önceki bölümde incelendiği gibi tehdit = imkân kabiliyet x niyet şeklinde formüle edilebilir. Hatta bu çerçevede hem imkân kabiliyetler hem de niyetin belirlenebilmesinde BV ve YZ de kullanılabilir. Sonuç olarak bilgisayar tarafından sırasıyla komşuların tehdit olma durumlarını belirleyen bir liste ortaya konulabilir. Bu listenin etkinliği uzmanların oluşturduğu bir sürü tarafından değerlendirilebilir. Uzmanlar kendilerindeki örtük ve açık bilgileri, duygusal zekâlarını kullanarak kendi listelerini oluşturabilirler. Bilgisayarın ve İnsanların verdiği kararlarla oluşturulabilecek hibrit yeni liste çok daha gerçekçi sonuçlar verebilecektir. Bu karar verme sürecine sensörlerden gelen gerçek zamanlı bilgilerin hazırlanacak bir algoritma ile ilave edilmesi çok daha doğru ve etkin sonuçlar verebilecektir. Dijital çağda gelişen teknoloji ile kullanılabileceği değerlendirilen ve Şekil 2.7'de gösterilen yöntem bu çalışmada önerilmektedir.

Birçok grup halinde karar verme veya sürü algoritması ve yöntemi vardır. Parçacık Sürü Optimizasyonu (Particle Swarm Optimization, PSO) benzer amaçla kullanılabilen algoritmalardan birisidir. Söz konusu yaklaşımın tarımda, mühendislikte, metalürjide, sağlıkta, doğal ve sosyal bilimlerde kullanıldığı ifade edilmektedir[92].

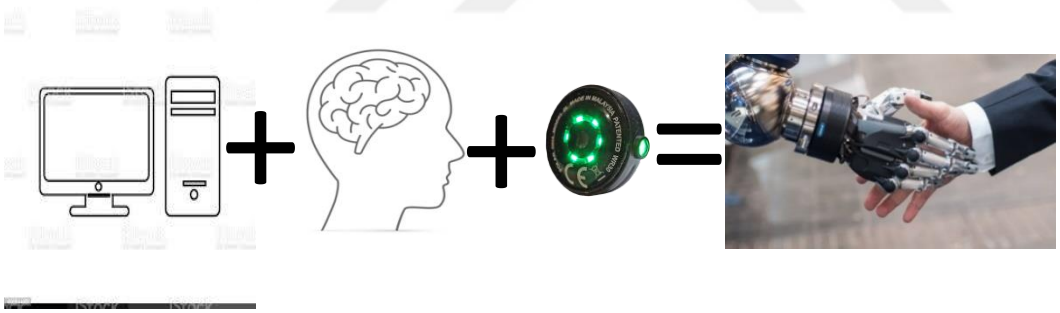
Dijital çağın sunduğu teknolojik imkânlar göz önüne alındığında makine-insan etkileşiminin gerçekleştirildiği benzer süreçlerin gelecekte çok daha yaygın kullanılması beklenebilir. Bu sayede makinenin ve insanın üstün yönleri birbirlerini tamamlayacak şekilde bir arada kullanılabilecektir. Ancak bu maksatla veri bilimcilerinin önemli hazırlıklar yapması gerekmektedir. Örneğin hal tarzları veya

[92]Ramirez-Ochoa, Perez-Dominguez, Marinez-Gomez, Luviano-Cruz, PSO, *Swarm Intelligence-Based Evolutionary Algorithm as Decision-Making Stratetgy: A Review*, 2022, s. 14.

seçenekler oluşturarak bilinen bilinmeyenler üzerinde uzmanların seçim yapmasını veya karar vermesini sağlamaları gerekmektedir. Yukarıda örnek olarak açıklanan basit yönteme benzer başka çözümlerin üretilmesi üzerinde çalışılabilir.

Daha önce üzerinde durulduğu gibi modelleme çerçevesinde dijital ikizin yaratılması, sistem dinamikleri anlayışı ile güvenlik ortamının modellenmesi gibi yöntemler karşımıza çıkmaktadır. Bu ve benzeri modellerin strateji tasarımında aynen bir mühendislik tasarımında olduğu gibi prototip olarak ortaya konulması ve paydaşlarla beraber üzerinde çalışılması, ara stratejik değerlendirmeler yapılırken de yine kullanılması önemli faydalar sağlayabilecektir. Benzer modellerin uluslararası ilişkilerde silahlanma yarışı, devletlerarası çatışmaların yayılması gibi sosyal bilimlerin çalışma konularında kullanıldığı görülmektedir. Bu modellere yine gerçek zamanlı uygun sensör bilgilerinin dahil edilmesi çok daha faydalı sonuçlar ortaya çıkarabilecektir. İdeal bir sistem modeli Şekil 1.4'te, önceki bölümde gösterilmiştir.

Şekil 2.7: Makine ve İnsan Hibrit Karar Verme Yöntemi



Bilgisayar **İnsan** **Sensör** **Karma Sürü Zekâsı**

Kaynak: Yazar tarafından oluşturulmuştur.

2.6. SONUÇ

Güvenlik ortamındaki ve teknolojik alandaki gelişmelerden kaynaklanan faktörlerin dijital çağ güvenlik stratejisi tasarımını önemli ölçüde etkileyebileceği değerlendirilmektedir. Bu anlamda etkin bir değerlendirme yapılabilmesi için yeterli

zaman geçmemiş ve kaynak yayımlanmamış olmasına rağmen, kısmen de olsa bir değerlendirme yapılarak dijital çağa uygun bir güvenlik stratejisi tasarımı ve yönetimi modeli üzerinde çalışılabilir. Bununla beraber değerlendirmelerde meydana gelen olayların olgunlaşması için yeterli zaman geçmediği, yeterli belgelerin ortaya çıkmadığı göz önünde bulundurulmalıdır.

Dijital çağda güvenlik ortamında; belirsizlik, muğlaklık artarken; teknolojinin kullanımıyla tarihin akışı hızlanmış; stratejik şoklar, yeni tehditler, yeni aktörler ortaya çıkmıştır. Arap Ayaklanmaları, salgın hastalıklar, yeni tip terör saldırıları, teknolojiye bağımlılık dijital çağdaki tehditlere örnek teşkil ederken; özel askeri şirketler, devlet dışı aktörler, uluslararası şirketler yeni tip aktörlere örnek gösterilebilir. Neoliberal düzenin zayıflaması, mali krizlerin meydana gelmesi, uluslararası örgütlerin zayıflaması kural tabanlı küresel sistemi ve küresel işbirliğini olumsuz etkilemektedir. Rusya-Ukrayna savaşı ise dijital çağda ulus-devletlerin yıkıcı etkisi olabilecek klasik savaşa ve hatta nükleer savaşa bile başvurabileceklerinin önemli bir örneğini teşkil etmektedir.

Dijital çağ güvenlik ortamının etkilerinin başında; klasik mantıkla güvenlik stratejileri tasarımı ve bu sayede millî menfaatlerin gerçekleştirilmesinin oldukça zor olduğu gerçeği gelmektedir. Bu nedenle güvenlik stratejileri tasarımının ve yönetiminin günümüz koşullarına uyarlanması gerekmektedir. Dijital çağda, güvenlik ortamında meydana gelen değişiklikler dikkate alındığında klasik strateji tasarımı etkinliğini, belki de geçerliliğini yitirdiği, en azından dijital çağdaki güvenlik ortamının şartlarına uyum sağlaması için gerekli tedbirlerin alınması gerektiği açık olarak ortaya çıkmıştır.

Dijital çağdaki güvenlik stratejileri tasarımını etkileyebilecek teknolojik gelişmeler çerçevesinde; bilgisayar teknolojisindeki gelişmelerin tasarımı önemli ölçüde etkileyebileceği kabul edilmesine rağmen, diğer teknolojik gelişmeler de tasarımı önemli ölçüde etkileme potansiyeline sahiptir. Güvenlik stratejisi tasarımını etkileme potansiyeli olan teknoloji ve buluşlardan bazıları; BV, YZ, internet, nesnelerin interneti, sosyal medya, metaverse, cep telefonları, yeni sensör teknolojileri, otonom sistemler, kuantum bilgisayarlar, siber savaş yöntemleri, uzay teknolojileri olarak özetlenebilir. Bunun yanında medya kuruluşlarının, televizyon ve radyo gibi haberleşme araçlarının da etkinliği teknoloji sayesinde artmıştır. Bu

teknolojik gelişmeler dikkate alınmadan dijital çağda güvenlik stratejisi tasarlanması imkânsız hale gelmiştir.

Teknolojik gelişmelerin güvenlik stratejisi tasarımına etkileri kapsamında; BV ve YZ'nin beraber kullanımı stratejik tasarım sürecinin her safhasında etkinliği arttırma potansiyeline sahiptir. Ancak yaratıcı bir yaklaşımla BV ve YZ'nin üzerinde çalışılan safhanın şartlarına uyarlanması gerekmektedir. Stratejinin yönetimi konusunda da benzer yaklaşım geçerlidir. Stratejinin yönetim sürecinde, BV ve YZ kullanımı dijital çağın şartlarına süratle uyum sağlamasına önemli ölçüde yardımcı olabilecektir. İnternet, siber güvenlik, uzay teknolojileri, medyadaki gelişmeler gibi yeni teknolojilerin de tasarım sürecinin her safhasında dikkate alınması önemli bir kuvvet çarpanı olabilecektir.

Bu değerlendirmeler ışığında dijital çağda güvenlik stratejisi tasarımı ve yönetimine etki edebilecek faktörler ve parametreler olarak; süratli değişim, belirsizlik ve muğlaklık, yeni aktörler, yeni tehditler, siber ve uzay ortamı dijital çağın ortaya çıkarttığı, strateji tasarımı ve yönetiminde dikkate alınması gereken önemli faktörler olarak ön plana çıkmaktadır. Bu faktörler ve dijital çağ teknolojileri dikkate alınarak, karar verme, kriz yönetimi başta olmak üzere, strateji tasarımı ve yönetiminde kullanılan süreçlerin gözden geçirilmesi uygun olacaktır.

Karar alma süreçleri tasarımda dikkate alınması gereken önemli bir konudur. Bu anlamda stratejik seviye karar alma ve bu kararlar alınırken başta sürü zekâsı gibi teknolojilerden faydalanılması artık zorunluluk halini almıştır. Ayrıca özellikle BV, YZ, İnternet gibi teknolojik gelişmeler dikkate alınmadan yapılacak bir güvenlik strateji tasarımı dijital çağda geçerli olmayacaktır. Bunun yanında siber güvenlik, bilgi harekât gibi teknolojik gelişmelerin getirdiği bazı yöntemlerin tasarımda mutlaka dikkate alınması gerekmektedir. Bunun aksi rakip aktörlerin her zaman bir adım, hatta bazen çok daha fazla önde olmasına neden olabilecektir. Aynı şekilde tasarımın kolaylaştırılabilmesi için modelleme, dijital ikiz gibi teknolojik imkânlardan faydalanılması, önemli kolaylıklar sunarak dijital çağa uygun bir model oluşturabilmemizi sağlayabilecektir.

Bu değerlendirmeler çerçevesinde tezin sorusu cevaplandırılmış ve tezin hipotezi kapsamında yeni bir model üzerinde çalışılmasının uygun olacağı değerlendirilmiş; yeni bir modelin oluşturulmasında kullanılabilecek bazı faktörler incelenmiştir.

Sonuç olarak; güvenlik stratejisi tasarımı modeli olarak incelenen klasik model, dijital çağın ihtiyaçlarına cevap vermesi oldukça zordur. Bu nedenle hipotezde öne sürüldüğü şekilde klasik güvenlik stratejisi tasarım modelinde bazı değişikliklerin yapılması ve dijital çağ teknolojilerinden azami faydalanılması uygun olacaktır.

Bir sonraki bölümde bu bölümde incelenen hususlardan faydalanılarak, dijital çağ güvenlik stratejisi tasarım modeli önerilmesi ve bu modelin etkinliğinin artırılması için teknolojik gelişmelerden faydalanılması incelenecektir.

ÜÇÜNCÜ BÖLÜM

DİJİTAL ÇAĞA UYGUN BİR GÜVENLİK STRATEJİSİ TASARIM MODELİ ÖNERİSİ

Tezin birinci bölümünde güvenlik stratejisi tasarımının kavramsal çerçevesi; ikinci bölümünde ise dijital çağdaki güvenlik ortamının ve teknolojik gelişmelerin güvenlik stratejisi tasarımına ve yönetimine etkisi incelenmiştir. Aynı zamanda yeni bir modelin oluşturulmasını etkileyebilecek faktörler ortaya konulmaya çalışılmıştır. İnceleme sonucunda süratli değişim, belirsizlik ve muğlaklık, yeni aktörler, siber ve uzay ortamı, dijital çağ teknolojileri, dijital çağda karar verme, kriz yönetimi gibi konular ön plana çıkmıştır. Bu hususların işaret ettiği faktörler dikkate alınarak daha kullanışlı ve dijital çağa uygun bir model önerilebileceği düşünülmektedir.

Dijital çağın ortaya çıkarttığı yeni şartlar; sürekli ve süratle değişen stratejik güvenlik ortamına, güvenlik stratejilerinin aynı tempoda uyarlanma ihtiyacının gittikçe arttığını işaret etmektedir. Bu uyarlama ihtiyacı, güvenlik stratejisinin dayandığı politik amacın, millî menfaatin, tehdit kaynağının değiştirilmesi; yeni güç unsuru yaratılması, yeni konsept oluşturulması, hatta stratejinin tamamen terk edilmesi gibi tasarımın ana temelini oluşturan kararların dahi verilmesini kapsayabilir. Ayrıca tasarımda bir unsurun değiştirilmesi diğer unsurlar üzerinde domino etkisi yaratabilecektir. Değerlendirme esnasında bu faktörün de düşünülmesi önem taşımaktadır.

Diğer taraftan stratejinin temel yapı taşlarından birisi varsayımlardır. Bu varsayımlardan bazıları rakibin hareket tarzlarını ve muhtemel senaryoları konu alabilir. Dijital çağda rakip taraf kendi mantığı, kültürü, tarihten aldığı dersler gibi faktörlerin etkisinde beklenmeyen, hatta tasarımcıya çok ters gelecek şekilde tepkiler gösterebilecektir. Varsayımların geçersiz olduğu stratejinin icra süreci esnasında ortaya çıktıkça, stratejide değişiklik yapılması ihtiyacı ortaya çıkabilecektir. Dolayısıyla güvenlik stratejilerinin, güvenlik ortamının dijital çağdaki değişim hızına uygun şekilde güncelliğini koruması, etkinliğini devam ettirebilmesi oldukça zorlaşmıştır. Bu nedenle gelinen aşamada stratejiye ihtiyaç olup olmadığı bile sorgulanmaya başlanmıştır.

İlk bakışta klasik güvenlik stratejisi tasarlama modelinin yerine yalnızca dijital çağa uygun bir modelin önerilmesi ortaya çıkan problemlerin çözümünü sağlayabileceği izlenimi edinilebilir. Ancak daha önceki bölümlerde güvenlik stratejisi tasarım ve yönetiminin dijital çağa uygun bir şekle getirilmesi çerçevesinde ortaya konulan problem sahalarının çözümü maksadıyla yalnızca bir model ortaya konulmasının yeterli olmayacağı; beş konu üzerine yoğunlaşılmasının gerektiği sonucu ortaya çıkmıştır. Ancak bu şekilde stratejik güvenlik ortamının dinamik yapısına uyumlu, dinamik bir strateji tasarım modeli oluşturulması sağlanabilir. Bu beş konunun bir bütün halinde dikkate alınması güvenlik stratejinin daha gerçekçi, dijital çağın ihtiyaçlarına cevap verebilecek bir yapıda tasarlanabilmesini sağlayabilecektir.

Dolayısıyla bu beş konunun dijital çağa uygun strateji tasarlama modelinin bir parçası olarak kabul edilmesi uygun olacaktır. Bu konular:

Modelleme, prototip üretimi, deneme,

Periyodik değerlendirme sistemi,

Yeni güvenlik stratejisi modeli,

Strateji yönetim sistemi,

Dijital çağ teknolojilerinin kullanımı olarak ifade edilebilir.

Bu konulardan; modelleme, prototip üretimi, deneme konusu “Tasarım Süreci”alt başlığı altında; periyodik değerlendirme sistemi, yeni güvenlik stratejisi modeli, stratejik yönetim sistemi ise “Model Önerisi” alt başlığı altında incelenecektir. Teknoloji kullanımı ise her iki başlıkta da dikkate alınacaktır.

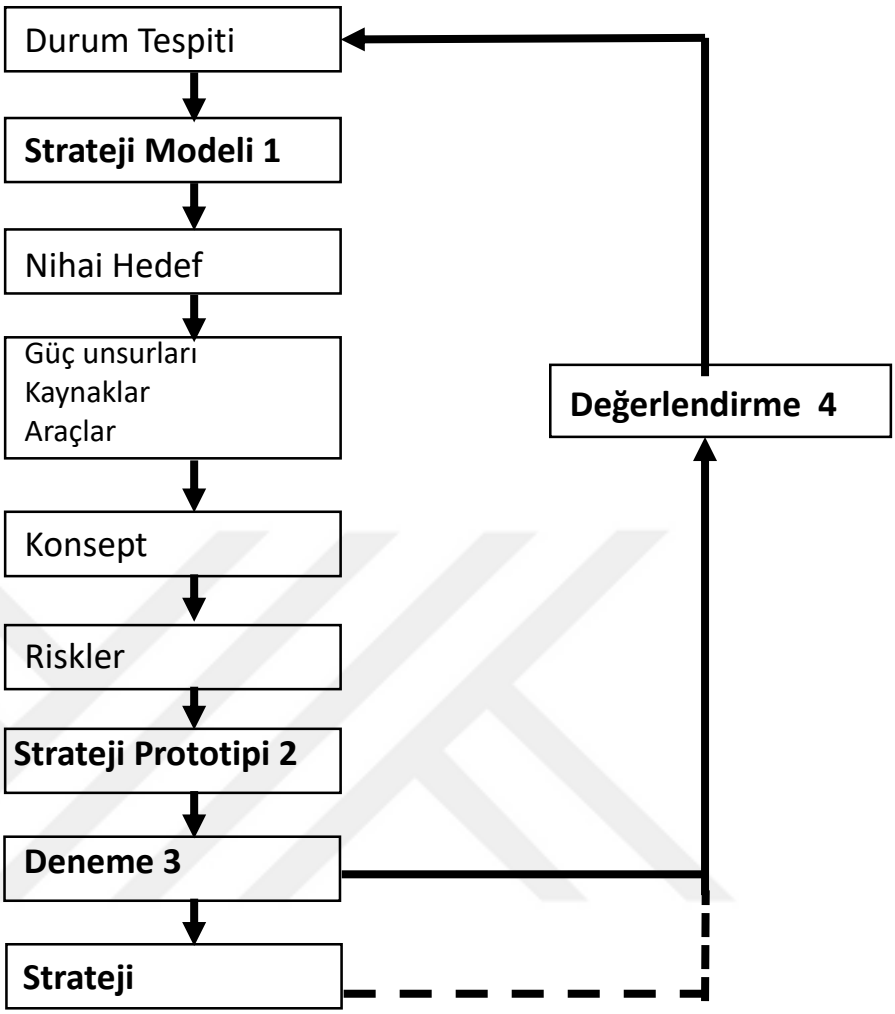
3.1. GÜVENLİK STRATEJİSİ TASARIM SÜRECİNE YÖNELİK MODEL ÖNERİSİ

Birinci bölümde, Şekil 1.3’te ortaya konulan model; durum tespiti, nihai hedef, güç unsurları-kaynaklar-araçlar, konsept, riskler olmak üzere beş ana safhayı içermektedir. Bu süreci dijital çağa uyumlu hale getirebilmek maksadıyla dört yeni safha eklenebilir. Bunlar; stratejinin modelinin oluşturulması, stratejinin prototipinin yaratılması, prototipin denenmesi, değerlendirme safhaları olabilir. Bu safhalar ilave edilerek

önerilen tasarım süreci modelinin yeni hali Şekil 3.1'de gösterilmektedir. Şekilde koyu renkle gösterilenler yeni ilave edilen safhalardır.

Durum tespitini müteakip güvenlik stratejisinin bir modelinin oluşturulması, stratejik model üzerinde simülasyonlar yapılarak; nihai hedefin, güç unsurlarının, konseptin ve risklerin daha gerçekçi belirlenebilmesini sağlayabilecektir. Çıkan sonuçlarla güvenlik stratejisinin belirlenen unsurlarından oluşturulan bir güvenlik stratejisi prototipi denemeye tabi tutulabilecek, deneme sonucunda elde edilen sonuçlar durum tespiti safhasından itibaren değerlendirmeye tabi tutularak güvenlik stratejisi unsurlarının başarı şansı yüksek olacak şekilde belirlenebilmesi sağlanabilecektir. Bu dört safhanın eklenmesiyle birlikte, bir mühendisin araba, silah vb. tasarlamasına benzer bir sistem yaklaşımıyla, başarı şansını arttırabilecek şekilde stratejinin tasarımı gerçekleşmiş olabilecektir. Benzer bir yaklaşım stratejinin yönetiminde de kullanılabilecektir. Tasarım anlayışı ile stratejinin başarı şansı arttırılırken, icra ve yönetim sürecinde de stratejinin güncel kalması sağlanabilecektir. Ancak burada strateji konusunda yapılacak modelleme, deneme gibi çalışmalar basitlik esas alınarak yapılmalıdır. Bunun aksi bir yaklaşım stratejik tasarımın ve yönetimin başarı şansını olumsuz etkileyebilecektir. Bu yaklaşım çalışmada bir katkı olarak sunulmaktadır. Müteakip maddelerde sürece yeni ilave edilen; modelleme, prototip üretimi, deneme konuları incelenmiştir.

Şekil 3.1: Dijital Çağ Güvenlik Stratejisi Tasarım Süreci



Kaynak: Yazar tarafından oluşturulmuştur.

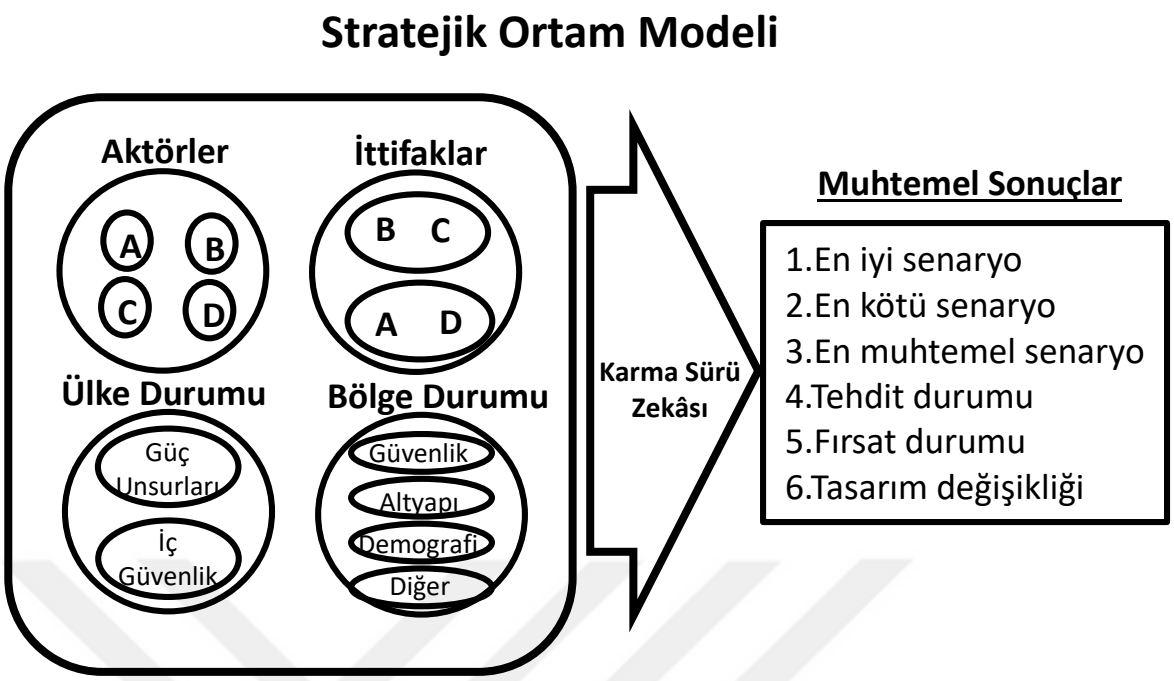
3.1.1. Stratejik Ortam Modeli

Tasarım öncesi, prototip üretilmeden stratejik seviyede, teorik olarak bir modelin oluşturulması; çalışmaların daha etkin yapılması, olabilecek hataların başlangıçta giderilebilmesi, stratejik mantığın daha gerçekçi oluşturulabilmesi gibi faydaları sağlayabilecektir. Taktik seviyede model oluşturulması ve tasarım yapılması stratejik seviyeye göre çok daha kolaydır. Bunun en önemli nedenleri; stratejik seviyenin geniş bir alanı, uzun bir zaman aralığını, daha kapsamlı güç unsurlarını kapsaması, aktörlerin ve paydaşların sayısının, çeşidinin artmış olması gibi faktörlerdir. Bunun yanında taktik seviyedeki çalışmalar nispeten cari olayları ve yakın geleceği içermesi nedeniyle

gözle çok daha kolay görülebilir ve modellenebilir. Örneğin bir gün önceden herhangi bir şehirdeki güvenlik olaylarının meydana gelebileceğinin haber alınması, bu olayların engellenmesi maksadıyla tedbir alınması ve taktik seviye bir modelin oluşturulması daha basittir. Bu modelde topluluk, güvenlik kuvvetleri, vatandaşlar gibi aktörler dikkate alınabilir. Olayın muhtemel yeri de şehirde belirli olduğu için, olay mahallinin haritası veya fotoğrafının üzerine aktörlerin yerleştirilmesi planlama için yeterli bir model oluşturabilecek, bu model satranç tahtası gibi kullanılabilecektir. Ancak şehrin tamamının, güvenlik dâhil, uzun vadeli, stratejik seviyede yönetimi konusunda yapılacak çalışma çok daha karmaşık ve tahayyül edilmesi daha zor bir problem ortaya koyabilecektir. Doğal olarak stratejik seviye modelin üretilmesi daha zor olabilecektir.

Stratejik seviyede kullanılabilecek bir model önerisi Şekil 3.2'de gösterilmektedir. Bu çalışmada, bu strateji modeli bir katkı olarak sunulmaktadır. Model oluşturulmadan önce, güvenlik stratejisi tasarım amacının ve buna bağlı olarak problem tanımının gözden geçirilmesi önemlidir. Bu hususların belirlenmesi strateji modelinin oluşturulmasında hayati önemi haizdir. Amaca hizmet etmeyecek yapıdaki bir model daha başlangıçtan itibaren yanlış istikamette ilerlenmesine neden olabilecektir. Modelde önerilen elemanlar değiştirilebilir, ilave elemanlar eklenebilir veya elemanlardan bazıları çıkarılabilir. Hatta tamamen farklı bir yaklaşımla başka bir model de üretilebilir. Modelden amaç tasarımcıların zihin haritalarının, düşüncelerinin, öngörülerinin oluşmasını; gelecekte oluşabilecek gelişmelerin tahmin edilmesini kolaylaştırabilecek bir model ortaya konulabilmesidir.

Şekil 3.2: Stratejik Ortam Modeli



Kaynak: Yazar tarafından oluşturulmuştur.

Modelde öncelikle stratejik önemi olan bölge belirlenmelidir. Bölge, tek bir coğrafi alan, şehir, ülke olabileceği gibi geniş bir bölge, hatta küresel bir güç için bütün yeryüzü olabilir. Bölgenin özelliklerini yansıtan; demografi, coğrafya, güvenlik durumu, alt yapı gibi ihtiyaç duyulan diğer bilgiler tespit edilebilir. Terörizm, istihbarat, bilgi harekâtı, teknoloji geliştirme gibi fonksiyonel güvenlik stratejisi tasarımında coğrafi alan belirlenemeyebilir. Bu nedenle modelin oluşturulması daha zor olabilir. Bu maksatla, sistem dinamikleri veya dijital çağın sunduğu diğer modelleme teknikleri kullanılabilir.

Bölge tespit edildikten sonra bu bölgedeki aktörler tespit edilir. Her bir aktörün millî menfaatleri, bununla bağlantılı olarak bölgeye yönelik faaliyetlerinin amaçları gibi hususlar ortaya konulabilir. Aktörlerin bölgeye yönelik menfaatleri hayati, yaşamsal, öncelikli gibi bir derecelendirmeye tabi tutulabilir. Bu aktörlerin daha önce incelendiği gibi tehdit olma durumları ortaya konulabilir. Bu aktörlerin oluşturdukları ittifaklar en az aktörler kadar önemlidir. İttifakların menfaatlerinin ve amaçlarının belirlenmesi diğer önemli bir unsurdur. En son olarak stratejiyi tasarlayan aktörün mevcut durumu; güç unsurları ve iç güvenlik durumu gibi faktörlerden faydalanılarak tespit edilebilir. Bu unsurların çoğu zaten durum tespit safhasında ortaya konuluş

olmalıdır. Bazı hususlar bilinmese bile varsayım olarak ortaya konulabilir. Varsayımın doğruluğu teyit edilmeye çalışılabilir.

Modelin ana elemanları belirlendikten sonra tespit edilen bölgeye yönelik en iyi, en kötü, en muhtemel senaryolar, tehdit ve fırsat durumu belirlenmeye çalışılır. En iyi senaryo, stratejiyi tasarlayan aktörün millî menfaatleri için en uygun şartları sağlayan, buna bağlı olarak ortaya konulan tehdidin etkisiz hale getirilebildiği, fırsatların değerlendirilebildiği bir senaryodur. En kötü senaryo ise bunun tam tersidir ve olumsuz sonuçlar ortaya çıkma ihtimali yüksektir. En muhtemel senaryo ise mevcut şartlarda, gerçekleşme ihtimali en yüksek senaryodur. Bu senaryo en kötü, en iyi veya her ikisinin bir karışımı olabilir. Tasarım muhtemel senaryo esas alınarak yapılırken, en kötü senaryoya yönelik tedbir alınması gerekir. Senaryo tabanlı yöntemin yerine aktörlerin muhtemel hal tarzları ortaya konularak da çalışma yapılabilir. Bu yöntem daha ziyade taktik seviyede, nispeten daha az faktörün dikkate alınması gerektiği bir ortamda kullanılabilir. Stratejik seviyede aktör sayısı fazla, zaman aralığı uzun, coğrafya geniş olması gibi nedenlerden dolayı senaryo tabanlı çalışılması daha basit olabilecektir. Ancak senaryo ile birlikte aktörlerin, özellikle de etkin aktörün hal tarzlarının senaryo ile birlikte tespit edilip dikkate alınması daha iyi bir modelleme ortamı sağlayabilecektir.

Ortaya konulan muhtemel senaryo çerçevesinde aktörlerin tehdit durumu konusunda bir fikir elde edilebileceği gibi muhtemel fırsatlar konusunda da bir fikir oluşturulabilir. Bu çalışmada stratejik seviyede problem mevcut tehdidin veya fırsatın yanında gelecekte oluşabilecek tehdit veya fırsatların ortaya konulabilmesidir. Strateji uzmanları deneyim kazandıkça bu konuda analiz yapma kabiliyetleri artabilecektir. Bu konuların model esas alınarak seminer çalışması çerçevesinde tartışılması ve analiz edilmesi bile bu hususlarda önemli ipuçlarının oluşmasını sağlayabilecektir.

Modelleme esas alınarak stratejinin yönetimi esnasında strateji tasarımının temel parametrelerinde değişiklik ihtiyacı da değerlendirilebilir. Bu şekilde dinamik olan stratejik güvenlik ortamındaki değişiklikler daha kolay tespit edilip uyum sağlanabilecektir. Bu değerlendirmeler yapılırken daha önce incelenen karma sürü anlayışı kullanılabilir. Örneğin senaryolar tespit edilirken uzmanlardan oluşan bir sürüden (gruptan), belirlenmiş senaryoları iyi, kötü ve muhtemel olarak değerlendirmesi istenebilir. Sürü terimi; dijital çağda, doğadaki kuşlar, karıncalar,

arılar gibi canlıların gösterdiği doğal, ancak olağan üstü doğru tepkilerde kullanılan yöntemlerden faydalanılabilmesi maksadıyla kullanılmaktadır.

BV ve YZ kullanılarak aktörlerin ve ittifakların, davranış analizleri yapılabilir, eğilimleri tespit edilebilir. Yine BV ve YZ kullanılarak daha önce incelendiği gibi tehdit olma durumları değerlendirilebilir. Uzman değerlendirmeleri eklenerek değerlendirmeler daha sağlıklı bir yapıya kavuşturulabilir.

3.1.2. Güvenlik Stratejisi Prototipi

Çok özet olarak; herhangi bir ürünün mühendislik prensipleri çerçevesinde önce teorik olarak tasarlanması, piyasaya sürülmeden önce bir prototipinin üretilmesi ve denenmesi, deneme sonucunda belirlenen problem sahaları giderilerek, tekrar bir prototip oluşturularak denenmesi ve nihai ürüne ulaşılması, tasarım yaklaşımıyla ürünlerin hazırlanması yöntemidir. Benzer bir yaklaşımın strateji oluşturulmasında da kullanılabileceği değerlendirilmektedir. Stratejik tasarım yaklaşımında en önemli faktörlerden birisi zamandır. Bazen yeterli zaman olmadığında strateji tasarımında bu yöntemin kullanılması mümkün olmayabilir. Bu durumda dahi çok genel bir çerçevede hazırlanan bir prototipin üretilmesi ve denenmesi düşünülmelidir.

Hazırlanan stratejik ortam modeli kullanılarak, tehdit durumunu karşılayabilecek, fırsatları değerlendirebilecek; nihai hedef, güç unsurları, konsept, risklerden oluşan bir güvenlik stratejisi prototipi hazırlanabilir. Güvenlik stratejisi prototipinin yanında varsayımlar, millî menfaatler, stratejinin tasarlanma amacı, problemin tanımı, tehdit-hedef ilişkisi gibi durum tespitinde ortaya konulan, stratejinin tasarlanmasında kullanılan stratejik mantık da bu prototipin bir parçası olarak kabul edilmelidir.

3.1.3. Güvenlik Stratejisi Prototipinin Denenmesi

Mühendislik alanındaki tasarım süreci ile strateji tasarım sürecinin ayrıldığı en önemli noktalardan birisi deneme safhasıdır. Mühendisler tasarladıkları ürünün prototipini neredeyse gerçek şartlarda, belirli bir deney ortamında test edebilirler. Ancak güvenlik stratejisi prototipinin denenmesi için seminer çalışması, bilgisayar destekli veya manuel stratejik seviye oyunlama, masa başı tatbikatı gibi teknikler kullanılabilir.

Gerçek şartlarda deneme oldukça zordur. Stratejik seviye oyunlamanın genel olarak iki temel amacı vardır. Bunlar eğitim ve analiz çalışması olarak ifade edilebilir. Burada stratejik seviyede analiz çalışması üzerinde durulacaktır.

Harp oyunlaması tekniği orduların harbe hazırlık seviyelerinin arttırılması, kuvvet ihtiyaçlarının tespit edilmesi, herhangi bir planın denenmesi, askeri liderlerin eğitilmesi gibi maksatlarla 1800'lü yılların başından beri kullanılmaktadır. Harp oyunlaması özet olarak; kırmızı ve mavi iki tarafın olduğu, hakemlerin nezaretinde, belirli kurallar çerçevesinde gerçek çatışmaların dershane ortamında simüle edilmesidir. Taraf sayısı turuncu, kahverengi, sarı gibi daha da fazla olabilir. Orduların başlangıç durumundan (start exercise, startex) itibaren hedefin ele geçirilmesine kadar icra ettikleri bütün görevler dinamik olarak modellenir. Orduların intikalleri, manevraları, atışları, hava taarruzları, birbirleriyle yakın muharebeye girmeleri gibi bütün görevleri modellenir. Atışlar, yakın muharebe, manevra gibi görevlerin modelleme sonucu, bir sonraki safhaya girdi olurlar. Bu sonuçlar ilerleme hızı, zayiat, lojistik malzeme sarfı şeklinde olabilir. Sonuçlar daha önce belirlenmiş bazı kurallar, formüller ile hesaplanırlar. Harp oyunları dijital çağda bilgisayar destekli olarak çok daha hızlı tasarlanır ve oynanabilir. Ancak birinci bölümde, kavramsal çerçevede incelenen politik ve icra safhalarının dikkate alınmasını içeren stratejik seviye bir oyunlamanın, taktik seviye oyunlamaya göre tasarlanması ve oynanması zordur. Bu nedenle genellikle stratejik seviye oyunlamalar seminer çalışması, masa başı tatbikatı gibi tekniklerle hazırlanır.

Bu çerçevede güvenlik stratejisi tasarımı prototipinin denenmesi için kullanılacak oyunlama, seminer çalışması veya masa başı tatbikatı şeklinde hazırlanabilir. Oyunlamanın başında, oyunlamanın amacı ortaya konulmalıdır. Buradaki genel amaç prototip olarak hazırlanmış bir güvenlik stratejisinin denenmesidir. Stratejik modelde tespit edilmiş aktörler, ittifaklar ve stratejik coğrafi bölgenin nasıl temsil edileceğine karar verilir. Aktörler ve ittifaklar kendi stratejilerini hazırlarlar, coğrafi bölge için uygun bir harita hazırlanabilir. Aktörler ve harita, dünya üzerindeki gerçeklikle ilgisi olmadan jenerik olarak yaratılmış olabilir. Oyunlamanın yapılacağı periyodlar belirlenir. Stratejik seviye oyunlama için altı ay, bir sene gibi bir zaman aralığı kullanılabilir. Çünkü stratejik seviye hamlelerin, etkilerin, sonuçlarının alınması uzun bir zaman aralığına ihtiyaç duyar. Ayrıca güvenlik stratejisi uzun bir zaman aralığını kapsayacağından dolayı kısa zaman aralıkları ile oyunlamanın

yapılması hem stratejik seviyenin özelliklerine hem de üç-beş yıl gibi uzun bir zaman aralığında, dijital çağın belirsizlik özelliği dikkate alındığında, geleceğe yönelik senaryoların tahmin edilmesi oldukça zor, hatta neredeyse imkânsız olabilecektir. Bu nedenle stratejinin kapsadığı zaman aralığının tamamının yerine kritik olan belirli dönemlerin oyunlamasının yapılması düşünülebilir.

Stratejik seviye seminer çalışmasında taraflara genel bir senaryo ve başlangıç durumu verilir. Müteakiben verilecek ara durumlarla oyunun ilerlemesi sağlanır. Tarafların reaksiyonları, hamleleri daha önce belirlenmiş kurallar çerçevesinde hakemler tarafından değerlendirilir. Yöneticiler veya kontrolörlerin görevi oyunlamanın amacı veya planlamanın dışına çıkmasının engellenmesidir. Aktörleri temsil edecek personel veya takım söz konusu aktörün özellikleri, yapısı, davranışları hakkında bilgi sahibi, hatta uzman olmalıdır. Strateji protipini deneyen taraf ise ilgili kamu kurum ve kuruluşlarından gerçek temsilciler ile katılabilir. Bu çerçevede örnek bir stratejik seviye oyunlama tertibi Şekil 3.3'te sunulmuştur. Bu oyunlama tertibi bir katkı olarak sunulmaktadır. Amaca uygun, daha değişik tertipler de kullanılabilir.

Dijital çağda bugün için aktörlerin temsil edilmesi şahıslar tarafından yapılırken, gelecekte, YZ kullanılarak aktörlerin özellikleri ile eğitilmiş bilgisayarlar sayesinde aktörlerin, hakemlerin temsil edilmesi, kuralların tanımlanması sağlanabilecektir. Hatta YZ tarafından strateji tasarımının bütününün başarı şansının değerlendirilmesi bile yapılabilecektir. Benzer yaklaşım insanın satrançta makineye karşı oynaması modelinde görülmektedir. Taktik seviyede sanal kum sandığı kullanılarak hal tarzlarının denemesi çalışmaları günümüzde devam etmektedir. Hologramlarla aktörlerin temsil edilmesi, konuşturulması, coğrafyanın sanal olarak ortaya konulması gibi hususlar yakın bir gelecekte kullanıma sunulabilecektir. Ayrıca bilindiği gibi internette birçok strateji oyunu bulunmaktadır. Dolayısı ile bu oyunlara benzer şekilde güvenlik stratejilerinin dijital ikizlerinin oluşturulması mümkün olabilecektir. Ancak ne olursa olsun insan unsurunun, duygularının bir şekilde bu modele dâhil edilmesi uygun olacaktır.

Stratejik oyunlamadan önce; amaç, aktörlerin özellikleri, hakemler, genel ve başlangıç senaryosu, verilecek ara durumlar, sorulacak sorular, kurallar, oyunlamanın sonlandırılması gibi hususların iyi bir çalışma ile profesyonel bir ekip tarafından belirlenmesi oyunlamanın başarısı için şarttır. Ancak oyunlama neticesinde stratejinin kesin olarak başarılı veya başarısız olabileceği sonucuna ulaşılması gibi yanlış bir

izlenim edinilmemelidir. Bunun yerine belirli dönemlerde oluşabilecek problem sahalarının tartışılıp, strateji tasarımının sorgulanması, sorunlarının giderilmesine çalışılması daha doğru bir hareket tarzı olabilecektir.

Prototipin stratejik oyunlama ile denenmesi yöntemi yalnızca güvenlik stratejisinin tasarımı esnasından değil icra esnasında da, uygun zaman aralıkları ile tekrar edilerek güvenlik stratejisinin güncel kalması, sorunların tespit edilmesi, krizlerin önceden hissedilmesi sağlanabilir. Bu nedenle stratejik oyunlama konusuna ayrı bir önem verilmesi uygun olacaktır.

Dijital çağda, oyunlama yöntemiyle güvenlik stratejisi tasarımı çalışmaları yapılmaya devam edilmektedir. Bu maksatla "Hedgemony" adı verilen bir manuel stratejik seviye oyun tasarlanmış ve ABD'nin 2018 Millî Güvenlik Stratejisi Tasarımı çerçevesinde faydalanılmıştır.[93]

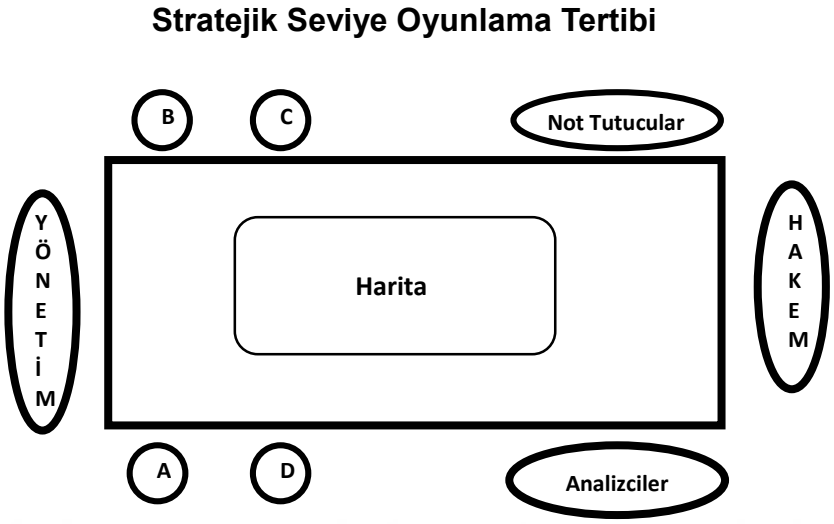
3.1.4. Güvenlik Stratejisi Prototipinin Değerlendirilmesi

Prototipin denenmesine başlamadan önce değerlendirmenin nasıl yapılacağına yönelik bir planlama yapılması gerekmektedir. Aslında değerlendirmenin planlanması durum tespit safhasında hem prototipin değerlendirilmesi hem de gerçek güvenlik stratejisinin icra esnasında nasıl değerlendirileceğinin ortaya konulması için hayati önemi sahiptir. Güvenlik stratejinin icrası esnasında değerlendirilmeye yönelik inceleme dijital çağa uygun bir strateji modeli başlığı altında yapılacaktır.

Prototipin denenmesi safhasında nelerin değerlendirileceği, durum tespitinde ortaya konulan stratejinin mantığı, millî menfaatler, millî güç unsurlarının yeterlilik durumu ile tasarımında ve icrada değer taşıyan senkronizasyonun sağlanması, kriz yönetimi gibi hususları içerebilir. İlgili personel oyunlama safhasında özellikle bu hususlara dikkat eder ve not tutar. Zaten oyunlamanın tasarımında değerlendirilecek olan konulara uygun olarak senaryonun oluşturulması, ara durumlar ile değerlendirme konularının çalışılabilmesi, tartışılabilmesi için şartların oluşturulması üzerinde durulması uygun olacaktır.

[93]Wong, Yuna Huh ve Health, Garrett, *Is the Department of Defense Making Enough Progress in Wargaming*?, 2021.

Şekil 3.3: Stratejik Seviye Oyunlama Tertibi



Kaynak: Yazar tarafından oluşturulmuştur.

Prototipin oyunlaması tamamlandıktan sonra bir faaliyet sonu incelemesi yapılarak ve değerlendirilmesi planlanan konuların tartışılması yapılarak, durum tespitinde belirlenen konular ile güvenlik stratejisi prototipinin elemanları konusunda değerlendirmeler yapılabilir. Gerekli düzeltmeler yapıldıktan sonra yeniden oluşturulan prototip yeni bir deneye tabi tutulabilir. Burada kullanılan mantık, aynen bir laboratuvarda deney ortamının hazırlanması ve deneyin yapılması yöntemi ile benzerdir.

3.1.5. Güvenlik Stratejisi Tasarım Sürecinde Kullanılabilecek Dijital Çağ Teknolojileri

Güvenlik stratejisi tasarım sürecinde dijital çağda kullanılan, başta BV ve YZ olmak üzere bazı teknolojilerin amaca uygun olarak, yerinde kullanılması güvenlik stratejisi tasarımının başarı şansını arttırırken, stratejinin güncel kalmasını ve daha etkin yönetilebilmesini sağlayabilecektir. Bu teknolojilerin ortaya konulması gelecekte yapılacak teknolojik çalışmalara girdi sağlayabilecektir. Bu maksatla kullanılabilecek yöntemler, tasarım süreci esas alınarak müteakip maddelerde bir katkı olarak önerilmiştir. Bu teknolojilerin geliştirilmesi maksadıyla BV ve YZ çalışan

mühendislerle güvenlik stratejisi uzmanlarının beraber çalışması gerekmektedir. Teknolojinin kullanımının şartlara ve içerisinde bulunulan duruma göre değişebileceği, her bir durumun ayrı bir kullanım yöntemini gerektirebileceği akılda tutulmalıdır. Strateji tasarım aşaması safhaları esas alınarak teknolojinin muhtemel kullanım alanları aşağıda belirtilmektedir. Teknolojinin gelişmesiyle paralel olarak liste gözden geçirilmelidir. Bu çalışmada bu öneriler katkı olarak sunulmaktadır.

Durum tespiti safhası:

Küresel veya bölgesel olayların tespiti,

Bu olaylardaki veya gelen bilgilerden anomali tespiti,

Potansiyel tehditlerin belirlenmesi,

Erken uyarı sistemi,

Değişik yöntemler ile internetten açık kaynak bilgisi elde edilmesi,

Görüntülerin, seslerin ve metinlerin duygu analizinin yapılması,

Medya, internet ve diğer kaynaklardan gelen bilgilerin önemli olan kısımlarının özetlenmesi,

Bilgilerin birleştirilmesi ve görselleştirilmesi,

Sensörlerden gelen bilgilerin analiz edilmesi olarak ifade edilebilir.

Stratejik Model Üretilmesi:

Aktörlerin ve ittifakların modellenmesi,

Sanal olarak harita veya stratejik seviyede üzerinde çalışılacak ortamın oluşturulması,

Hedef bölgeye yönelik coğrafi, demografik, altyapı gibi bilgilerin analizi,

Ülke durum analizi,

Karma sürü yöntemiyle; senaryoların, tehdit ve fırsat durumu ile tasarım değişikliği ihtiyacının belirlenebilmesi olarak ifade edilebilir.

Nihai Hedef:

Millî menfaatlerin sınıflandırılması,

Tehditlerin sınıflandırılması,

Millî menfaat-tehdit-hedef gibi stratejik mantık kullanılarak nihai hedef ve alt hedeflerin tespiti,

Nihai hedef ve alt hedeflerin sayısal hale getirilerek ölçülebilmesi olarak ifade edilebilir.

Millî Güç Unsurları:

Millî güç durumunun sayısal olarak ifadesi ve takibi,

Geliştirilmesi gereken millî güç durumunun analizi olarak ifade edilebilir.

Konsept:

Hedefe uygun millî güç tahsisi,

Konsept modellenmesi ve denenmesi,

Siber savunma, bilgi harekâtı gibi teknolojik imkân kabiliyetlerin kullanımı olarak ifade edilebilir.

Riskler:

Risklerin tespiti, listelenmesi, takibi,

Maliyet analizi,

Verimlilik analizi olarak ifade edilebilir.

Güvenlik Stratejisi Prototipi ve Prototipin Denemesi:

Aktörlerin ve İttifakların modellenmesi,

Stratejik seviye oyunlamanın yapılması,

Performansın ölçülmesi olarak ifade edilebilir.

3.2. GÜVENLİK STRATEJİSİ TASARIMI VE YÖNETİMİ MODELİ ÖNERİSİ

Dijital çağdaki değişim, dönüşüm ve şartlar dikkate alınarak güvenlik ortamına ayak uydurabilecek, güncel kalabilecek bir güvenlik stratejisi modelinin geliştirilmesi bir ihtiyaç olarak kendisini hissettirdiği daha önce vurgulanmıştır. Bu çerçevede özet olarak aşağıda belirtilen problemlere cevap verebilecek bir modelin oluşturulması öngörülmektedir.

Süratli değişime ayak uydurabilecek,
Kapsamlı yaklaşıma imkân sağlayabilecek,
Koordinasyonu sağlayabilecek,
Teknoloji kullanımını kolaylaştırabilecek,
Stratejik şokları veya krizleri yönetebilecek,
Proaktif bir yaklaşımı mümkün kılacak,
Süratle karar verilmesini sağlayabilecek,
Stratejik, Operatif, taktik seviye arasındaki uyumu sağlayabilecek,
Yönetimi kolay olacak,
Belirsizliklere azami cevap verebilecek bir sistem ortaya konulmaya çalışılmıştır.

Bu ana başlıklara cevap verebilecek dijital çağa uygun bir tasarım modeli Şekil 3.4'te önerilmektedir.

Daha önceki bölümlerde belirtildiği gibi güvenlik stratejisi tasarım mantığının temelini, mevcut durumdan millî menfaatlerin gerçekleştirilebileceği düşünülen nihai hedefe ulaşmak oluşturmaktadır. Bu çerçevede hazırlanacak konsept eldeki araç ve kaynaklar ile nihai hedefe ulaşılmasını sağlayacaktır. Bilindiği gibi birinci bölümde "Stratejik Konsept Tasarımı" başlığı altında incelendiği gibi konseptin değişik şekillerde ortaya konulması mümkündür. Şekil 3.4'teki modelde belirli zaman aralıkları dikkate alınarak, örnek olarak dört genel yol haritası ve her bir yol haritasının gerçekleştirmesi için hedefler belirlenmiştir. Bu hedeflerin birleşimi nihai hedefe ulaşılmasını sağlayacağı öngörülmektedir. Bu yol haritalarının her birisinin içerisinde tek çizgi ile gösterilen değişik araçların ayrı ayrı yol haritaları ve ara hedefleri bulunmaktadır. Bu araçlar; Askeri, Bilgi harekâtı, Ekonomik ve Diplomatik olarak baş harfleri gösterilerek belirtilmiştir. Genel yol haritalarının içerisinde hedefin özelliğine göre değişik araçların kullanımı öngörülmektedir. Bu araçlara ilave; hukuk, kolluk kuvvetleri, teknoloji gibi başka araçlar da ilave edilebilir.

Modelin üst kısmında zaman aralıkları belirtilmiştir. Geçmişte strateji tasarımları 10, hatta 20 yıllık bir aralıkla yapılmaya çalışılırken dijital çağda daha kısa aralıkların esas alınması uygun olacaktır. Bu çerçevede altı aylık dönemlerle iki senelik bir süreç dikkate alınmıştır. Duruma göre strateji tasarım süresi 10 yıl gibi daha uzun bir zamanı esas alması durumunda yıllık gözden geçirmeler ve değerlendirmeler önem kazanabilecektir. Tasarlanacak stratejinin konusuna göre dönemlerin, sürelerin değiştirilmesi düşünülebilir. Her bir periyodun sonunda bir sonraki periyoda geçişte değişen şartlara stratejik tasarımın uyarlanabilmesi için ilave talimatlar yayımlanabilir. Daha önce tasarım sürecinde belirtilen stratejik oyunlamanın değerlendirme sisteminden elde edilen veriler dikkate alınılarak icra edilmesi önemli faydalar sağlayabilecektir.

Tasarımda kullanılan ara hedefler, stratejinin istenen istikamette ilerleyip ilerlemediğinin ortaya konulması maksadıyla önemli göstergeler olarak algılanabilir. Ancak hedeflerin ele geçirilmesi ile ortaya çıkan sonuçlar sistem yaklaşımı içerisinde daha önce tasarlanan ile mukayese edilmesi, eğer beklenen sonuçlar oluşmamış ise yeni bir ara hedefin ortaya konulması, daha fazla güç unsuru tahsis edilmesi gibi beklenen sonucun alınmasını sağlayabilecek girdiler yapılması üzerinde durulmalıdır. Ayrıca ara hedefler dijital çağda süratle değişen güvenlik ortamına süratle uyum sağlanması için alınan ve alınması gereken tedbirlerin değerlendirilmesi için önemli bir fırsat sunmaktadır.

Genel yol haritalarının içerisindeki araçları kullanan her bir kurumun planlamaları operatif, yani kendi branşlarını esas alan planlamalar olarak düşünülebilir. Bu nedenle stratejik seviyede ayrıntılı bir planlama yapılmasına gerek olmadığı düşünülse bile, bu araçların beklenen sonuçları üretip üretmediklerinin stratejik açıdan kontrol edilebilmesi maksadıyla bu seviyede ara hedeflerin takip edilmesi önem taşımaktadır. Bu şekilde taktik ve operatif seviye ile stratejik seviye arasında uygun bağlantı kurulabilmesi sağlanabilecektir. Dolayısı ile icra ile stratejik hedefin irtibatlandırılması için önemli bir fırsat oluşabilecektir.

Dijital çağda değişim hızına ayak uydurabilmemizi sağlayacak diğer önemli bir konu muhtemel kriz/risk noktalarının önceden tahayyül edilmesi ve takip edilebilmesidir. Herhangi bir kriz/risk noktasına yaklaşırken stratejik süreç içerisinde krizin/riskin daha iyi tanımlanabilmesi, anlaşılabilmesi ve alınan tedbirlerin gözden geçirilebilmesi sağlanabilecektir. Başlangıçta belirlenebilen kriz/risk noktalarının yanında yapılan değerlendirmeler neticesinde yeni kriz noktaları belirlenebilir ve

planlamalar yapılabilir. Değerlendirme çalışması ve stratejik oyunlama esnasında ileriye yönelik muhtemel kriz noktalarının belirlenmesi, krizlerin önceden hissedilmesi ve tedbir alınması için önemli bir kuvvet çarpanı olabilecektir. En azından kriz veya risk olasılıklarının araştırılması için gayret sarf edilecektir.

Karar noktaları genel olarak önemli bir sorunla veya karar almayı gerektiren bir durumla karşılaşmadan, ön almak maksadıyla tespit edilen noktalar olarak tanımlanabilir. Öncelikle sorun veya karar almayı gerektiren durum tespit edilmeli müteakiben karar noktası belirlenmelidir. Örneğin herhangi bir kriz daha ortaya çıkmadan belirli bir süre öncesinden krizin varlığının kabul edilmesi veya ihtimalat planının devreye sokulması kararı alınabilir. İhtimalat planlamasının amacı stratejik gidişatın tekrar normal yörüngesine oturtulması ve stratejik istikametten sapılmasının engellenmesi maksadıyla bir dizi önlemin devreye sokulması olarak ifade edilebilir. Değerlendirme sonucunda stratejik tasarımın temel unsurları olan hedef-güç unsuru-konsept gibi elemanlarda değişiklik, hatta stratejik tasarımın tamamının gözden geçirilmesi bile gündeme gelebilir. Ancak yapılacak değişikliklerde mümkün olduğu kadar başlangıçta yapılan tasarımın korunması icrada kolaylık ve devamlılık sağlamada önem taşımaktadır. Stratejik tasarımın bir anda tamamının değiştirilmesi, alt kademelerde yapılması gereken faaliyetler de dikkate alındığında oldukça zahmetli ve hassas bir konudur.

Strateji tasarımında en önemli konulardan birisi de güç unsurlarının yeterli olmamasıdır. Bu nedenle bir önceliklendirme yapılması veya sıklet merkezi belirlenmesi uygun olacaktır. Bu anlamda örnek olarak belirlenmiş olan dört genel yol haritasından birisinin ve her bir genel yol haritasının içerisinde ise bir aracın ve/veya kurumun sıklet merkezi ve/veya koordinatör olarak belirlenmesi, ayrıca kritik hedeflerin birleştirilmesiyle kritik stratejik istikametin planlanması tasarım ve icrada önemli kolaylıklar sunabilecektir. Önerilen bu tedbirler belirsizliğin ve muğlaklığın hâkim olduğu dijital çağda güvenlik stratejisinin genel istikametinin belirlenmesini sağlayabilecektir. Belirlenen bu tedbirlerin konseptin daha kolay oluşturulmasına da faydası olabilecektir.

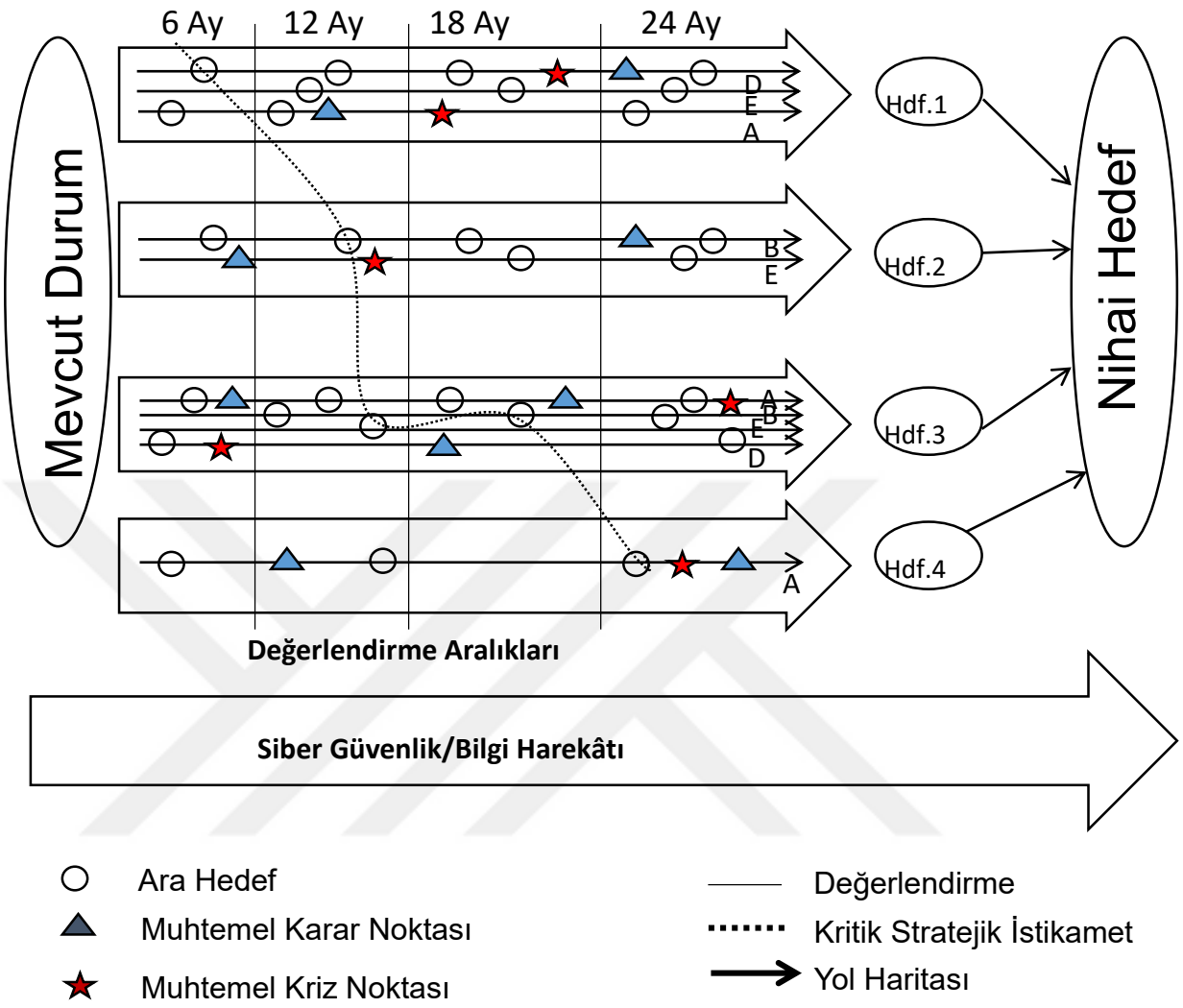
Ara hedefler, karar noktaları, kriz/risk noktaları gibi kontrol noktalarına doğrusal veya lineer bir şekilde, birbiri ardına ulaşılması veya beklenen zaman aralığında ulaşılması beklenilmemelidir. Bazı hedeflere beklenilenden önce ulaşılabilecek, bazılarına ise ulaşılamayacaktır. Bu nedenle yapılacak değerlendirmede tasarımın tamamı dikkate alınmalıdır.

Yukarıda açıklanan tasarımın, belirlenen problem sahalarına cevap verebilecek bir çatı sağlayabileceği düşünülmektedir. Ancak birinci bölümde incelendiği gibi strateji tasarımının bir hipoteze dayandığı ve bilinmeyenlerin oldukça fazla olduğu dikkate alındığında tasarımcının veya icrayı yönetenlerin stratejik şoklara ve değişiklik yapmaya her an hazır olması ve şaşırmaması gerekmektedir. Eğer değişiklik yapılacaksa da dikkatli bir şekilde yapılarak stratejik mantığın devamlılığı sağlanmalıdır.

Diğer önemli bir konu ise bir önceki bölümde incelenen SLBİ'dir. SLBİ sayesinde tasarımın başında stratejik karar verecek liderin bilgi ihtiyacı tespit edilmesi önemli derecede kolaylık sağlayacaktır. Bu maksatla tasarımın başında, hangi konularda liderin bilgilendirilmesi gerektiği tanımlanabilir. Bir liste hazırlanabilir. Paydaşlardan SLBİ konusunda görüş alınarak ilaveler yapılabilir ve sonunda stratejik seviye liderin onayı alınabilir. Bu sayede liderin gereksiz bilgi ile yanlış yönlenmesi, zaman kaybetmesi engellenebilir.

Dijital çağın teknolojilerinin gündeme getirdiği diğer önemli bir konu ise siber güvenlik ve bilgi harekâtıdır. Bu konu mutlaka stratejinin bir parçası olmalıdır. Bu konu stratejik iletişim başlığı altında toplanabilir. Dijital çağda siber güvenlik ve bilgi harekâtı dikkate alınmadan tasarlanacak bir güvenlik stratejisi, daha başlangıçta başarısız olmaya mahkûm olacaktır. Belirli periyodlarla bu konulardaki tasarım, ana strateji tasarımı ile koordineli olarak mutlaka gözden geçirilmeli, somut ölçülebilir performans kriterleri dikkate alınarak değerlendirmeler yapılarak tedbirler alınmalıdır. Bu konu ile ilgili ayrı bir inceleme veya çalışma başlatılabilir.

Şekil 3.4: Dijital Çağ Güvenlik Stratejisi Modeli Önerisi



Kaynak: Yazar tarafından oluşturulmuştur.

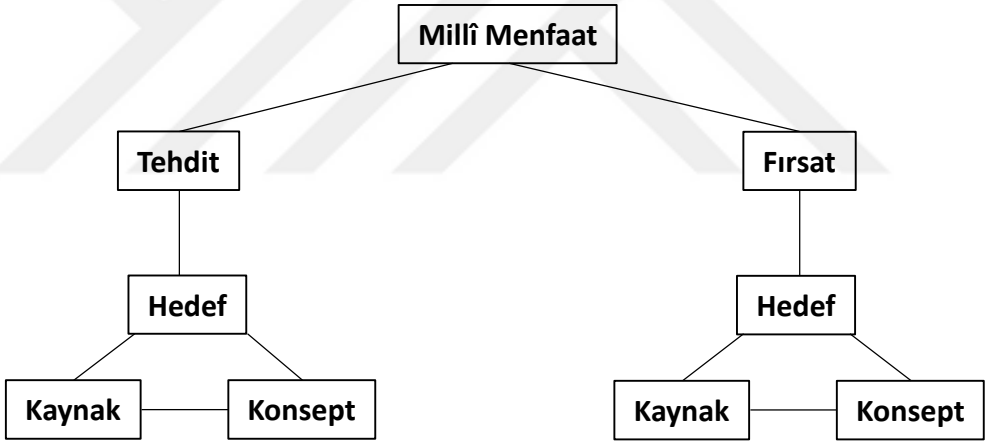
3.3. GÜVENLİK STRATEJİSİNİN PERİYODİK DEĞERLENDİRİLMESİ

Güvenlik stratejilerinin değerlendirilmesi diğer meslek guruplarında kullanılan stratejilerin değerlendirmesinden bazı farklılıklar arz edebilir. Bu nedenle bazı hususların göz önünde bulundurulması gerekmektedir. Bu çerçevede güvenlik stratejisinin esas aldığı millî menfaate veya menfaatlere tehdit oluşturan veya fırsatın gerçekleştirilmesini sağlayan hedefin değerlendirilmesi önem kazanmaktadır. Bu nedenle eğer tehdit varsa, hedefin etkisiz hale getirilmesiyle tehdidin bertaraf edildiği

ve neticede millî menfaatin korunduğunun tespit edilmesi veya fırsatı sağlayacak hedef ele geçirildiğinde millî menfaatin daha ileriye götürülebildiğinin tespit edilmesini sağlayabilecek bir değerlendirme modeli kurulması gerekmektedir. Bu maksatla özellikle millî güvenlik stratejisinin değerlendirilmesinde kullanılabilecek bir model katkı olarak bu çalışmada Şekil 3.5'te önerilmektedir.

Birinci bölüm Şekil 1.8'de bir stratejinin risk değerlendirmesine yönelik model gösterilmektedir. Ancak bu model sadece stratejinin değerlendirmesini esas aldığından dolayı, stratejinin nihai hedefi olan millî menfaatin korunduğu veya ilerletildiğine yönelik bir model önermemektedir. Bu nedenle millî menfaat-tehdit-hedef ve hedefe bağlı olarak güç unsuru ve konseptin bir bütün halinde göz önüne alındığı bir model Şekil 3.5'te önerilmektedir. Bu model üzerinde çalışılan güvenlik stratejisinin özellikleri dikkate alınarak gözden geçirilebilir ve ihtiyaca göre uyarlanabilir.

Şekil 3.5: Güvenlik Stratejisi Değerlendirme Modeli



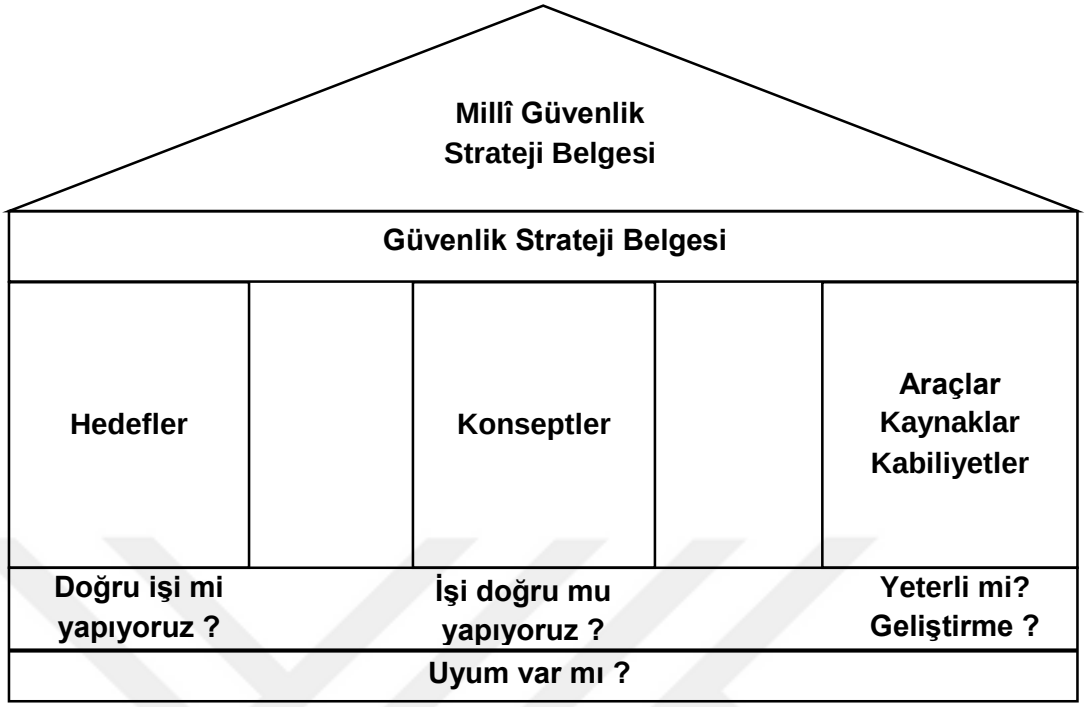
Kaynak: Yazar tarafından oluşturulmuştur.

Şekil 3.5'teki model esas alınarak aşağıdan yukarı bir değerlendirme planı hazırlanması uygun olabilecektir. Bu sistemde Şekil 3.6'da gösterildiği gibi öncelikle doğru bir hedef seçilip seçilmediği kontrol edilmesi maksadıyla "doğru işi mi yapıyoruz" sorusu sorulmalı, müteakiben "bu işi doğru mu yapıyoruz" sorusu sorularak hazırlanan konseptin uygun olup olmadığı kontrol edilebilir. Son olarak eldeki kaynaklar, kabiliyetler, millî güç unsurları yeterli mi değerlendirilir. Eğer yeterli değilse, geliştirilmesi için alınacak tedbirler incelenebilir. Her bir unsur değerlendirildikten sonra üç unsur arasında bir uyum var mı, yani denge bozulmuş mu

kontrol edilir. Geçmişte ABD'nin Afganistan'ın işgalini sorgulaması ve Taliban ile barış görüşmelerine başlaması "doğru işi mi yapıyoruz" sorusunun sonucu olduğu ifade edilebilir. ABD'nin Irak'ın işgalinden sonra 2007 yılında geniş kapsamlı bir terörle mücadele konsepti yürürlüğe koyması "işi doğru mu yapıyoruz" konusuna iyi bir örnek teşkil edebilir. Ancak burada unutulmaması gereken önemli bir konu nihai hedefin doğru seçilmediği, buna karşın konseptin çok iyi uygulandığı ve kaynakların etkin tahsis edildiği durumlar sayesinde başarılı sonuçların alınabileceğini vurgulamakta fayda vardır. Bunun tam tersi hedef doğru seçilip konseptin uygulanmasında ve kaynakların verimli kullanılmasında sorunlarla karşılaşılmış olunabilir.

Hedef-kaynak-konsept üçgeni değerlendirildikten sonra; seçilen hedefin tehdidi etkisiz hale getirip getirmediği veya fırsatın kullanılmasını sağlayıp sağlamadığı değerlendirilmelidir. En son olarak da millî menfaatin korunup korunmadığı veya ilerletilip ilerletilmediği değerlendirilebilir. Dolayısıyla stratejinin kavramsal olarak daha önceki bölümlerde açıklandığı gibi politika ile taktik seviye icra arasında bir köprü olduğu dikkate alındığında; hem politik hem de icranın dikkate alındığı bir değerlendirme yapılmış olacaktır. Bunun yanında taktik seviyedeki icranın da dikkate alınması ve bütüncül bir yaklaşımla değerlendirmenin yapılması sağlıklı sonuçlar verebilecektir. Bu nedenle değerlendirme planının en önemli kısımlarından birisi sahadan, belirlenen esaslar dâhilinde raporların alınmasıdır. Raporun formatı ve raporda belirtilen hususların nasıl, hangi periyodlarla analiz edileceği dikkatle planlanmalıdır.

Şekil 3.6: Güvenlik Stratejisi Değerlendirme Sistemi



Kaynak: Yazar tarafından oluşturulmuştur.

Maliyet, stratejinin değerlendirilmesinde önemli bir yere sahiptir. Bu maliyet ekonomik, insan zayiatı, ülkenin bir kısmının zarar görmesi, hatta ülkenin işgale uğraması gibi hususları kapsayabilir. Strateji tasarlanırken bir kısım maliyetler öngörülebilir ve hesaplanabilir. Ancak bazılarının hesaplanması oldukça zordur. Stratejiyi tasarlayanların stratejinin hayata geçirilmesi konusunda karar vericilere veya liderlere maliyetler konusunda iyi bilgi vermeleri gerekmektedir. Bu şekilde karar vericilerin stratejinin icrasıyla elde edilecek hedefler ve bu hedeflere ulaşmak için harcanacak maliyetleri mukayese etmesi sağlanabilir. Maliyetler belirlenen hedeflerin değerinden fazla ise stratejinin tasarımının tekrar gözden geçirilmesi gerekecektir. Bunun yapılmaması, göz ardı edilmesi veya ihmal edilmesinin önemli sonuçları olacaktır. Bu nedenle ülkenin millî menfaatlerinin ve haklarının iyi bir şekilde belirlenmesi, bu menfaatlerin veya hakların değerinin tespit edilmesi, bu menfaat veya haklara yönelen tehdidin belirlenmesi, tehdidin ciddiyetinin belirlenmesi önem kazanmaktadır. Tasarımcı, maliyet etkinliği çerçevesinde, oluşturduğu güvenlik stratejisinin makul bir maliyetle tehdide karşı millî menfaatlerin korunmasını sağlaması veya fırsatların değerlendirmesini yapması ve karar vericilere sunması

gerekmektedir. Hatta gerekirse tasarımın başında hedeflerin daha makul belirlenmesini kapsayacak şekilde tasarımda değişiklik de yapabilmelidir. Tasarımcının diğer göz önünde tutacağı önemli bir konu ise uygulanacak strateji sonucunda ülkenin gücünün artması, azalmamasıdır. Bu çerçevede özellikle belirlenecek hedeflerin uzun vadede ülkeye ekonomik sorun olarak geriye dönmesi, ilave kaynak sağlamak yerine kaynaklarının azalmasına neden olması oldukça önemli bir sorun kaynağıdır. Diğer taraftan millî menfaatlerin tehdit altında olduğunun tespit edilmesi, buna karşın harekete geçilmemesi, strateji tasarlanmaması başka bir sorun olarak karşımıza çıkacaktır.

Değerlendirme için kalıp bir modelin önerilmesinden daha ziyade; tasarlanan güvenlik stratejisinin amacı, özellikleri, tehdit, stratejik ortam gibi hususlar değerlendirilerek bir model oluşturulması daha fonksiyonel olabilecektir.

3.4. RİSK YÖNETİM MODELİ

Değerlendirme ile birlikte tasarlanan stratejiye oluşabilecek risklerin hesaplanması önem taşımaktadır. Risklerin hesaplanması için de sihirli bir yöntem bulunmamaktadır. Tasarım ve icra sırasında yapılan analizler, elde edilen istihbarat kullanılarak belirlenebilecek risk alanları sadece bir olasılık olarak kalacaktır. Dolayısı ile tasarımcı riskin hem ortaya çıkma olasılığını hem de stratejiyi etkileme miktarını değerlendirebilmek için bir yöntem ortaya koymaya çalışmalıdır.

Daha önceki bölümlerde incelendiği gibi güvenlik stratejisi çerçevesinde risklerin iki yönlü olduğunun bir kez daha vurgulanmasında fayda vardır[94]. Bunlar stratejinin uygulanmasına riskler ve stratejinin uygulanmasından kaynaklanan risklerdir. Stratejinin uygulanmasına risk tasarımın başarısız olmasına neden olan risklerdir. Bu riskler stratejinin tasarım aşamasında nispeten ortaya konulabilir ve risk yönetimi için tedbir alınabilir. Stratejinin uygulanmasından kaynaklanan riskler ise ilave tehditler olarak ortaya çıkabilecektir.

Şekil 3.5 esas alınarak güvenlik stratejisinin değerlendirmesinde kullanılabilecek bir model önerilmiştir. Bu model ile koordineli olarak kullanılabilecek güvenlik stratejilerinin risk yönetimi için dört aşamalı bir yaklaşım

[94]Heffington, Steven; Oler, Adam; Tretler, David, *A National Security StrategyPrimer*, 2019, s.44.

Şekil 3.7’de gösterilmektedir. Bu sistem bu çalışmada bir öneri olarak sunulmaktadır. Bunlar:

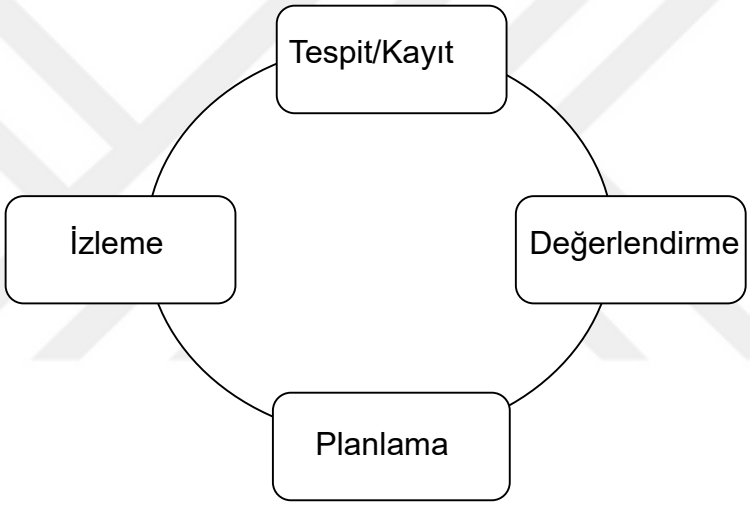
Risklerin Tespiti/Kayıt Altına Alınması (zamanlama dâhil)

Değerlendirme/Önceliklendirme

Planlama

İzleme

Şekil 3.7: Risk Yönetim Sistemi



Kaynak: Yazar tarafından oluşturulmuştur.

Risk Tespiti/Kayıt :

Güvenlik stratejisinde muhtemel risk alanları üç bölümde incelenebilir. Katkı olarak sunulan risk alanları gruplandırması aşağıda açıklanmaktadır.



Birinci Grup: Bu grup tasarımın başında millî menfaatlerin, tehdidin ve bu tehdidin bertaraf edilebilmesi için etki altına alınması gereken hedeften oluşmaktadır. Genel olarak millî menfaatlerin belirlenmesi tarihi süreç ve değişik kuruluşların da katkısıyla oluşturulduğunda önemli bir risk barındırmayabilir. Ancak yine de millî menfaatlerin yanlış tespit edilmesinden dolayı risk oluşabileceği, bu riskin diğer adımları da etkileyebileceği göz önüne alınmalıdır. Bu grupta risk barındırabilecek en önemli konulardan birisi tehdidin belirlenmesidir. Tehdidin ortaya çıkma olasılığı ve stratejiyi etkileme miktarı dikkate alınması gereken önemli bir faktördür. Örneğin bir aktör tehdit olarak tespit edilebilir. Ancak bu aktörün yeterli imkân kabiliyeti, gücü yoksa olasılık azalabileceği gibi aynı zamanda etkileme miktarı da az olabilecektir. Bunun yanında bu tehdittin bertaraf edilebilmesi için tespit edilen hedefin seçimi de belirli riskler barındırabilir. Örneğin tespit edilen hedef tehdidin bertaraf edilmesini sağlamayabilir veya millî kaynakların tükenmesine neden olabilir.

İkinci Grup: Bu grup tespit edilen hedefin bertaraf edilebilmesi için kullanılabilecek millî güç unsurları, kaynaklar, araçlar ve ortaya çıkan maliyetle ilgilidir. Millî güç unsurlarının belirlenen hedefi bertaraf edip edemeyeceği yönünde gerekli analizler yapılması sonucunda bu konuda belirli bir hissiyat oluşacaktır. Ancak millî güç unsurlarının diğer alanlardaki stratejilerde de kullanılmaları etkinliklerini azaltarak risk oluşturabilme potansiyeli olabilecektir. Benzer konunun kullanılacak araçlar için de dikkate alınması uygun olabilecektir. Stratejinin gerçekleşmesi için kullanılması öngörülen her türlü kaynağın öncelikle envanteri oluşturulmalı, yapılan harcamalar ve kayıplar nedeniyle gelinen durum sürekli takip edilmelidir. Strateji tasarımının ve icranın uzun süre devam edeceği düşünüldüğünde kaynakların sürekli takip edilmesi ve yeterliğinin sorgulanması oluşabilecek riski azaltabilecektir. Kaynakların belirli hedeflerin bertaraf edilmesi için harcanan kısmı ise maliyeti oluşturacaktır. Yukarıda belirtildiği gibi maliyetin elde edilen millî menfaate değip değmeyeceğinin analiz edilmesi hayati önemi haizdir. Güçlü aktörlerin ellerindeki bol miktardaki kaynak, güvenlik stratejilerinin başarıya ulaşması, başarıya ulaşamaz ise yeni bir strateji yürürlüğe sokabilmeleri için bir avantaj olarak görülebilir.

Üçüncü Grup: Bu grup millî güç unsurları, araçlar ve kayaklar ile hedefin buluşmasını sağlayan unsurları kapsamaktadır. Bunlar konseptler, icra mekanizması, izleme sistemi olarak ifade edilebilir. Daha önce açıklandığı şekilde değişik konseptler kullanılabilir. Seçilen her konseptin veya yöntemin diğerine göre avantajlı durumu olabilecektir. Yapılan seçim neticesinde belirli bir konseptin kullanılması ile diğer konseptlerin avantajlarından faydalanılamayacak, belirli riskler oluşabilecektir. Konseptin icra edilmesi için kullanılacak mekanizmanın iyi tasarlanması bu konudaki riskin asgariye indirilmesini sağlayabilecektir. İcra mekanizmasının tasarlanması konusunda yapılan seçim de belirli bir risk alanı oluşturabilir. İcra mekanizmasının sağlıklı oluşturulamaması, tasarım çok iyi olsa bile icranın etkinliğini, dolayısıyla stratejinin başarısını etkileyebilecektir. Mekanizmaya ilave olarak, izleme sisteminin iyi kurulamaması durumsal farkındalığı ve buna bağlı olarak risk yönetimini etkileyebilecektir. Risklerin uygun şekilde izlenememesi stratejinin icrasını direkt olarak etkileyen önemli bir unsur olarak karşımıza çıkabilecektir.

Yukarıda açıklandığı şekilde belirlenen risklerin listelenmesi yönetimini kolaylaştıracaktır. Bu çerçevede Tablo 3.1 kullanılabilir. Bu tablo çalışmada katkı

olarak sunulmaktadır. Söz konusu tablonun değişik durumlara uygun olarak gözden geçirilmesi uygun olabilecektir.

Değerlendirme:

Herhangi bir riskin değerlendirilmesi; Tablo 3.1'de gösterildiği gibi ortaya çıkma olasılığı, stratejiyi etkileme miktarı ve zamanlamasını kapsayabilir. Değerlendirme yapılmasını müteakip bu parametreler kullanılarak bir önceliklendirme yapılabilir.

Ortaya çıkma olasılığı, günümüz teknolojik imkân ve kabiliyetleri kullanılarak nispeten daha somut hesaplanabilir. Bu çerçevede belirlenen bir aktörün davranışlarının, söylemlerinin, savunma harcamaları gibi faktörlerin takip edilmesi önemli veriler sağlayabilecektir.

Stratejiyi etkileme miktarı ise yapılacak modellemeler ile nispeten somut verilere dayandırılabilir. Ancak bu verilerin birer karar destek aracı olarak kullanılması, nihai kararın insan tarafından verilmesinin esas alınması uygun olacaktır.

Risk değerlendirmesi konusunda ticari olarak birçok analizci ve şirket tarafından kullanılan Tablo 3.2'den[95] faydalanılabilir. Önemli olan bu tablodaki yaklaşımı stratejik seviyede kullanılan faktörler dikkate alınarak güvenlik stratejisi tasarımı yaklaşımıyla uyumlu olarak kullanabilmektir.

Tablo 3.1: Risk Tespit / Kayıt Tablosu

Sıra No	Risk Tanımı	Ortaya Çıkma Olasılığı	Etkileme Miktarı	Zamanı	Değerlendirme

Kaynak: Yazar tarafından oluşturulmuştur.

[95] Özdemiroğlu, Fatih, *Risk Matrisi Nedir?* 2021.

Ortaya çıkma olasılığı olarak; çok küçük, küçük, orta, yüksek ve çok yüksek olarak beş kategori oluşturulabilir. Etkileme miktarı olarak çok hafif, hafif, orta, yüksek, çok yüksek şeklinde yine beş kategori yapılabilir. Satır ve sütunlardaki rakamların çarpımından çıkan sonuçla değerlendirmenin neticesi belirlenebilir (Tablo 3.2).

Belirli bir riskin ortaya çıkma zamanının önceden hissedilebilmesi, öngörülmesi planlamanın zamana bağlı olarak yapılmasını, hatta alınabilecek tedbirler ile riskin ortaya çıkmasının engellenmesini bile sağlayabilecektir. Değerlendirmeden elde edilen sonuçlar Tablo 3.1'de son sütuna kaydedilir.

Planlama:

Risklerin stratejiyi mümkün olduğu kadar az etkilemesi için dört yöntem önerilebilir. Bunlar; kaçınma, aktarma, azaltma (yönetme), kabul etme olarak sıralanabilir. Tasarım aşamasında tespit edilen bir riskten, tasarımda yapılabilecek değişiklikler ile kaçınma sağlanabilecektir. Aktarma konusunda ise, NATO gibi bir güvenlik ittifakına müdahil olarak riske başka bir organizasyon tarafından tepki gösterilmesi sağlanabilecektir. Bunun yanında alınan ilave tedbirler ile riskin azaltılması da sağlanabilir. Bu çerçevede ihtimalat planlarının hazırlanması iyi bir çözüm oluşturabilir. En son olarak da riski kabul etmek ve gerekli tedbirleri alarak devam etmek göz önüne alınabilir.

İzleme:

Güvenlik stratejilerinde risk yönetiminin en önemli halkalarından birisi izleme konusudur. Bu maksatla iyi bir izleme sistemi kurulması hayati önemi haizdir. Bu izleme sisteminin en önemli halkasını raporlar oluşturmaktadır. Raporların hangi kuruluş tarafından, hangi başlıklar altında hazırlanacağının ortaya konulması gerekmektedir. Bu çerçevede raporların zamanlaması, belirli riskler için emarelerin belirlenmesi, raporlarda bu emarelere yönelik girdilerin olması uygun olacaktır.

İzleme neticesinde alınacak sonuçlar çerçevesinde yalnızca belirli bir riske karşı tedbir alınmasının yanında risk yönetiminin tamamının da belirli aralıklarla gözden geçirilmesi ve güncellenmesi gerekebilecektir. İzlemenin sonucunda tespit edilen yeni riskler kaydedilir.

3.5. GÜVENLİK STRATEJİSİ YÖNETİM MODELİ

Güvenlik stratejilerinin yönetimi ile teknolojinin birleştirilmesi çerçevesinde John Boyd tarafından ortaya atılan, OODA (Observation, Orientation, Decision, Action) çevrimi; gözlem, uyumlandırma, karar, icra elemanlarından oluşan sistem, önemli bir model olarak karşımıza çıkmaktadır.[96] Söz konusu model, kriz yönetimi, organizasyon yönetimi gibi sosyal konularda kullanılmasının yanında; robotların, otonom veya uzaktan komutalı, YZ kullanılan sistemlerin tasarımında da karşımıza çıkmaktadır. Bu çevrimi rakibine göre daha süratli işleten taraf, karşı tarafta, karışıklık ve düzensizlik yaratarak felç olmasını sağlayacak ve başarılı olacaktır. Stratejik seviyede koordinasyon ve karar alma zor olduğu için bu çevrimin başarıyla uygulanması rakip tarafa üstünlük sağlaması noktasında daha da etkin olabilecektir. Ancak çevrimin koordineli olarak uygulanması ve karar alınmasının her iki taraf içinde stratejik seviyede zor olacağının göz önünde tutulması uygun olacaktır. Dolayısı ile teknolojiyi kullanarak iyi organize olan tarafın başarılı olması ve mücadeleyi kazanma şansı daha yüksek olacaktır. Müteakip maddelerde GUKİ döngüsü (Şekil 3.8) incelenmiştir.

3.5.1. GUKİ Döngüsü

Daha önce belirtildiği gibi GUKİ döngüsünü rakipten daha hızlı işletebilen taraf, rakibe göre durumsal üstünlüğü (inisiyatif) ele geçirir ve rakibin karar verme döngüsünün içine girer ve onun karar verme sistemini akamete uğratır. Daha hızlı karar alabilen tarafın kararlarının etkilerini karşı taraf anlamlandırasıya kadar diğer taraf başka bir karara geçecek, karşı tarafın geçmişteki karar üzerinde uğraşmasına neden olabilecektir. Dolayısıyla kararları hızlı bir şekilde veremeyen taraf diğer tarafın kararlarına yalnızca reaksiyon göstermeye çalışacak inisiyatifi ele geçiremeyecektir. Bir süre sonrada stratejik olarak karar alamaz duruma gelebilecek, yani felç olacaktır. Dijital çağın yukarıda belirtilen sürat, değişim, muğlaklık, belirsizlik gibi artan özellikleri dikkate alındığında bu husus çok daha önemli bir konuma gelmektedir.

[96]Finney, Nathan K, *On Strategy: A Primer*, 2020 ,s 71.

Tablo 3.2: Risk Değerlendirme Tablosu

	Etkileme Miktarı				
Olasılık	1 (Çok Hafif)	2 (Hafif)	3 (Orta)	4 (Yüksek)	5 (Çok Yüksek)
1 (Çok Az)	Düşük	Düşük	Düşük	Düşük	Düşük
2 (Az)	Düşük	Düşük	Düşük	Orta	Orta
3(Orta)	Düşük	Düşük	Orta	Orta	Yüksek
4 (Yüksek)	Düşük	Orta	Orta	Yüksek	Yüksek
5 (Yüksek)	Düşük	Orta	Yüksek	Yüksek	Çok Yüksek

Kaynak: (Özdemiroğlu, 2021).

Gözlem:

Ortamı incelemek (tara, gözden geçir) ve bilgi toplamak; ancak bilgiyi mümkün olduğunca çok kaynaktan toplamak anlamına gelmektedir. Etkili gözlem yapmanın önündeki başlıca zorluklar; karar verme ve planlamada kullanılabilecek uygun bilgiye ulaşmada hangi bilginin takip edileceği ve bunlar arasından uygun olanın nasıl seçileceğidir.

Uyumlandırma:

Stratejik durumun resmini oluşturmak için bilginin kullanılması, yani algının ortaya çıkacağı safhadır. Veriyi bilgiye dönüştürmek olarak da tanımlanabilir. Daha çok ve

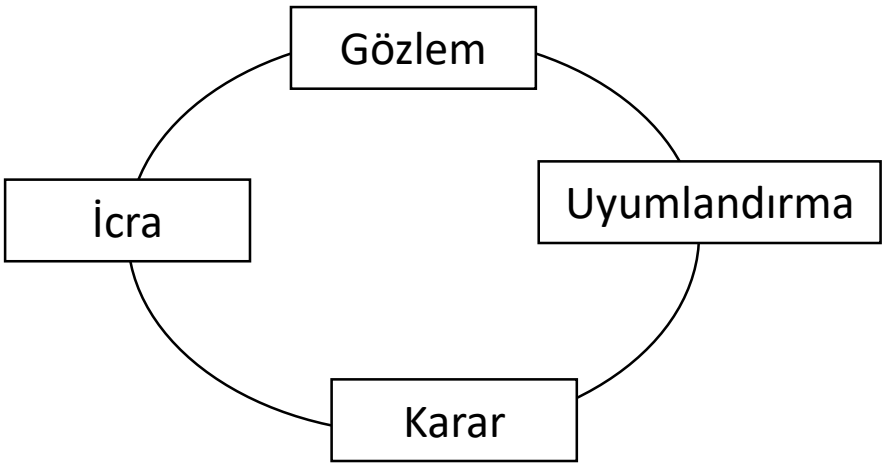
güncel bilgi elde ettikçe, eski resmin yerine yeni resim oluşturulur. Ayrıca uyumlandırma ham verinin bilgiye dönüştürülmesine yardımcı olur. Bilgi, algılama, uygun karar verme ve planlamanın temel taşıdır. Bir insanın çevresinde birçok şeyi izlediği, ancak kendisi için önemli olan konuya odaklandığı iyi bir örnek teşkil etmektedir. Önemli olmadığı düşünülen ve odaklanılmayan konu problem olarak karşımıza çıkabilir. Diğer taraftan önemli olduğunu düşündüğümüz, ancak önemli olmayan bir konu ise kaynak, gayret sarfına neden olabilecektir. Bu nedenle uyum; GUKİ döngüsünün en önemli aşamasıdır.

Kazanmak için, rakipten daha hızlı bir tempoda/ritimde hareket edilmeli ve rakibin döngüsünün içine girilmelidir. Sürekli değişen durumlar yaratmak, rakibi, değerini yitirmiş ham veri ile ilgilenmeye ve bu veriyi güncellemede yanlış yönlere sapmaya zorlar. Dolayısıyla rakibe odaklanmada veya uyumlandırmada hata yaptırır. Dolayısıyla rakip, karara giden yolda ihtiyacı olan zamandan yoksun bırakılır. Bu tarz bir hareket rakibin nazarında karşı tarafı belirsiz (tahmin edilemez) kılar ve bundan dolayı rakibin iç sistemlerinde karışıklık ve düzensizlik oluşur. Rakip taraf, devamlı değişen sorunlar ve belirsizlik nedeniyle resmi tam oluşturamaz; ayrıca, çalışma programlarını ve prosedürlerini, karşılaştıkları problemlere adapte etmede yeterli zaman bulamaz ve aldatmayla durum rakip için daha kötü bir hal alabilir.

Karar Verme:

Seçenekleri düşünmeyi ve hareket tarzlarından birini seçmeyi ifade eder. Amaç rakipten daha hızlı ve daha iyi tercihler yapabilmektir. Geleceği öngörme yeteneği, başarı ve başarısızlık arasındaki farkı oluşturur. Zaman ve belirsizlik karar verme sürecini etkileyen iki önemli parametredir. Kararsız kalmak en kötü sonucu verir. Verilebilecek en kötü karar bile kararsızlıktan daha iyidir. Verilen karar iyi bir değerlendirme sistemiyle incelenmeyi müteakip toplanan bilgilerle yeni kararlar verilebilir. Karar verilememesi ise stratejik felce neden olarak, çok daha tehlikeli sonuçlar ortaya çıkarabilecektir. Bir önceki bölümde incelenmiş olan karar verme sürecinin etkin işletilmesinin önemi bu çerçevede ortaya çıkmaktadır.

Şekil 3.8: GUKİ Döngüsü



İcra Etme:

Verilen kararı uygulamaktır. Bu safhayı müteakiben döngü başa döner ve tekrar başlar. İcra sonucunda performansın sonuçları izlenebilir/gözlemlenebilir, geri beslemeler verilebilir. Dijital çağda olayların çok süratle geliştiği bir durumda GUKİ döngüsü esas alınarak çağa uygun bir strateji yönetim sistemi modellenebilir.

Dijital çağada güvenlik stratejisi tasarımı kadar, yönetimi de oldukça önemlidir. Yönetim modelinin tasarım ile uyumlu ve dijital çağa uygun bir yapıda olması stratejinin başarıyla uygulanması için önemli bir faktördür. Bu çerçevede tez çalışmalarında elde edilen bilgiler ve deneyimler ile GUKİ döngüsü dikkate alınarak Şekil 3.9'da bir model önerilmiştir. Önerilen modelde; tasarım, icra/izleme (uyumlandırma) ve değerlendirme olmak üzere üç ana safha bulunmaktadır. Tasarım safhası daha önce yeteri kadar incelendiği için üzerinde durulmayacaktır.

Strateji tasarımının tamamlanmasını müteakip, tasarımı teslim alıp uygulamaya koyabilecek bir icra grubu oluşturulması uygun olur. İcra grubunun görevi üzerinde çalışılan belirli bir stratejinin yönetimini sağlamaktır. Güvenlik stratejisinin ilgili kurumlara yayımlanmasıyla icra başlayabilir. Güvenlik stratejisine ilave olarak stratejik bir planın hazırlanması ve devreye sokulması icrayı kolaylaştıracaktır. Birinci bölümde strateji ile planlamanın aynı şeyi ifade etmediği incelenmiştir. Bu grubun yönetim faaliyetini kolaylaştırabilecek en önemli husus çalışma programının hazırlanması ve diğer kurumlarla irtibatlı olarak takip edilmesidir. İcra grubunda her

bir yol haritası için bir genel koordinatör olması uygun olacaktır. İcranın en önemli konularından birisi stratejik durumu ifade eden bir stratejik resim oluşturulmasıdır. Bu çerçevede uyumlandırma veya değerlendirme devreye girmektedir. Gelen bilgilerden hangisinin stratejik değeri olduğuna karar verilmesi gerekmektedir. Dijital çağda kullanılabilecek bir model bir önceki bölümde Şekil 2.4'te gösterilmiştir. İcra grubu, hem stratejik resmi oluşturmaktan hem de kısa vadeli, basit planların hazırlanması ve hatta verilen yetkiler çerçevesinde bazı kararların verilmesinden sorumlu olabilir. Ancak stratejik seviyede, icracının esas taktik seviye olduğu unutulmamalıdır. Bu nedenle bu çalışmaların ağırlıklı olarak taktik seviyede yapılması, stratejik seviye tarafından takip edilmesi ve stratejik hedefe ulaşacak şekilde yönlendirilebilmesi çok daha faydalı olabilecektir.

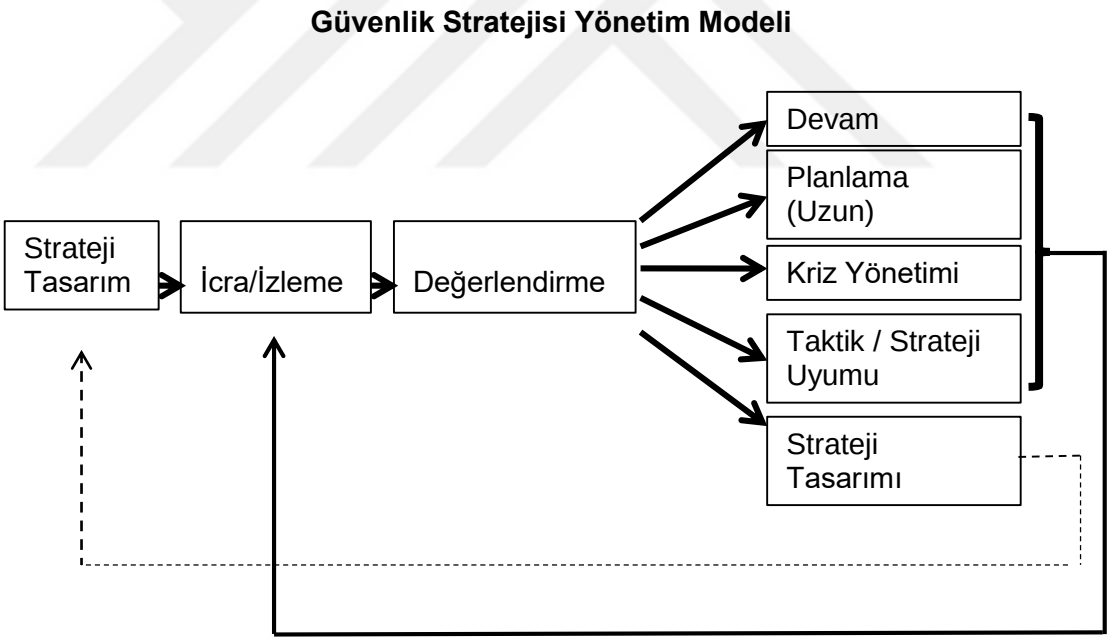
Değerlendirme (uyumlandırma) safhası icranın en önemli safhası denilebilir. İzleme veya stratejik resimden gelen bilgiler ışığında bir değerlendirme yapılır. Değerlendirme konusunda ayrıntılı inceleme yukarıda yapılmıştır. Değerlendirme sonucunda Şekil 3.9'da gösterilen beş durumdan birisine karar verilebilir. Bir şey yapılmasına gerek olmadığına, aynı şekilde devam edilmesine de karar verilebilir. Buna karşın gelecekte çıkabilecek bir probleme veya duruma yönelik olarak uzun vadeli bir planlama yapılarak, stratejinin icrası esnasında, daha problemle karşılaşılmadan zaman varken ve hatta problem daha başlangıç seviyesindeyken planlama yapılarak tedbir alınabilir. Daha önce incelendiği gibi bir kriz durumu hissedilebilir. Bu çerçevede kriz yönetim sürecine karar verilebilir. Diğer önemli bir karar ise taktik seviyede icra edilen faaliyetlerin stratejik seviye ile uyumlu olduğunun izlenip değerlendirilip karar verilmesidir. Bu dört faaliyetin sonucunda verilen kararlar neticesinde icraya ve verilen kararların izlenmesine geri dönülür. Bu dört kararın dışında strateji tasarımı ile ilgili bir husus tespit edilirse, tasarıma geri dönülebilir. Bu çerçevede stratejik durum veya çerçeve değişmiş olabilir. Tehdit değişmiş olabilir. Dolayısı ile stratejinin güncel kalmasının sağlanması maksadıyla tasarım gözden geçirilir. Bu pek arzu edilen bir durum olmamalıdır. Çünkü tasarımda yapılacak değişiklik bütün kademeleri etkileyebilecektir. Küçük düzeltmeler ile tasarımın mümkün olduğu kadar aynı kalması daha faydalı olabilir. Bu çalışmada Şekil 3.9'da gösterilen model bir katkı olarak sunulmaktadır.

Stratejik icranın başlamasıyla beraber beklenmedik olaylar, stratejik şokların meydana gelme olasılığı oldukça yüksektir. Bu nedenle bir kriz yönetim grubu oluşturulmalıdır. Kriz yönetim grubunun temel görevi meydana gelen krizin önce

değerlendirilmesi, müteakiben de stratejik tasarıma uygun hal tarzlarının liderlere sunulmasıdır. Bunun yanında ayrı bir stratejik planlama grubunun da kurulması uygun olacaktır. Yapılan değerlendirmeler ışığında stratejik düşünme tekniğine uygun olarak belirli bir süre önceden alınması gereken tedbirlerin, yapılması gereken planlamaların yapılması sağlanabilir. Bu şekilde proaktif veya hiç değilse preaktif planlama devam ettirilebilir.

Bu mekanizmalar kullanılarak GUKİ döngüsü çerçevesinde bir icra döngüsü oluşturulabilir. Bu icra döngüsünün ve yukarıda belirtilen planlama gruplarına ilave olarak stratejik izleme merkezi kurulması ve işletilmesi hayati önemi haizdir. Bu stratejik izleme merkezi güncel gelişmeleri takip ederek gerekli işlemlerin yapılmasını sağlayabilecektir.

Şekil 3.9: Güvenlik Stratejisi Yönetim Modeli



Kaynak: Yazar tarafından oluşturulmuştur.

3.6. GÜVENLİK STRATEJİSİ YÖNETİMİNDE TEKNOLOJİ KULLANIMI

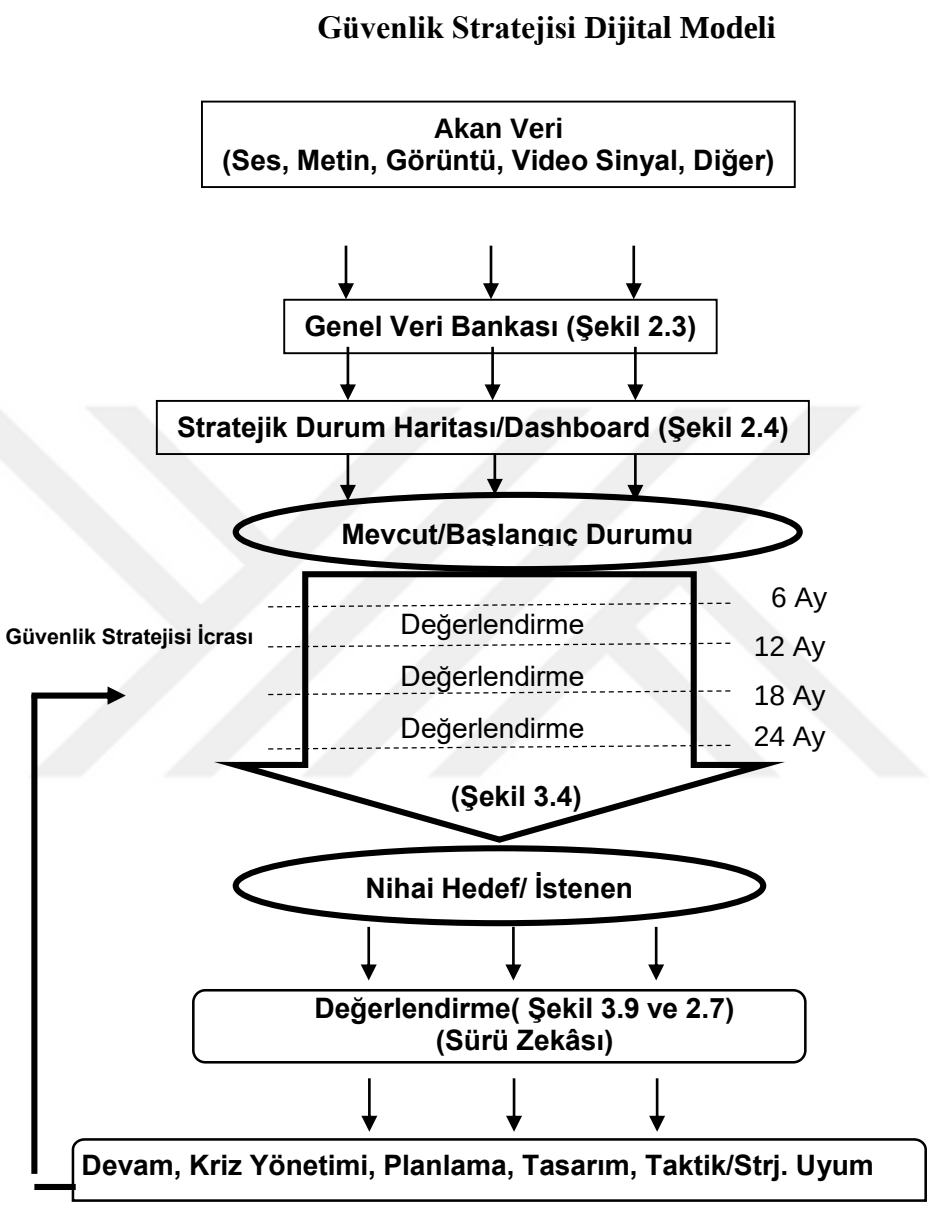
Güvenlik stratejisi yönetiminde teknoloji kullanımı konusunda yapılan araştırmalarda literatürde fazla çalışma tespit edilememiştir. Bu nedenle Şekil 3.10'da önerilen sistem literatüre tezin konusunda belirtildiği gibi yeni önerilen bir modeldir. Model daha önceki bölümlerde üzerinde çalışılan ve incelenen alt modellerin birleştirilmesinden oluşmaktadır. Alt modellerin tez çalışmasında nasıl oluşturulduğu daha önceki bölümde gösterilmiştir.

Akan veri çerçevesinde gelen BV'nin uygun şekilde genel veri bankasına depolanması gerekmektedir. Genel veri bankası belirli aralıklar ile sürekli güncellenmeli, akan veri uygun şekilde, ihtiyaç duyulduğunda kolaylıkla ulaşılabilecek şekilde depolanmalıdır. Bu maksatla değişik depolama teknikleri kullanıldığı bilinmektedir.

Genel veri bankasındaki veri kullanılarak stratejinin icrasının takip edilebileceği bir stratejik durum haritası veya dashboard oluşturulmalıdır. Hem durum haritası hem de dashboard beraber oluşturulması da düşünülebilir. Dashboardlar iş hayatında yaygın olarak kullanılmaktadır. Bu maksatla elde edilen verilerden oluşturulan grafiklerin toplu olarak gösterildiği panolara dashboard denilebilir. Bu sayede stratejik verilerin toplu olarak, karar vericiye yardımcı olacak şekilde coğrafi ve istatiksel olarak görülmesi sağlanmış olacaktır. Bu verilerden önem arz edenler erken uyarı sistemi ile karar vericilerin dikkatini çekecek şekilde harita üzerinde veya dashboard üzerinde gösterilmesi çok faydalı olabilecektir. Strateji yönetiminin başlangıcında oluşan durumun belirli aralıklarla kaydedilmesi, değerlendirme safhasında çok önemli bir girdi olabilecektir. Değerlendirme yapılırken geçmişte istenen herhangi bir zamanla mevcut durum mukayese edilerek geleceğe yönelik bir projeksiyon yapılması görsel olarak mümkün olabilecektir. Aslında bu görseli oluşturan veri çok kıymetlidir. Bu veri kullanılarak değerlendirmenin çok daha sağlıklı yapılması için uygun zemin oluşabilecektir.

Değerlendirme, modelin en önemli bölümü olup dijital çağda teknolojinin de en fazla kullanılabileceği bölüm olarak görülebilir. Ancak bunun için bazı hazırlıkların tasarım aşamasında yapılması uygun olacaktır. Örneğin Şekil 3.10'da nokta nokta olarak gösterilen değerlendirme dönemlerine ulaşıldığında dashboard ve/veya stratejik durum haritasının yansıtması gereken şekil/görüntü, başlangıçta tahayyül edilmeye çalışılabilir.

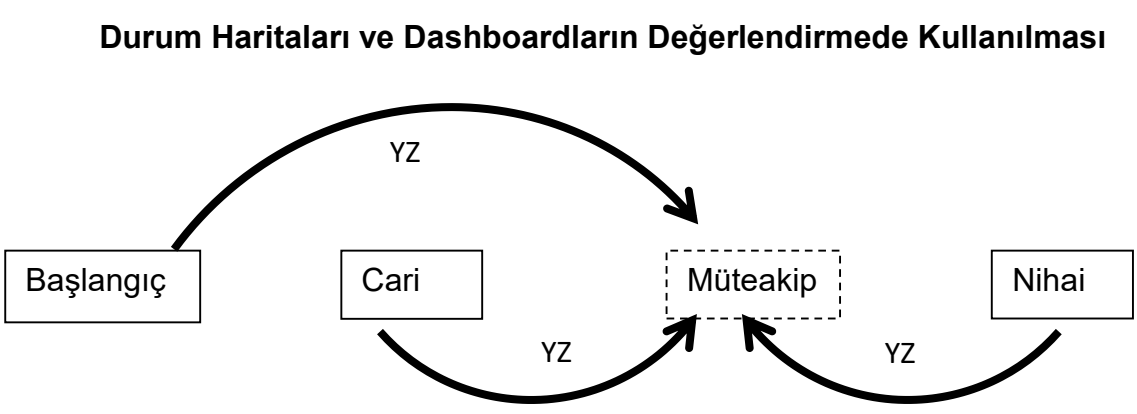
Şekil 3.10: Güvenlik Stratejisi Dijital Modeli



Kaynak: Yazar tarafından oluşturulmuştur.

Daha önce belirtildiği gibi durum haritasının/dashboardun oluşturulması maksadıyla kullanılan BV kıymetlidir. Bu veriyi YZ ile birlikte kullanarak stratejik açıdan önemli sonuçlar elde edilebilir. Bu çerçevede çalışmaya hedeften geriye doğru, yani nihai hedeften altı ay önceki durum değerlendirilerek başlanabilir ve mevcut duruma kadar bir tahminde bulunulabilir. Tahayyül edilen durumların tam anlamıyla gerçekleşmesi neredeyse imkânsızdır. Burada üzerinde durulması gereken konu, veriler arasındaki fark ve nerede problem olduğu, başarısızlık veya başarı olduğu, fırsat olduğunun tespit edilebilmesidir. Başlangıçta teknolojik olarak oluşturulmuş olan mevcut durumun stratejik haritası veya dashboard, tahayyül edilen nihai durumun, değerlendirme dönemindeki cari durum ile karşılaştırılarak arada tespit edilen farklardan önemli sonuçlar elde edilebilir. Bu dijital çağda değerlendirmenin teknoloji kullanılarak süratle ve daha etkin olarak yapılabilmesi için önerilen bir yöntemdir. Bu değerlendirme cari durumun oluşmasına kadar elde edilen BV ve YZ kullanılarak müteakip dönemde oluşabilecek stratejik durum haritası elektronik olarak tahayyül edilmeye çalışılabilir. Bu çerçevede Şekil 3.11'de gösterilen model bir katkı olarak sunulmaktadır. Hatta değişik hal tarzlarının, konseptlerin denenmesi bile bu yöntem ile mümkün olabilir.

Şekil 3.11: Durum Haritaları ve Dashboardların Değerlendirmede Kullanılması



Kaynak: Yazar tarafından oluşturulmuştur.

Değerlendirme konusu daha önce incelenmiştir. Orada belirtilen hususlara ilave olarak, icra esnasında sağlıklı bir değerlendirme yapılabilmesi maksadıyla uygun verilerin elde edilebilmesi için bir plan yapılması uygun olacaktır. Değerlendirme planındaki en önemli konu sayısal olarak verilerin alınabilmesidir. Metin olarak gelen raporların da sayısal hale dönüştürülmesi düşünülebilir. Bu çerçevede çok basit bir değerlendirme planı modeli örneği Tablo 3.3'te gösterilmektedir. Bu değerlendirme planı çalışmada bir katkı olarak sunulmaktadır.

Değerlendirme sonucunda elde edilen veriler Şekil 3.7 ve Şekil 2.7'de gösterilen şekilde değerlendirmeye tabi tutulabilir. Her safhaya insanın dâhil edilmesinin önemli olduğu düşülmektedir. Güvenlik stratejisi dijital modelinin gerekli uyarlamalar ile iş hayatında da kullanılabileceği değerlendirilmektedir. Dijital çağın sunduğu teknolojiler geliştikçe dijital modelin etkinliği daha da artabilecektir. Sonunda algoritması kuvvetli olan tarafın stratejik mücadeleyi kazanacağı fikri ön plana çıkmaktadır.

Daha önce kısmen belirtildiği gibi stratejik yönetim için bazı gurupların oluşturulması uygun olacaktır. Bunlar: İcra, Değerlendirme, Tasarım, Kriz, Planlama, Siber/Bilgi Harekâtı, Veri Yönetimi olarak ifade edilebilir. Veri ve bilgi yönetimi dijital çağda en az stratejinin tasarlanması kadar önemlidir. Bu konularla ilgili çalışmalardan istifade edilerek bu guruplar oluşturulabilir. Bilgisayarın organizasyonlarda kullanılmasıyla bilişim bölümlerinin kurulması buna iyi bir örnek teşkil edebilir. Benzer yaklaşım sergilenebilir.

Tablo 3.3: Değerlendirme Planı Örneği

Konu	**Gösterge**	**Rapor Sorumlusu**	**Raporlama Metodu**	**Rapor Aralığı**
Tehdit	T=NxİI	Savunma Bakanlığı	Metin Veri	Her Ay
Maliyet	Harcanan Para Zayiat	Maliye Bakanlığı	Veri	Her Ay
Güç Unsurları	Ekonomik Ordunun gücü Diplomatik temsilcilik Nüfus …	Bütün Bakanlıklar	Metin Veri	Her Ay
Siber tehdit	Siber saldırı miktarı, cinsi	Siber savunma	Metin Veri	Her Hafta

Kaynak: Yazar tarafından oluşturulmuştur.

Değerlendirme maksadıyla kullanılabilecek diğer bir yöntem ise; güvenlik stratejisi kullanılarak ulaşılmak istenen duruma yönelik değişik güç unsurları tarafından uygulanan yol haritalarının, hedeflerin veya etkilerin sonuçları değerlendirilerek istenilen nihai hedefe ulaşılmasını sağlayıp sağlamadığının tespit edilebilmesidir. Bu maksatla emarelerin rakamsal veya somut değerler olarak ortaya konulması uygun olacaktır. Bu değerlendirme "doğru işi mi yapıyoruz" sorusunun cevabını da verebilecektir. Bununla irtibatlı olarak hedefe ulaşılması için tahsis edilen

güç unsurunun veya taktik seviyedeki unsurların performansı da önem kazanacaktır. Bu performans değerleri işin doğru yapıldığının tespit edilebilmesi maksadıyla önemlidir. Şekil 3.6'da ortaya konulan sistemin uygulanması bu yöntemle yapılabilecektir.

Bu değerlendirme yöntemi konusunda bir örnek verilmesi konunun daha iyi açıklanmasını sağlayabilecektir. A ve B ülkelerinin savaştıkları ve savaş sonucunda barış antlaşması imzalamaları konusu iyi bir örnek teşkil edebilir. A ülkesinin millî menfaati ve tehdit olarak değerlendirilen B ülkesinin tehdit olmaktan çıkarılması maksadıyla barışın sağlanması nihai hedef olarak tespit edilmiş olabilir. Barış ortamının sağlanabilmesi maksadıyla üzerinde durulan konulardan birisi anlaşma imzalanması ve sınırların çizilmesi, diğeri uygun arazinin ele geçirilmesi olabilir. Ancak bu iki alt hedef yapılan değerlendirme sonucunda yeterli olmayabilir. Bunun yanında ittifakların kurulması, savunma planlamasının gözden geçirilmesi ve doğru silah sistemlerinin temin edilmesi gibi caydırıcılık sağlayan ilave hedefler konulması gerekebilir. Bu çerçevede diplomasinin anlaşma müzakerelerindeki performansı, silahlı kuvvetlerin doğru araziyi ele geçirmedeki performansının da değerlendirilmesi gerekmektedir. Diplomatlar anlaşmayı imzalarlar, ancak barışın sağlanması için uygun bir anlaşma olmayabilir. Silahlı kuvvetlerin uygun arazi olarak değerlendirdiği bölge barışı sağlayabilecek bir coğrafya olmayabilir. Dolayısı ile hem doğru işin yapılmasında hem de işin doğru yapılması konusunda sorun tespit edilebilir.

3.7. SONUÇ

Yapılan incelemeler ve değerlendirmeler sonucunda dijital çağa uygun bir güvenlik stratejisi tasarım ve yönetim modeli ortaya koyabilmek için yalnızca tasarım konusunda bir model ortaya konulmasının yeterli olmayacağı değerlendirilmektedir. Bu çerçevede beş konu üzerinde çalışılması uygun olabilecektir. Bunlar aşağıda belirtilmiştir.

Modelleme, prototip üretimi, deneme,

Periyodik değerlendirme sistemi,

Yeni güvenlik stratejisi modeli,

Strateji yönetim sistemi,

Dijital çağ teknolojilerinin kullanımı olarak ifade edilebilir. Bu konular özet olarak aşağıda belirtilmektedir.

Birinci bölümde, Şekil 1.3'te ortaya konulan model; durum tespiti, nihai hedef, güç unsurları-kaynaklar-araçlar, konsept, riskler olmak üzere beş ana safhayı içermektedir. Bu süreci dijital çağa uyumlu hale getirebilmek maksadıyla dört yeni safha eklenebilir. Bunlar; stratejinin modelinin oluşturulması, strateji prototipinin yaratılması, deneme, değerlendirme safhaları olabilir. Bu safhaların eklenmesiyle birlikte mühendislerin bir araba, silah gibi bir malzemeyi tasarlamalarına benzer bir yaklaşımla güvenlik stratejisi tasarımının yapılabileceği değerlendirilmektedir. Bu maksatla yeni bir tasarım süreci modeli önerilmiştir.

Birinci bölüm Şekil 1.8'de bir stratejinin risk değerlendirmesine yönelik model gösterilmektedir. Ancak model sadece stratejinin değerlendirmesini esas aldığından dolayı, stratejinin nihai hedefi olan millî menfaatin korunduğu veya ilerletildiğine yönelik bir model önermemektedir. Bu nedenle millî menfaat-tehdit-hedef ve hedefe bağlı olarak güç unsuru ve konseptin bir bütün halinde göz önüne alındığı yeni bir model önerilmiştir. Bu model, üzerinde çalışılan güvenlik stratejisinin özellikleri dikkate alınarak gözden geçirilebilir ve ihtiyaca göre uyarlanabilir. Bu model esas alınarak bir değerlendirme planı hazırlanması uygun olabilecektir

Dijital çağın şartlarına cevap verebilecek yeni bir güvenlik stratejisi modeli önerilmiştir. Bu modelde; güç unsurlarının hedef temelinde gruplandırılması ve koordinatör tespit edilmesi, muhtemel karar ve kriz noktalarının belirlenmesi, kritik hattın belirlenmesi, değerlendirme periyotları ile siber ve bilgi harekâtı konularına ağırlıklı olarak yer verilmiştir.

Güvenlik stratejilerinin yönetimi ile teknolojinin birleştirilmesi çerçevesinde John Boyd tarafından ortaya atılan, OODA (Observation, Orientation, Decision, Action) çevrimi; gözlem, uyumlandırma, karar, icra elemanlarından oluşan sistem, önemli bir model olarak karşımıza çıkmaktadır.[97] Söz konusu model, kriz yönetimi, organizasyon yönetimi gibi sosyal konularda kullanılmasının yanında; robotların, otonom veya uzaktan komutalı, YZ kullanılan sistemlerin tasarımında da karşımıza çıkmaktadır.

[97]Finney, Nathan K, *On Strategy: A Primer*, 2020, s.71.

Dijital çağada güvenlik stratejisi tasarımı kadar yönetimi de oldukça önemlidir. Yönetim modelinin tasarım ile uyumlu ve dijital çağa uygun bir yapıda olması stratejinin başarıyla uygulanması için önemli bir faktördür. Bu çerçevede tez çalışmalarında elde edilen bilgiler ve deneyimler ile GUKİ döngüsü dikkate alınarak bir model önerilmiştir. Önerilen modelde; tasarım, icra/izleme (uyumlandırma) ve değerlendirme olmak üzere üç ana safha bulunmaktadır.

Güvenlik stratejisi yönetiminde teknoloji kullanımı konusunda yapılan araştırmalarda literatürde fazla çalışma tespit edilememiştir. Bu nedenle önerilen sistem yeni bir modeldir. Model daha önceki bölümlerde üzerinde çalışılan ve incelenen alt modellerin birleştirilmesinden oluşmaktadır.

Söz konusu modelde akan veri olarak gelen BV'nin uygun şekilde genel veri bankasına depolanması ve güncellenmesi gerekmektedir. Genel veri bankasındaki veri kullanılarak stratejinin icrasının takip edilebileceği bir stratejik durum haritası veya dashboard oluşturulmalıdır. Strateji yönetiminin başlangıcında oluşan durumun belirli aralıklarla kaydedilmesi, değerlendirme safhasında çok önemli bir girdi olabilecektir. Değerlendirme yapılırken geçmişte istenen herhangi bir zamanla mevcut durum mukayese edilerek geleceğe yönelik bir projeksiyon yapılması görsel olarak mümkün olabilecektir. Aslında bu görseli oluşturan veri çok kıymetlidir. Bu veri kullanılarak değerlendirmenin çok daha sağlıklı yapılması için uygun zemin oluşabilecektir. Değerlendirme, modelin en önemli bölümü olup dijital çağda teknolojinin de en fazla kullanılabileceği bölüm olarak görülebilir. Ancak bunun için bazı hazırlıkların tasarım aşamasında yapılması uygun olacaktır. Örneğin değerlendirme dönemlerine ulaşıldığında dashboard ve/veya stratejik durum haritasının yansıtması gereken şekil/görüntü, başlangıçta tahayyül edilmeye çalışılabilir.

Başlangıçta teknolojik olarak oluşturulmuş olan mevcut durumun stratejik haritası veya dashboard, tahayyül edilen nihai durumun, değerlendirme dönemindeki cari durum ile karşılaştırılarak arada tespit edilen farklardan önemli sonuçlar elde edilebilir. Bu dijital çağda değerlendirmenin teknoloji kullanılarak süratle ve daha etkin olarak yapılabilmesi için önerilen bir yöntemdir. Bu değerlendirme özet olarak cari durumun oluşmasına kadar elde edilen BV ve YZ kullanılarak müteakip dönemde oluşabilecek stratejik durum haritası elektronik olarak tahayyül edilmeye çalışılabilir.

Bu konu başlıklarının tamamı konusunda incelemeler ve model önerileri yapılmıştır. Bu bölümde yeni bir güvenlik stratejisi modeli, buna bağlı olarak strateji

yönetim sistemi ile yönetim maksadıyla faydalanılabilecek teknolojiler incelenmeye çalışılmıştır. Güvenlik stratejilerinin dijital çağa uyum sağlamasında üzerinde durulması gereken en önemli hususlardan birisinin risk ve değerlendirme konusu olduğu sonucuna varılmıştır.

Değerlendirmenin BV ve YZ kullanılarak uygun bir model esas alınarak yapılmasının önemli olduğu düşünülmektedir. Bu nedenle amaca ulaşmak maksadıyla uygun verinin tespit edilebilmesi, bu verinin doğru şekilde elde edilmesi, işleme tabi tutulması, sonuçların ilgili birimlere zamanında iletilmesi önem kazanmaktadır.

Aynı şekilde risk değerlendirmesi de önemlidir. Bu maksatla, hem güvenlik stratejisinin uygulanmasına hem de uygulama sonucunda oluşacak risklerin tamamının başlangıçtan itibaren değerlendirilmesi, maliyetlerin dikkate alınması stratejinin başarısı için oldukça önemlidir. Dijital çağın sağladığı imkânlar çerçevesinde risk değerlendirmesi için de BV ve YZ kullanılabilecektir. Verinin doğru olarak yönetilmesi, yönlendirilebilmesi için gerekli tedbirlerin alınması önemlidir.

Risk ve değerlendirmenin dijital çağda etkin yapılabilmesi maksadıyla veri hayati önemi haizdir. Bu nedenle verinin doğru olarak işleme tabi tutulabilmesi maksadıyla veri bilimciliği, veri analizciliği gibi dijital çağın bir gereği olarak ortaya çıkmış olan uzmanlık alanlarında gerekli personelin yetiştirilmesi; strateji tasarım ve yönetim teşkilatına dâhil edilmesi gelinen aşamada bir mecburiyet haline gelmiştir. Benzer şekilde siber güvenlik ve bilgi harekâtı personeli için de geçerlidir.

SONUÇ

Soğuk Savaşı müteakip, son otuz yılı aşan bir sürede oluşan güvenlik ortamı gittikçe daha istikrarsız bir karakter sergilemeye devam etmektedir. Bu çerçevede, Rusya-Ukrayna savaşı, Azerbaycan-Ermenistan savaşı ve ABD-Çin gerginliği gibi krizler küresel ve bölgesel risklere yönelik endişeleri arttırmaya devam etmektedir. Bu krizlere ilave olarak; Kovit-19 salgını, iklim değişikliği, enerji krizi, tahıl krizi ve ekonomik krizler küresel güvenlik ortamının çok daha tehlikeli bir duruma evrilmesine neden olmuştur. Gelecekte bu krizlere başka krizlerin ilave edilmesi olasılık dâhilindedir.

Küresel ve bölgesel krizlerin artmaya devam ettiği bir güvenlik ortamında güvenlik stratejisi tasarımı ve yönetimi her zamankinden daha önemli hale gelmiştir. Ancak güvenlik stratejisi kavramı konusunda kabul görmüş bir tanımın bulunmaması ve hem strateji hem de güvenlik kavramının tarih boyunca değişikliğe uğramış olması, kavramın anlaşılmasını ve uygulanabilmesini zorlaştırmaktadır. Türkiye'de güvenlik stratejisi çalışmalarının oldukça yeni olması ve doküman sayısının yeterli olmaması uzmanlar tarafından konunun anlaşılmasını ve gerçekçi olarak uygulanabilmesini zorlaştıran önemli bir neden olduğu değerlendirilmektedir.

Diğer taraftan dijital çağda teknolojik gelişmeler gittikçe süratlenmekte, günlük hayatımızın yanında güvenlik ortamında önemli değişikliklere neden olmaktadır. Dijital çağ teknolojilerinin zaten tehlikeli bir hal alan küresel güvenlik ortamındaki gelişmeleri çok daha hızlandırdığı, bunun da güvenlik ortamını daha da tehlikeli bir şekle soktuğu ifade edilebilir. Bu çerçevede güvenlik ortamında meydana gelen krizlerin tedrici olarak tırmanmasının yerine dijital çağda stratejik şoklar yaşanmaktadır. Stratejik şokların özelliği beklenmeyen bir zamanda, çok süratli olarak ortaya çıkmaları ve etkilerinin geçmişe göre çok daha geniş alanda ve daha büyük olmasıdır. Bilişim teknolojilerinde meydana gelen çığır açıcı teknolojiler insanın daha süratli düşünebilmesini, karar alabilmesini sağlamıştır. Böyle bir ortamda, tasarlanan güvenlik stratejileri çok kısa zaman içerisinde cari durum ile uyumunu kaybederek geçersiz hale gelmektedir. Bu çerçevede dijital çağ teknolojileri kullanabilen taraf için önemli bir kuvvet çarpanı olurken, bu teknolojileri geliştirmekte ve kullanmakta geç kalan taraf için beka sorunlarına neden olabilir.

Bu nedenle belirsizliğin arttığı ve teknolojik gelişmelerin değişim ve dönüşümü hızlandırdığı bir konjonktürde güvenlik strateji tasarımı ve yönetimi her zamankinden daha önemli bir hale gelmiştir. Doğal olarak böyle bir ortamda güvenlik stratejisi açısından geçmişin çözümlerinin günümüzün problemlerine çözüm olabileceğine yönelik ciddi endişeler bulunmaktadır. Bu çerçevede güvenlik stratejileri tasarımı ve yönetiminin planlı, bilinçli ve bir sistem dâhilinde yapılmasına olan ihtiyaç daha da artmıştır.

Yukarıda belirtilen hususlar çerçevesinde akla ilk gelen soru; klasik güvenlik stratejisi tasarımı ve yönetimi modeli dijital çağın şartlarına cevap verebilmekte midir?

Bu soruya verilen cevabın olumsuz olması durumunda müteakiben sorulacak soru ise; klasik model dijital çağa uygun hale nasıl getirilebilir?

Bu kapsamda genel olarak nitel araştırma tekniklerinden keşfedici ve betimleyici yöntemler kullanılarak, tümden gelim tekniği ile tezin soruları incelenmiştir. Metin ve süreç analiz yöntemleriyle keşfedici bir bakış açısıyla klasik güvenlik stratejisi modeli kapsamlı bir şekilde ortaya konulmuştur. Dijital çağın ortaya çıkarttığı yeni sorunlar, sınamalar ve bunların güvenlik stratejilerinin tasarımı ve yönetimine muhtemel etkileri keşfedici bir bakış açısıyla, kişisel gözlem, durum analizi, metin analizi ve deneyimlerden faydalanılarak incelenmiştir. Tezin genelinde geçmişte, uzun bir süre zarfında elde edilmiş olan kişisel deneyimlerden ağırlıklı olarak faydalanıldığı özellikle vurgulanmalıdır.

Strateji kavramının kullanımı incelendiğinde çok farklı ve değişik sonuçlar ile karşılaşılmaktadır. Bilindiği gibi strateji devlet yönetimi, politika, felsefe, tarih, işletme, kamu yönetimi, spor, pazarlama, şirket yönetimi gibi birçok alanda kullanılmaktadır. Bu çerçevede strateji kavramının bazen oyun kurma, bazen düşünme sistemi oluşturma, bazen de taktik seviyede bir faaliyeti açıklamak gibi maksatlar ile kullanıldığı görülmektedir. Bazen de strateji kavramının gizemli, etkileyici, prestij kazandırıcı bir şekilde algıyı yönlendirmesinden istifade edildiğine şahit olunmaktadır. Bu nedenle strateji kavramının anlaşılması ve strateji tasarımının gerçekçi bir şekilde yapılması zorlaşmaktadır.

Güvenlik stratejisi tanımı yapılması gerekirse; menfaatlere ulaşılması veya tehditlerin bertaraf edilebilmesi için stratejik tasarımcı tarafından tanımlanması gereken hedefler, millî güç unsurları veya kaynaklar ve bunların kullanım konsepti

olarak ifade edilebilir. Bu cümledeki tasarımcı tarafından tanımlanması gereken ifadesi stratejinin sanatsal özelliğini yansıtan unsurdur.

Güvenlik stratejisi tasarımı diğer alanlarda üretilen stratejiler ile önemli benzerlikler gösterse de kimin güvenliğinin sağlanacağı, bu çerçevede tehdidin ne olduğu, tehdidin bertaraf edilmesi için hangi hedeflere ulaşılmasının gerektiği, kullanılacak kaynak ve araçların neler olabileceği gibi kendine özgün kararları içermektedir. Bu çerçevede güvenlik yaklaşımları dikkate alınarak üç düzeyde analiz yapılabilir. Bunlar uluslararası sistem, ulus-devlet ve bireysel düzeylerdir[98]. Bu analiz düzeyleri dikkate alınarak güvenlik konusunda değişik yaklaşımlar ve modeller üretilmiştir. Ancak güvenlik yaklaşımlarının bilinmesi, anlaşılması yeterli değildir. Güvenlik yaklaşımlarının icraata dökülebilmesi güvenlik stratejisi tasarımı ve yönetimi ile mümkün olabilmektedir.

Güvenlik stratejisi denildiğinde akla ilk gelen Millî Güvenlik Stratejidir. Millî güvenlik stratejisine yön veren doküman Millî Güvenlik Siyaset Belgesidir. Millî Güvenlik Stratejinin yayımlanmasını müteakip Millî Savunma Stratejisi hazırlanabilir. Millî Savunma Stratejisi ile uyumlu Askeri Strateji hazırlanır. Politikadan stratejiye geçiş burada başlar. Askeri Stratejinin esas görevi Millî Savunma Stratejisinde verilen esaslar veya görevler doğrultusunda askeri-politik seviyede yapılması gerekenleri ortaya koymaktır. Bir anlamda politik olarak verilen direktifin askeri dile çevrilmesidir. Yani strateji politik seviyeden operatif veya askeri profesyonel seviyeye bir köprü olarak değerlendirilebilir. Askeri Stratejinin oluşturulmasını müteakip operatif seviye olarak nitelendirebileceğimiz her bir harekât alanına yönelik ağırlıklı olarak askeri hususların yer aldığı bir operatif seviye plan hazırlanır. Bu planda stratejik seviyede belirlenen hedeflerin taktik seviyedeki faaliyetler ile birleştirilmesi yani köprü kurulması gerçekleştirilir. Taktik seviye planlama ise yalnızca bir muharebe veya faaliyete ait bir planlamadır. Güvenlik bürokrasisinin politik seviye ile taktik seviye arasındaki ilişki askeri örnekle açıklanmaya çalışılmıştır. Bu örnek bankacılık, sağlık, eğitim gibi diğer alanlara da uyarlanabilir.

Tarihi süreçteki örneklerin incelenmesi strateji kavramının açıklanmasına yardımcı olmaktadır. Bu maksatla Thucydides, Sun Tzu, Carl von Clausewitz gibi düşünürlerin eserlerinin okunması stratejinin kavramsal boyutunun anlaşılmasına

[98]Nye, S. Joseph ve Welch, David, *Küresel Çatışmayı ve İşbirliğini Anlamak*, 2017, s. 75.

yardımcı olmaktadır. Doğal olarak tarihi süreçte tarım toplumundan sanayi toplumuna geçiş; güvenlik stratejisi tasarımını, çalışmalarını, yapısını önemli ölçüde değiştirmiştir. Aynı çerçevede günümüzde, dijital çağda güvenlik stratejisi tasarımının bir kez daha değişime uğradığı değerlendirilmektedir.

Yukarıda belirtilen soruların cevaplandırılabilmesinde bir başlangıç noktası sağlayacak şekilde, öncelikle klasik güvenlik stratejisi kavramının incelenmesi ve açıklanmasının yapılması gerekmektedir. Güvenlik stratejisi tasarımında genel olarak klasik stratejisi tasarımı olarak; Arthur F. Lykke Jr tarafından ortaya konulan ve denklem olarak da ifade edilen yaklaşım kabul görmektedir. Strateji = Hedef + Konsept + Kaynak[99] (Güç unsuru). Lykke'nin yaklaşımının bir başlangıç noktası olarak alınabileceği değerlendirilmektedir. Bu çerçevede, klasik güvenlik stratejisi tasarımında; durum tespiti, nihai hedefin belirlenmesi, güç unsurlarının belirlenmesi, konseptin hazırlanması, risklerin tespit edilmesi safhalarından oluşan beş safhalı bir süreç kullanılabilir.

Strateji tasarımı bir plan değildir. Planlar da genellikle strateji hazırlanması prensiplerinde; nihai hedef+konsept+güç unsurları esas alınarak hazırlanır. Ancak stratejist tasarımı yaparken birçok bilinmeyeni bilinir hale getirerek planlamanın yapılacağı zemini oluşturur. Stratejilerin belirlediği zemin çerçevesi esas alınarak planlar daha deterministik ve lineer bir yapı oluşturabilir.

Klasik strateji tasarlama süreci her ne kadar Lykke'nin makalesinde bir formül olarak ifade edilmekteyse de strateji tasarımının sabit formül ile tanımlanması uygun bir hal tarzı olarak görülmemelidir. Çünkü değişik durumlar, amaçlar, konular için değişik strateji tasarım modelleri ve mantıkları kullanılabilecektir. Belirli bir durum ve amaç için kullanılan strateji tasarım modeli ve mantığı başka bir durum için geçerli olmayacaktır. Bu çerçevede tasarımın içeriği ve formatı da değişik olabilecektir.

Strateji tasarım sürecinin ilk safhası durum analizi yapılmasıdır. Sun Tzu'nun "Hem düşmanınızı hem de kendinizi tanıyorsanız yüz tane savaştan bile korkmanıza gerek yok" ifadesi stratejik durum analizinin önemini en iyi vurgulayan sözlerden birisidir. Durum analizi tasarım faaliyetlerine önemli bir zemin ve girdi sağlayabilecektir. Stratejik durum analizi stratejik tasarımın başında yapılan bir faaliyet olarak görülmesine rağmen, stratejinin yönetimi aşamalarında ağırlıklı olarak

[99] Lykke, Arthur F. Jr., Defining Military Strategy, *Military Review*, C. 69, S. 5, 1989.

sürekli kullanılacak önemli bir yapıdır. Bu nedenle durum analizi sistematiği bu husus göz önünde tutularak, başlangıçtan itibaren süreç içerisinde etkin bir şekilde kullanılabilecek bir yapıya oturtulmalıdır.

Durum analizi genellikle "stratejik çerçeve" başlığı altında strateji dokümanlarında yer almaktadır. Durum analizinde millî menfaatler-haklar-değerler, tehditler, fırsatlar, faraziyeler, problemin tanımlanması, küresel, bölgesel ve ülke içi durum, tahditler gibi hususlar yer alabilir. Tasarımcıların yaptıkları en önemli hata yukarıda belirtildiği gibi stratejinin amacına göre durum analizinin içeriğini oluşturamamaları, yani stratejik çerçeveyi çizememeleridir. Bu bölüme ilgili ilgisiz konuların doldurulması analizin kalitesini etkilerken, tasarımcının dikkatini dağıtabilecek, yanlış bir istikamete odaklanmasına neden olabilecektir. Doğal olarak bu husus zincirleme olarak tasarım sürecinin diğer safhalarını da olumsuz etkileyebilecektir. Durum analizinin etkinliğini arttırmak maksadıyla, faktör analizi, sistem analizi, GZTF analizi, beş halka metodu gibi metotlar kullanılabilir. Bu metotlar durum analizine yardımcı olacak şekilde bu bölümde açıklanmıştır.

Strateji tasarım sürecinin ikinci safhası nihai hedefin belirlenmesidir. Nihai hedef, stratejik tasarımın uygulanması neticesinde elde edilmesi düşünülen nihai durum olarak açıklanabilir. Strateji mevcut durum ile arzulanan durum arasında bir köprü olarak görüldüğünde, nihai hedeften geriye doğru, mevcut duruma kadar safhalar halinde tasarımın yapılması nispeten daha kolay olacaktır. Bu çerçevede nihai hedeften önceki adımların ortaya konulması, mevcut durumdan yola çıkarak müteakip adımların ortaya konulmasından daha gerçekçi ve daha kolay değerlendirmelerin yapılmasını sağlayabilecektir.

Güvenlik stratejisi tasarımında ne yapılacağı, nasıl yapılacağından çok daha önemlidir. Ne yapılacağı istenen amaca uygun olarak belirlenmediği takdirde daha başlangıçta stratejinin istikameti yanlış olacak, nasıl sorusu burada daha başlangıçta önemini yitirecektir. Ne yapılacağının doğru olarak belirlenebildiği bir durumda, nasıl yapılacağı konusunda sıkıntı olsa bile düzeltmek için fırsat olabilecektir. Ancak ne yapılacağı yanlış olarak belirlendiğinde düzeltme yapılması çok daha zor olabilecektir.

Strateji tasarımının üçüncü safhası güç unsurları/kaynakları/araçların belirlenmesidir. Millî güç unsurları konusunda bir devletin millî gücünü belirleyen üzerinde anlaşmaya varılmış bir liste veya formül bulunmamaktadır. Genel olarak coğrafi, politik, ekonomik, askeri, demografik, kültürel, bilimsel ve teknolojik güç

olarak yedi başlık altında toplanabilir. Ancak bu listeye günümüzde başta sağlık alt yapısı, doğal kaynaklar (Coğrafyadan ayrı olarak değerlendirilmesi gerekebilir.) olmak üzere ilave unsurlar da eklenebilir. Burada kritik olan husus herhangi bir aktörün bu listede yer alan unsurları stratejik hedeflere ulaşılması için kullanılabilecek imkân ve kabiliyetlere dönüştürebilme kapasitesidir. Bu kapasite millî güç sistemi olarak adlandırılabilir.

Millî güç unsurlarının yanında bu gücün kullanılma yöntemi; yani sistemi önemlidir. Bu sistem aynen potansiyel bir gücün kinetik güç haline getirilmesine benzetilebilir. Millî Güç Sistemi; millî güç unsuru, aktör veya kurum, araçtan oluşabilir[100]. Bu sistemde millî güç unsuru banka hesabında bulunan kaynak veya hammadde olarak algılanabilir. Bu unsurlar kullanılarak milletin refahının sağlanmasının yanında, güçlü devlet kuruluşlarının oluşturulması, geliştirilmesi sağlanır. Ancak bu unsurlar sonsuz değil, sınırlıdır. Bu güç unsurlarının, hesapsızca kullanılması, zayıflaması devletin zayıflaması anlamına gelecektir. Güç kullanım sistemi üç unsurun bir araya getirilmesiyle potansiyel, yani statik gücün kinetik hale getirilmesini sağlayabilir. Ancak önerilen bu sistemin anlaşılması, oluşturulması ve güvenlik stratejisinin icrası anlamında idare edilmesi oldukça zordur. Bu nedenle süreç tasarımı mümkün oldukça basit yapılmalıdır.

Bir devletin sadece kaynaklarının veya imkân ve kabiliyetlerinin olması güçlü olduğu anlamına gelmemektedir. Bu kaynakları veya imkân ve kabiliyetleri işe veya sonuca dönüştürebilmesi için araçlara ihtiyacı bulunmaktadır. Çok güçlü araçlarınız olabilir, ancak kaynaklarınız yeterli olmayabilir. Bu kaynak veya imkân ve kabiliyetlerin millî menfaatler doğrultusunda kullanılabilmesi için araçların kullanılması gerekmektedir. Kaynak/imkân ve kabiliyetler ile araçların etkin kullanılabilmesi için bir sistem yani mekanizma yaratılması gerekmektedir. Bu sistem veya mekanizmanın bütününe millî güvenlik sistemi diyebiliriz.

Strateji tasarımının dördüncü safhası konsept tasarımıdır. Güvenlik stratejileri tasarımının en zor bölümlerinden birisi, belki de en zoru; millî menfaatler çerçevesinde, kaynak ve imkân, kabiliyetler millî güç unsurları kullanılarak bir sistem dâhilinde hedeflerin ele geçirilmesi için bir yol haritası hazırlanmasıdır. Hedefler "ne" yapılacağını, kaynaklar ve imkânlar, kabiliyetler "ne ile yapılacağını", yol haritası ise

[100]Heffington, Steven; Oler, Adam; Tretler, David; *A National Security Strategy Primer*, 2019, s. 32.

"nasıl yapılacağını" ortaya koyacaktır (Şekil 1.7). Eldeki kaynak ve imkân, kabiliyetlerin sınırlı olması bu bölümün zor olmasının temel nedenlerinden birisini oluşturmaktadır. Bu bölümün zor olmasının diğer bir nedeni ise araçların birbirlerinin etkilerini olumsuz etkilemeyecek şekilde koordine edilmesidir. Aynı aracın birden fazla hedefe angaje olması ve birden fazla kurumu/kuruluşu ilgilendirmesi zorluğu daha da artırmaktadır.

Strateji tasarımının beşinci ve son safhası risklerin belirlenmesi ve yönetilmesidir. Güvenlik stratejileri tasarımındaki önemli adımlardan birisi maliyet/risk analizidir. Bu analiz tasarım safhasında yapılacağı gibi icra safhasında da yapılması gereken önemli bir işlemdir. Hatta strateji tasarlanırken icra safhasında maliyet/risk analizi yapılması gerektiği dikkate alınarak tasarımda gerekli düzenlemelerin yapılması ve buna ilave olarak bir stratejinin değerlendirme planının yapılması özellikle önemlidir.

Başlangıçta yapılacak maliyet/risk analizinde; nihai hedef/hedefler-kaynaklar/kabiliyetler-araçlar/konseptler arasında bir dengenin ve uyumun olduğu teyit edilmelidir. Bu unsurlar arasında bir uyum olmadığı takdirde risk oluşabilecektir. Böyle bir riskin oluşması güvenlik stratejisinin temelini oluşturan saç ayaklarının bir tarafa doğru dengesinin bozulmasına benzetilebilir[101](Şekil 1.8). Bunun yanında güvenlik stratejisi tasarımı belirli hedeflere ulaşılmasını sağlarken, başka alanlarda da risk oluşturabilir. Bu riskin de dikkate alınmasının uygun olacağı düşünülmektedir.

Güvenlik ortamındaki ve teknolojik alandaki gelişmelerden kaynaklanan faktörlerin dijital çağda yukarıda açıklanan klasik güvenlik stratejisi tasarımını önemli ölçüde etkileyebileceği değerlendirilmektedir. Dijital çağın yeni başladığı dikkate alındığında; etkin bir değerlendirme yapılabilmesi için yeterli zaman geçmemiş ve kaynak yayımlanmamış olmasına rağmen, kısmen de olsa bir değerlendirme yapılarak dijital çağa uygun bir güvenlik stratejisi tasarımı ve yönetimi modeli üzerinde çalışılabilir.

Dijital çağda güvenlik ortamında; belirsizlik, muğlaklık artarken; teknolojinin kullanımıyla tarihin akışı hızlanmış; stratejik şoklar, yeni tehditler, yeni aktörler ortaya çıkmıştır. Arap Ayaklanmaları, salgın hastalıklar, yeni tip terör saldırıları, teknolojiye bağımlılık dijital çağdaki tehditlere örnek teşkil ederken; özel askeri şirketler, devlet

[101] Lykke, Arthur F. Jr., Defining Military Strategy, Military Review, C. 69, S. 5, 1989.

dışı aktörler, uluslararası şirketler yeni tip aktörlere örnek gösterilebilir. Neoliberal düzenin zayıflaması, mali krizlerin meydana gelmesi, uluslararası örgütlerin zayıflaması kural tabanlı küresel sistemi ve küresel işbirliğini olumsuz etkilemektedir. Rusya-Ukrayna savaşı ise dijital çağda ulus-devletlerin yıkıcı etkisi olabilecek klasik savaşa ve hatta nükleer savaşa bile başvurabileceklerinin önemli bir örneğini teşkil etmektedir.

Dijital çağ güvenlik ortamının klasik güvenlik stratejisi yaklaşımına etkilerinin başında; klasik mantıkla güvenlik stratejileri tasarımı ve bu sayede millî menfaatlerin gerçekleştirilmesinin oldukça zor olduğu gerçeği gelmektedir. Bu nedenle güvenlik stratejileri tasarımının ve yönetiminin günümüz koşullarına uyarlanması gerekmektedir. Dijital çağda, güvenlik ortamında meydana gelen değişiklikler dikkate alındığında klasik strateji tasarımı etkinliğini, belki de geçerliliğini yitirdiği, en azından dijital çağdaki güvenlik ortamının şartlarına uyum sağlaması için gerekli tedbirlerin alınması gerektiği açık olarak ortaya çıkmıştır.

Dijital çağdaki güvenlik stratejileri tasarımını etkileyebilecek teknolojik gelişmeler çerçevesinde; bilgisayar teknolojisindeki gelişmelerin tasarımı önemli ölçüde etkileyebileceği kabul edilmesine rağmen, diğer teknolojik gelişmeler de tasarımı önemli ölçüde etkileme potansiyeline sahiptir. Güvenlik stratejisi tasarımını etkileme potansiyeli olan teknoloji ve buluşlardan bazıları; BV, YZ, internet, nesnelerin interneti, sosyal medya, metaverse, cep telefonları, yeni sensör teknolojileri, otonom sistemler, kuantum bilgisayarlar, siber savaş yöntemleri, uzay teknolojileri olarak özetlenebilir. Bunun yanında medya kuruluşlarının, televizyon ve radyo gibi haberleşme araçlarının da etkinliği teknoloji sayesinde artmıştır. Bu teknolojik gelişmeler dikkate alınmadan dijital çağda güvenlik stratejisi tasarlanması imkânsız hale gelmiştir.

Teknolojik gelişmelerin güvenlik stratejisi tasarımına etkileri kapsamında; BV ve YZ'nin beraber kullanımı stratejik tasarım sürecinin her safhasında etkinliği arttırma potansiyeline sahiptir. Ancak yaratıcı bir yaklaşımla BV ve YZ'nin üzerinde çalışılan safhanın şartlarına uyarlanması gerekmektedir. Stratejinin yönetimi konusunda da benzer yaklaşım geçerlidir. Stratejinin yönetim sürecinde, BV ve YZ kullanımı dijital çağın şartlarına süratle uyum sağlamasına önemli ölçüde yardımcı olabilecektir. İnternet, siber güvenlik, uzay teknolojileri, medyadaki gelişmeler gibi

yeni teknolojilerin de tasarım sürecinin her safhasında dikkate alınması önemli bir kuvvet çarpanı olabilecektir.

Bu değerlendirmeler ışığında dijital çağda güvenlik stratejisi tasarımı ve yönetimine etki edebilecek faktörler ve parametreler olarak; süratli değişim, belirsizlik ve muğlaklık, yeni aktörler, yeni tehditler, siber ve uzay ortamları gibi hususlar strateji tasarımı ve yönetiminde dikkate alınması gereken önemli faktörler olarak ön plana çıkmaktadır. Bu faktörler ve dijital çağ teknolojileri dikkate alınarak, karar verme, kriz yönetimi başta olmak üzere, strateji tasarımı ve yönetiminde kullanılan süreçlerin gözden geçirilmesi uygun olacaktır.

Karar alma süreçleri tasarımda dikkate alınması gereken önemli bir konudur. Bu anlamda stratejik seviye karar alma ve bu kararlar alınırken başta sürü zekâsı gibi teknolojilerden faydalanılması artık zorunluluk halini almıştır. Ayrıca özellikle BV, YZ, İnternet gibi teknolojik gelişmeler dikkate alınmadan yapılacak bir güvenlik strateji tasarımı dijital çağda geçerli olmayacaktır. Bunun yanında siber güvenlik, bilgi harekâtı gibi teknolojik gelişmelerin getirdiği bazı yöntemlerin tasarımda mutlaka dikkate alınması gerekmektedir. Bunun aksi rakip aktörlerin her zaman bir adım, hatta bazen çok daha fazla önde olmasına neden olabilecektir. Aynı şekilde tasarımın kolaylaştırılabilmesi için modelleme, dijital ikiz gibi teknolojik imkânlardan faydalanılması, önemli kolaylıklar sunarak dijital çağa uygun bir model oluşturabilmemizi sağlayabilecektir.

Bu değerlendirmeler çerçevesinde tezin soruları cevaplandırılmış ve tezin hipotezi kapsamında yeni bir model üzerinde çalışılmasının uygun olacağı değerlendirilmiş; yeni bir modelin oluşturulmasında kullanılabilecek bazı faktörler incelenmiştir.

Gelinen aşamada; güvenlik stratejisi tasarımı modeli olarak incelenen klasik modelin, dijital çağın ihtiyaçlarına cevap vermesi oldukça zordur. Bu nedenle hipotezde öne sürüldüğü şekilde klasik güvenlik stratejisi tasarım modelinde bazı değişikliklerin yapılması ve dijital çağ teknolojilerinden azami faydalanılması uygun olacaktır.

Yapılan incelemeler ve değerlendirmeler sonucunda dijital çağa uygun bir güvenlik stratejisi tasarım ve yönetim modeli ortaya koyabilmek için yalnızca tasarım konusunda bir model ortaya konulmasının yeterli olmayacağı değerlendirilmektedir.

Bu çerçevede beş konu üzerinde çalışılması uygun olabilecektir. Bunlar aşağıda belirtilmiştir.

Modelleme, prototip üretimi, deneme,

Periyodik değerlendirme sistemi,

Yeni güvenlik stratejisi modeli,

Strateji yönetim sistemi,

Dijital çağ teknolojilerinin kullanımı olarak ifade edilebilir. Bu konular özet olarak aşağıda belirtilmektedir.

Birinci bölümde, Şekil 1.3'te ortaya konulan model; durum tespiti, nihai hedef, güç unsurları-kaynaklar-araçlar, konsept, riskler olmak üzere beş ana safhayı içermektedir. Bu süreci dijital çağa uyumlu hale getirebilmek maksadıyla dört yeni safha eklenebilir. Bunlar; stratejinin modelinin oluşturulması, strateji prototipinin yaratılması, deneme, değerlendirme safhaları olabilir. Bu safhaların eklenmesiyle birlikte mühendislerin bir araba, silah gibi bir malzemeyi tasarlamalarına benzer bir yaklaşımla güvenlik stratejisi tasarımının yapılabileceği değerlendirilmektedir. Bu maksatla yeni bir tasarım süreci modeli önerilmiştir (Şekil 3.1).

Dijital çağın şartlarına cevap verebilecek yeni bir güvenlik stratejisi modeli önerilmiştir. Bu modelde; güç unsurlarının hedef temelinde gruplandırılması ve koordinatör tespit edilmesi, muhtemel karar ve kriz noktalarının belirlenmesi, kritik hattın belirlenmesi, değerlendirme periyotları ile siber ve bilgi harekâtı konularına ağırlıklı olarak yer verilmiştir (Şekil 3.4).

Birinci bölüm Şekil 1.8'de bir stratejinin risk değerlendirmesine yönelik model gösterilmektedir. Ancak model sadece stratejinin değerlendirmesini esas aldığından dolayı, stratejinin nihai hedefi olan millî menfaatin korunduğu veya ilerletildiğine yönelik bir model önermemektedir. Bu nedenle millî menfaat-tehdit-hedef ve hedefe bağlı olarak güç unsuru ve konseptin bir bütün halinde göz önüne alındığı yeni bir model önerilmiştir. Bu model, üzerinde çalışılan güvenlik stratejisinin özellikleri dikkate alınarak gözden geçirilebilir ve ihtiyaca göre uyarlanabilir. Bu model esas alınarak bir değerlendirme planı hazırlanması uygun olabilecektir (Şekil 3.5).

Güvenlik stratejilerinin yönetimi ile teknolojinin birleştirilmesi çerçevesinde John Boyd tarafından ortaya atılan, OODA (Observation, Orientation, Decision,

Action) çevrimi; gözlem, uyumlandırma, karar, icra (GUKİ) elemanlarından oluşan sistem, önemli bir model olarak karşımıza çıkmaktadır.[102] Söz konusu model, kriz yönetimi, organizasyon yönetimi gibi sosyal konularda kullanılmasının yanında; robotların, otonom veya uzaktan komutalı, YZ kullanılan sistemlerin tasarımında da karşımıza çıkmaktadır (Şekil 3.8).

Dijital çağada güvenlik stratejisi tasarımı kadar yönetimi de oldukça önemlidir. Yönetim modelinin tasarım ile uyumlu ve dijital çağa uygun bir yapıda olması stratejinin başarıyla uygulanması için önemli bir faktördür. Bu çerçevede tez çalışmalarında elde edilen bilgiler ve deneyimler ile GUKİ döngüsü dikkate alınarak bir model önerilmiştir. Önerilen modelde; tasarım, icra/izleme (uyumlandırma) ve değerlendirme olmak üzere üç ana safha bulunmaktadır (Şekil 3.9).

Güvenlik stratejisi yönetiminde teknoloji kullanımı konusunda yapılan araştırmalarda literatürde fazla çalışma tespit edilememiştir. Bu nedenle önerilen sistem yeni bir modeldir. Model daha önceki bölümlerde üzerinde çalışılan ve incelenen alt modellerin birleştirilmesinden oluşmaktadır.

Söz konusu modelde akan veri olarak gelen BV'nin uygun şekilde genel veri bankasına depolanması ve güncellenmesi gerekmektedir (Şekil 2.3). Genel veri bankasındaki veri kullanılarak stratejinin icrasının takip edilebileceği bir stratejik durum haritası veya dashboard oluşturulmalıdır (Şekil 2.4). Strateji yönetiminin başlangıcında oluşan durumun belirli aralıklarla kaydedilmesi, değerlendirme safhasında çok önemli bir girdi olabilecektir. Değerlendirme yapılırken geçmişte istenen herhangi bir zamanla mevcut durum mukayese edilerek geleceğe yönelik bir projeksiyon yapılması görsel olarak mümkün olabilecektir. Aslında bu görseli oluşturan veri çok kıymetlidir. Bu veri kullanılarak değerlendirmenin çok daha sağlıklı yapılması için uygun zemin oluşabilecektir. Değerlendirme, modelin en önemli bölümü olup dijital çağda teknolojinin de en fazla kullanılabileceği bölüm olarak görülebilir. Ancak bunun için bazı hazırlıkların tasarım aşamasında yapılması uygun olacaktır. Örneğin değerlendirme dönemlerine ulaşıldığında dashboard ve/veya stratejik durum haritasının yansıtması gereken şekil/görüntü, başlangıçta tahayyül edilmeye çalışılabilir (Şekil 3.10).

Başlangıçta teknolojik olarak oluşturulmuş olan mevcut durumun stratejik haritası veya dashboard, tahayyül edilen nihai durumun, değerlendirme dönemindeki

[102]Finney Nathan K, On Strategy: A Primer, 2020, s 71.

cari durum ile karşılaştırılarak arada tespit edilen farklardan önemli sonuçlar elde edilebilir. Bu dijital çağda değerlendirmenin teknoloji kullanılarak süratle ve daha etkin olarak yapılabilmesi için önerilen bir yöntemdir. Bu değerlendirme özet olarak cari durumun oluşmasına kadar elde edilen BV ve YZ kullanılarak müteakip dönemde oluşabilecek stratejik durum haritası elektronik olarak tahayyül edilmeye çalışılabilir. (Şekil 3.11)

Görüldüğü gibi konu başlıklarının tamamı konusunda incelemeler ve model önerileri yapılmıştır. Güvenlik stratejilerinin dijital çağa uyum sağlamasında üzerinde durulması gereken en önemli hususlardan birisinin risk ve değerlendirme konusu olduğunun bir kez daha vurgulanması uygun olacaktır.

Değerlendirmenin BV ve YZ kullanılarak uygun bir model esas alınarak yapılmasının önemli olduğu düşünülmektedir. Bu nedenle amaca ulaşmak maksadıyla uygun verinin tespit edilebilmesi, bu verinin doğru şekilde elde edilmesi, işleme tabi tutulması, sonuçların ilgili birimlere zamanında iletilmesi önem kazanmaktadır.

Aynı şekilde risk değerlendirmesi de önemlidir. Bu maksatla, hem güvenlik stratejisinin uygulanmasına hem de uygulama sonucunda oluşacak risklerin tamamının başlangıçtan itibaren değerlendirilmesi, maliyetlerin dikkate alınması stratejinin başarısı için oldukça önemlidir. Dijital çağın sağladığı imkânlar çerçevesinde risk değerlendirmesi için de BV ve YZ kullanılabilecektir. Verinin doğru olarak yönetilmesi, yönlendirilebilmesi için gerekli tedbirlerin alınması önemlidir.

Risk ve değerlendirmenin dijital çağda etkin yapılabilmesi maksadıyla veri hayati önemi haizdir. Bu nedenle verinin doğru olarak işleme tabi tutulabilmesi maksadıyla veri bilimciliği, veri analizciliği gibi dijital çağın bir gereği olarak ortaya çıkmış olan uzmanlık alanlarında gerekli personelin yetiştirilmesi; strateji tasarım ve yönetim teşkilatına dâhil edilmesi gelinen aşamada bir mecburiyet haline gelmiştir. Benzer hususlar siber güvenlik ve bilgi harekâtı personeli için de geçerlidir.

Bu tez gelecekte iki maksatla kullanılabilir. Bunlardan birincisi, içerdiği güvenlik stratejisi tasarımı ve yönetimi konusundaki nazari bilgiler ve açıklamalar çerçevesinde, uzmanların yetiştirilmesi maksadıyla yardımcı bir doküman olarak kullanılabilir. İkinci olarak güvenlik stratejisi tasarımı ve yönetiminin dijitalleştirilmesinde bir başlangıç dokümanı olarak kullanılabilir.

Tezde sunulan bilgilerle birçok konuda literatüre katkı yapılmaya çalışılmıştır. Ancak strateji tasarımının sanatsal yönünün olduğu dikkate alındığında önerilen modellerin üzerinde çalışılan konunun ve içerisinde bulunulan duruma göre uyarlamasının yapılması hayati önemi haiz olduğu göz önünde bulundurulmalıdır. Yapılabilecek en büyük hata strateji tasarımı ve yönetimi konusunda bir kalıp, formül veya süreç aranmasıdır.

Dijital çağda teknolojinin etkilemediği alan bulunmamaktadır. Doğal olarak güvenlik stratejisi ve tasarımı da daha önce açıklandığı şekilde teknolojik gelişmelerden etkilenecektir. Başta BV ve YZ olmak üzere günümüz teknolojileri güvenlik alanında gittikçe daha yaygın olarak kullanılmaya başlanmıştır. Bu teknolojilerin güvenlik stratejilerinin tasarımı ve yönetimine olan etkilerinin incelenmesi konusundaki çalışmalar oldukça yenidir, geliştirilmesine ihtiyaç duyulmaktadır. Tez teknolojik gelişmelerin güvenlik stratejisi tasarımı ve yönetiminde nasıl kullanılabileceğine yönelik öneriler sunmaktadır. Önerilen modellerden yola çıkarak yazılımlar geliştirilebilir. Bu yazılımların geliştirilmesinde strateji uzmanları ve yazılımcıların beraber çalışmaları gerekmektedir.

Strateji ve bilişim uzmanları tarafından oluşturulacak guruplarla başta; genel veri bankası, stratejik durum haritası, değerlendirme ve risk modelleri gibi konularda çalışmalar yapılabilir, yüksek lisans ve doktora tezleri hazırlanabilir. Aslında sadece bu konuları sürekli takip eden, üzerinde çalışan bir birimin kurulması da düşünülebilir. Dijital çağın teknolojilerini en iyi kullanan, güvenlik durumunu en iyi değerlendiren aktörlerin yalnızca güvenlik stratejisi tasarımında değil bütün alanlarda başarılı olma ihtimalleri artacaktır. Değişmeyen tek şeyin değişimin kendisi olduğu, teknolojik gelişmelerin sürekli ve süratle ortaya çıkmağa devam edeceği gerçeğinden hareketle değişime en iyi uyum sağlayan aktörün önemli bir avantaj sağlayabileceği gerçeği unutulmamalıdır.

Bu tez başlangıç olarak kabul edilip üzerinde çalışılabilecek ilk konulardan birisi; sosyal medya, haber ajansları ve internette güvenilir siteler kullanılarak küresel olayların harita üzerinde gösterilebildiği bir yazılım hazırlanması olabilir. Bu yazılımın hazırlanmasını müteakip elde edilen BV'nin depolanması, istenildiği zaman kullanılabilmesi için bir veri tabanı hazırlamak mümkün olabilir. Bu veriye sahip olunmasını müteakip YZ kullanılarak bu verinin istenildiği şekilde görsel hale getirilmesi, analizlerin yapılabilmesi üzerinde çalışılabilir.

Tezde ortaya konulmaya çalışılan modellerin istihbarat alanında kullanılması önemli bir avantaj sağlayabilir. Özellikle açık kaynaklardan elde edilen verilerin süratle özetlenebilmesi, önemli olduğu değerlendirilen verilerin zamanında karar vericilere sunulabilmesi bile önemli bir kuvvet çarpanı olabilir. Başta İHA'lar olmak üzere birçok algılayıcıdan görüntüler gelmektedir. Bunların birçoğu anlık olarak, eldeki imkânlar çerçevesinde değerlendirilmesi yapılarak depolanmaktadır. Diğer bir ifadeyle bu görüntülerin çoğu çöpe gitmektedir. Görüntü işleme yöntemiyle, bu görüntülerde tespit edilen nesnelerin doğru olarak tanımlamalarının yapılabilmesi ve geçmiş verilerle mukayese edilebilmesi yine önemli bir avantaj sağlarken, dijital çağ teknolojilerinin stratejik konularda kullanılabilmesinde iyi bir örnek olabilir. Yaratıcı bir anlayışla tezde önerilen modeller değerlendirilerek günümüzde güvenlik stratejisi tasarımı ve yönetimi konusunda karşılaşılan problemlere çözüm bulunabileceği gibi güvenlik stratejisi tasarım ve yönetiminin dijital çağa uygun bir hale getirilmesini sağlayabilir.

Sonuç olarak; dijital çağda ortaya çıkan, çok daha tehlikeli bir hale gelmiş olan yeni güvenlik ortamında güvenlik stratejisi tasarımı ve yönetiminin önemi gittikçe artmaya devam etmektedir. Dijital çağ teknolojileri günlük hayatımızın her alanını etkilemeye devam etmektedir. Önümüzdeki süreçte güvenlik stratejileri tasarımı ve yönetiminin dijitalleşmesi bir zorunluluktur. Güvenlik stratejisi tasarımı ve yönetimi konusunun daha iyi anlaşılması ve teknolojik imkânlar kullanılarak daha etkin hale getirilmesinde bu tezin önemli katkılar sunacağı değerlendirilmektedir. Güvenlik stratejisi tasarımı ve yönetiminde dijitalleşmeyi sağlayamayan ülkelerin millî güvenliklerinin tehlikeye girmesi söz konusu olabilecektir. Dijital çağ teknolojileri değişim ve dönüşümü hızlandırmalarının yanında, bu teknolojileri geliştirip kullanan taraf için bir güç unsuru, karşı taraf için ise bir tehdit olma özelliğine sahiptir. Dolayısıyla şimdiden bu konuda uzmanlar yetiştirmek, çalışmalar yapmak, gelecekte teknolojinin daha da gelişmesi neticesinde ortaya çıkabilecek yeni imkânların süratle kullanılabilmesini sağlayacaktır.

KAYNAKÇA

Ackoff, Russell, From Data to Wisdom, *Journal of Applied Systems Analysis*, C. 16, S. 1, 1989, s.3-9.

Aghuan, Ali, The Cyber Dimensions of ISIS's Occupation of Mosul, *The Washington Institute*, 2016.

Akhgar, Babak; Saathoff, Gregory B.; Arabnia, Hamid R.; Hill, Richard; Staniforth, Andrew; Bayerl, Petra Saskia, *Application of Big Data for National Security*, Butterworth-Heinemann, 2015.

Army.mod.uk, *77th Brigade, Influence and Outreach*, https://www.army.mod.uk/who-we-are/formations-divisions-brigades/6th-united-kingdom-division/77-brigade/, (E.T.1 Temmuz 2022).

Arı, Tayyar, *Uluslararası İlişkiler ve Dış Politika*, Alfa Yayınları, 2013.

Ayhan, Ufuk, *Metropoliten Alanlarda Güvenlik Sorunu ve Çözüm Önerileri*, Doktora Tezi, Ankara: Gazi Üniversitesi Sosyal Bilimler Enstitüsü, 2006.

Ayoub, Kareem ve Payne Kenneth, Strategy in the Age of Artificial Intelligence, *Journal of Strategic Studies*, 2016, C. 39, S. 5-6, 2015, s.793-819.

Özdemir, Hakan, ve Bakan, Selahaddin (2016). Ulus devletin oluşumu ve sorunları açısından Almanya ile Fransa'nın karşılaştırılması. *Bitlis Eren Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, C. 5, S.3, s.19-58.

Balkan, Serkan, *DAESH Drone Strategy Technology and The Rise of Innovative Terrorism*, Seta Publications, İstanbul 2017.

Buzan, Barry, *People, states & fear: an agenda for international security studies in the post-cold war era*, ECPR Press, 2008

Buzan, Barry, Wæver, Ole, ve De Wilde, Jaap (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Buzan, Bary and Wæver, Ole, Regions and Powers the Structure of International Security, 2003, s.40

Baylis, Jhon; Wirtz, James J.; Gray, Colin S., *Strategy in the Contemporary World*, Oxford University Press, 2019.

Berkebile, Richard E., *Military Strategy Revisited a Critique of the Lykke Formulation*, 2018.

Brands, Hals, *What Good is Grand Strategy*, Cornell University Press, 2014.

Bruce, Andy ve Langdon, Ken, *Strategic Thinking*, Dorling Kindersley LTD, 2000.

Bryant, David J., Rethinking OODA: Toward a Modern Cognitive Framework of Command Decision Making, *Military Psychology*, C. 18, S. 3, 2006. S.183-206.

Bukamal, H. (2022). Deconstructing insider–outsider researcher positionality. *British Journal of Special Education*, C. 49, S. 3, 327-349.

Carr, Edward H. *The Twenty Years Crisis*, Londra Palgrave Macmillan, 1939.

Charles, Caris ve Samuel, Reynolds, Middle East Security Report, *ISIS Governance in Syria*, ISW, 2014.

Chakravarthy, Bala; Lorange, Peter; Stewens, Günter Müller; Lecher, Christoph; *Strategy Process*, Wiley-Blackwell, 2003.

Chappel, George G, *A Terrorist Organization as a System: Unleashing Warden's Five-Ring Model*, New Port Naval War Coll, 2002.

Conradt, Larissa; List, Christian; Roper, Timothy J., Swarm Intelligence: When Uncertainty Meets Conflict, *The American Naturalist*, C. 182, S. 5, 2013, s.592-610.

Cox, Robert W., Social Forces, States and World Orders: Beyond International Relations Theory, *Millenium*, C. 10, S. 2, 1981, s.126-155.

Clausewitz, Carl von, *On War*, Princeton University Press, 1976.

Cancian, Mark F.; McPeak, Rick; Dalton, Melissa; Schaus, John; Metrick, Andrew; McElhinny, Colin, *Formulating National Security Strategy*, CSIS, 2017.

Digital 2022, *Global Overview Report*, bigumigu.com, (E.T.13 Mayıs 2022)

Digital 2022, We Are Social 2022: Dünyada ve Türkiye'de İnternet-Sosyal Medya Kullanımı, recrodigital.com, (E.T.13 Mayıs 2022).

Divanna, Joseph ve Austin, François, *Strategic Thinking in Tactical Times*, Palgrave MacMillan, New York 2004.

Drew, Dennis M., Snow, Donald M., *Making Strategy*, Air University Maxwell, 1988.

Doumpos, Michael ve Grigoroudis, Evangelos, *Multicriteria Decision Aid and Artificial Intelligence*, John Wiley and Sons, 2013.

Eriksson, Johan ve Giacomello, Giampiero, *International Relations and Security in the Digital Age*, Routledge, Londra 2007.

Hammond-Errey, Miah, *Big Data and National Security: A Guide for Australian Policymakers*, 2022

Finney, Nathan K., *On Strategy: A Primer*, Combat Studies Institute Press, 2020.

Fisunoğlu, Ali, System Dynamics Modeling in International Relations, *All Azimuth: A Journal of Foreign Policy and Peace,* C. 8, S. 2, 2019, s.231-253.

Fleming, M. H.; Brannan, S.J.; Mosher, A. G.; Altmire, B.; Metrick, A.; Boyle, M.; Say, R, *Unmanned Systems in Homeland Security*, Homeland Security Studies and Analysis Institute, Ocak 2015.

Freedman, Lawrence, *Strategy*, Oxford University Press, 2013.

Forest, James J.F., *Digital Influence Warfare in the Age of Social Media*, 2021.

Geeks for Geeks, *Changes Introduced By Napoleon in the Administrative System*, https://www.geeksforgeeks.org, 23 Mart 2023.

Grattan, F. Robert, *The Strategy Process; A Military-Business Comparison*, Springer, 2002.

Gray, Colin S., *Strategy & Defence Planning*, Oxford University Press, 2014.

Gray, Colin S., *Perspectives on Strategy*, Oxford University Press, 2013.

Greiner, Larry E. ve Cummings, Thomas G., *Dynamic Strategy-Making*, John Wiley and Sons, 2009.

Goria, Stephane, How to Adapt a Tactical Board Wargame for Marketing Strategy Identification, *Journal of Intelligence Studies in Business*, C. 2, S. 3, 2012, s.12-28.

Hart, Liddell, The Classic Book on Military Strategy; *Strategy* 2. Baskı, Mart 1991.

Haser, Demet, *Uluslararası İlişkilerde Güvenlik Kavramı: Soğuk Savaş Sonrası Dönem Güvenlik*, İstanbul Ticaret Üniversitesi, 2018.

Heffington, Steven; Oler, Adam; Tretler, David; *A National Security Strategy Primer*, National Defense University Press, 2019.

Heidegger, Martin, *Being and Time*, Suny Press, 2010.

Heinl, Caitriona H., *National Security Implications of Increasıngly Autonomous Technologies: Defining Autonomy, And Military And Cyber-Related Implications*, School of International Studies, 2015.

Hobbes, Thomas, *Leviathan*, Routledge, 2016.

Holcomb, James F., Managing Strategic Risk, *Cultural Trends*, C. 31, S. 3, 2022, s.240-256.

Hope, Mark, What is a Business Wargame, https://asymmetric.pro/what-is-a-business-wargame/, 2022, (E.T.29 Ocak 2022).

Joint Staff, *Planner's Handbook for Operational Design*, 2011.

Keller, Gary F., The Influence of Military Strategies on Business Planning, *International Journal of Business and Management*, C. 3, S. 5, 2008, s.129-134.

Kurtz, C.J., *Business Wargaming*, A Kappa White Paper, 2007.

Lau, Joyce, Who Are the Chinese Trolls of the "50 Cent Army"?, *Voice of America*, 2016.

Laskar, Manzoor Elahi, *Summary of Social Contract Theory by Hobbes, Locke and Rousseau*, SSRN, 2013.

Locke, John, *Hoşgörü Üzerine Bir Mektup*. çev. Melih Yürüşen, Ankara: Liberte Yayınları 2017.

Lykke, Arthur F. Jr., Defining Military Strategy, *Military Review*, C. 69, S. 5, 1989, s.2-8.

Machiavelli, Niccolo, *The Prince (1513).* Hertfordshire: Wordsworth Editions, 1993.

Mahnken Thomas G., *Net Assessment and Military Strategy*, Cambria Press, 2020.

Marine Corps War College, *Strategy Primer*, 2021.

Marwala, Tshilidzi, *Artificial Intelligence Techniques for Rational Decision Making*, Springer, 2014.

McFate, Sean, *Mercenaries and War: Understanding Private Armies Today*, National Defense University, 2019.

McCown, Neil R., *Developing Intuitive Decision-Making*, Joint Military Operations Department, 2010.

McCown, Margaret, *Strategic Gaming for the National Security Community*, *National Defense University*, Washington DC 2005.

Merriam Webster, https://www.merriam-webster.com/words-at-play/pyrrhic-victory-meaning, (E.T. 26 Mart 2023).

Miller, Christopher; Scott, Mark; Bender, Bryan, UkraineX: How Elon Musk's Space Satellites Changed the War on the Ground, 09 Haziran 2022, https://www.politico.com/news/2022/06/09/elon-musk-spacex-starlink-ukraine-00038039, (E.T. 09 Ekim 2022).

Mintzberg, Henry, *The Rise and Fall of Strategic Planning*, Pearson Education, 1994.

Morgenthau, Hans J., *Politics Among Nations. The Struggle for Power and Peace... Revised and Enlarged.[With Maps, and a Bibliography.]*. Alfred A. Knopf. 1955.

Lucarelli, Sonia; Marrone, Alessandro; Moro, Francesco N., *NATO Decision-Making in the Age of Big Data and Artificial Intelligence*, NATO, 2021.

Nye, S. Joseph ve Welch, David, *Küresel Çatışmayı ve İşbirliğini Anlamak*, Türkiye İş Bankası Yayınları, İstanbul 2017.

Nietzsche, Friedrich, *Thus Spoke Zarathustra (1883-1885)*

National Security Commission on Artificial Intelligence, *Final Report*, 2020.

NATO, *NATO 2022 Strategic Concept*, 2022.

NATO Science and Technology Organization, *Science and Technology Trends 2020-2040*, 2020.

Paret, Peter, *Makers of Modern Strategy,* Oxford University Press, 1986.

Patrikarakos, David, *War in 140 Characters, How Social Media is Reshaping Conflict in the Twenty-First Century*, Hachette, 2017.

Porter, Michael, *Competitive Strategy*, 1998

Ramirez-Ochoa, Perez-Dominguez, Marinez-Gomez, Luviano-Cruz, PSO, Swarm Intelligence-Based Evolutionary Algorithm as Decision-Making Stratetgy: A Review, *Symmetry,* C. 14, S.3, 2022, s.455.

Rousseau, Jean-Jacques, *Toplum Sözleşmesi 1762*, (Çev. Günyol, Vedat, 2006), Türkiye İş Bankası Kültür Yayınları, İstanbul 2006.

Richard, Rumelt P., *Good Strategy Bad Strategy*, Crown Business, 2011.

Onuf , Nicholas Word of Our Making: Rules and Rules in Social Theory and International Relations, Columnia University of South Caroline Press, 1989

Özkan, Gökhan, *Savunma İhtiyaçlarının Belirlenmesinde Farklı Bir Bakış Açısı: Sistem Dinamikleri Yaklaşımı*, STM, 2017.

Özer, Mehmet Akif ve İrdem, İbrahim, *Çıkmazların Karşısında Bürokrasi ve Ötesi,* Gazi Kitabevi, 2020.

Özpolat, H. (2017). Tanrının siyasetinden siyasetin Tanrısına egemenlik kuramının dönüşümü. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 23(2), 143-166.

Singer, P.W. ve Brooking, Emerson T, *LikeWar, Weaponization of Social Media*, Eamon Dolan Books, 2018.

Sandıklı, Atilla ve Emeklier, Bilgehan; Güvenlik Yaklaşımlarında Değişim ve Dönüşüm, *Uluslararası Balkan Kongresi: 21. Yüzyılda Uluslararası Örgütlerin Güvenlik Yaklaşımları ve Balkanlar'ın Güvenliği Bildiriler Kitabı*, 2011, s.28-29.

Slona, Julia, *Learning to Think Strategically*, 4. Baskı Routledge, 2020.

Sun Tzu, *On the Art of War*, Allandale Online Publishing, 2000.

Taylor, Christine, *Structured vs. Unstructured Data* (datamation.com), 21 Mayıs 2021.

Tellis, Ashley J, "What is in Our Interest": India and the Ukraine War, 2022.

Thomas, Timothy L., *Russia Military Strategy*, Foreign Military Studies Office, 2015.

Thucydides, *Peloponnesian War*, Çev. Martin Hammond, Oxford World's Classics, 2009.

Tickner, J.Ann, *Introducing Feminist Perspectives into Peace and Word Security Courses, 1995 ve Feminist Responses to International Security Studies*, 2004

Tillman, Taylor Nola, *Space Colonies Will Start Out Like the Wild West*, Grow Family-Friendly, 2016.

Tiryaki, Elif, *Açık Kaynak İstihbaratında Sosyal Medya Kullanımının Analizi*, Millî Savunma Üniversitesi, 2020.

Tracol, Clement, *Private Military Companies in the Contemporary Security Context*, E-International Relations, 2012.

Toma, Sorin-George ve Gradinaru, Catalin, From Military Strategy to Business Strategy, *Management Strategies Journal*, C. 31, S. 1, 2016. s.227-233.

Türk Dil Kurumu Sözlüğü, Türk Dil Kurumu, Ankara 2005, s.1811.

Underwood, Corinna, Automated Journalism-AI Application at New York Times, Reuters, and Other Media Giants, *Business Intelligence and Analytics*, 2019.

Ullman, Harlan, *Is Artificial Intelligence More Formidable Than Nuclear Weapons*, The Hill, 2021.

Unhcr.org, *Türkiye'deki Mülteci ve Sığınmacılar*,30 Haziran 2022

United States Army War College, *National Security Policy and Strategy*, 2016.

US Navy, Joint Doctrine 1-18, *Strategy*, 25 Nisan 2018.

US Navy, Joint Planning 5-0, 1 Aralık 2020.

Waltz, N Kenneth, Theory of International Politics, 1979, s.121

Wendt, Alexander Social Theory of International Politics,Cambridge University, 2003

Whitt, Kelly Kizer, *Who Owns All The Satellites?*, 8 Şubat 2022.

Wiraeus, David ve Creelman, James, *Agile Strategy Management in the Digital Age*, Palgrave Macmillan, 2019.

Zais, Mark M., Artificial Intelligence: A Decisionmaking Tecnology, *Joint Force Quarterly 99*, 2020.