T.C.
MİLLÎ SAVUNMA ÜNİVERSİTESİ
ALPARSLAN SAVUNMA BİLİMLERİ VE MİLLÎ GÜVENLİK ENSTİTÜSÜ
İSTİHBARAT ÇALIŞMALARI ANABİLİM DALI
İSTİHBARAT ÇALIŞMALARI PROGRAMI

HİBRİT HAREKÂT ORTAMINDA İSTİHBARATIN ÖZELLEŞMESİ: ABD ÖRNEĞİ

YÜKSEK LİSANS TEZİ

MAHMUT SEÇKİN ALIŞVERİŞCİ

TEZ DANIŞMANI: DOÇ. DR. SERKAN YENAL

ANKARA
EYLÜL, 2023

T.C.
MİLLÎ SAVUNMA ÜNİVERSİTESİ
ALPARSLAN SAVUNMA BİLİMLERİ VE MİLLÎ GÜVENLİK ENSTİTÜSÜ
İSTİHBARAT ÇALIŞMALARI ANABİLİM DALI
İSTİHBARAT ÇALIŞMALARI PROGRAMI

YÜKSEK LİSANS TEZİ

MAHMUT SEÇKİN ALIŞVERİŞCİ

Tezin Enstitüye Verildiği Tarih:
Tezin Savunulduğu Tarih:

Tez Oy birliği / Oy çokluğu ile başarılı bulunmuştur.

Unvan Ad Soyadı	**İmza**
Tez Danışmanı	
Jüri Üyeleri	

ANKARA
AĞUSTOS, 2023

ÖZGÜNLÜK RAPORU

Tez çalışmamın a) Kapak sayfası, b) Giriş, c) Ana bölümler ve ç) Sonuç kısımlarından oluşan toplam 132 sayfalık kısmına ilişkin, ……/……/……. tarihinde şahsım tarafından Turnitin adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan özgünlük raporuna göre, tezimin benzerlik oranı % …'tür.

Uygulanan filtrelemeler:

1. Kaynakça hariç
2. Alıntılar hariç/dâhil
3. 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Millî Savunma Üniversitesi Alparslan Savunma Bilimleri Enstitüsü Lisansüstü Tez Çalışması Özgünlük Raporu Alınması ve Kullanılması Uygulama Usul ve Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

MAHMUT SEÇKİN ALIŞVERİŞCİ

Tarih:

ETİK BEYAN

Millî Savunma Üniversitesi Enstitüleri Lisansüstü Tez Hazırlama Kılavuzu'nda yer alan kurallarına uygun olarak hazırladığım bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu, bildirir; aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Bu tezdeki düşünce, görüş, varsayım, sav veya tezler bana aittir; Millî Savunma Bakanlığı, Türk Silahlı Kuvvetleri, Kara Kuvvetleri Komutanlığı, Millî Savunma Üniversitesi ve Alparslan Savunma Bilimleri Enstitüsü sorumlu tutulamaz.

Mahmut Seçkin ALIŞVERİŞCİ

Tarih:

ÖNSÖZ VE TEŞEKKÜR

Savaş ve barış arasındaki çizginin her geçen gün bulanıklaştığı ve ülkelerin politik çıkarları doğrultusunda diğerleri üzerinde caydırıcılık ve politik savaşın ötesine geçer bir şekilde güç kullanımına şahit olduğumuz özellikle son on yılın büyük kısmını gelişmelerin içinde büyük karargâhta ya da bizzat komuta ettiğim birliğimle harekât alanında geçirdim. Gerek kullanılan taktik ve tekniklerdeki değişim, kullanılan teknolojilerdeki gelişim, gerekse mücadele sahasındaki aktörlerin çeşitliliği artık muharebenin bilinen konvansiyonel savaş ve terör örgütleri ile mücadele odaklı düzensiz harekâtın ötesine geçtiğini yaşayarak tecrübe ettim. Bu değişim, karar vericinin karşısına daha fazla bilinmez ve değişkenler çıkartırken planlama ve icraya ışık tutan istihbarat fonksiyonunu daha detaylı irdeleme ihtiyacı hissetmemi dürtüledi. Meslek hayatım boyunca içinde olduğum bu alandaki gelişmeleri araştırdığımda ise; bu gizemli fonksiyon alanının da ciddi bir dönüşüme sahne olduğunu, kamu tekelinin kırıldığını, teknoloji ve analiz yetenekleri ile sivil şirketlerin devletlere hizmet satar konuma geldiklerini, bu alana dev yatırımlar yapıldığını, ABD başta olmak üzere ülkelerin de sunulan bu hizmetler için dev bütçeler ayırmalarını öğrenmem bu konuya olan ilgimi artırdı. İstihbaratın özelleşmesine ilişkin genel bir yazın taraması yapmam neticesinde bu alanda çok fazla bir çalışma yapılmamış olduğunu tespit etmem, bu konuyu çalışmak istememin en önemli etkenini oluşturdu. Sivil istihbarat şirketleri ve düşünce kuruluşları makale ve dergi yazılarında çalışılmış olsa da savaşın dönüşümü ile eş güdüm içerisinde; yeni harekât tabanları, değişen tehditler, yeni teknolojilerle desteklenen yeni toplama ve analiz yetenekleri ile dönüşen istihbarat ihtiyaçlarını karşılamada bir çözüm yolu olarak ortaya çıkan istihbaratın devlet kurumları dışından teminini bütünleşik olarak inceleyen az sayıda çalışma olması ise en önemli motivasyon kaynağım olmuştur.

Tez çalışmamda; savaşın tarihsel süreç içerisinde dönüşümü ile istihbarat ihtiyaçlarında da bir değişimin ortaya çıktığı ve bu ihtiyaçları karşılamada bir çözüm yolu olarak istihbaratın özelleşmesi ele alınmaktadır. Çalışmada konu, askerî ve güvenlik istihbaratı ekseninde irdelenmiş ve bu alanda başat rolünü kimseye kaptırmayan ve hatta kendini istihbaratın dışarıdan teminine fazlasıyla kaptırmış olan ABD özelinde incelenmektedir.

Öncelikle bu araştırmanın her aşamasında bana büyük bir motivasyon sağlayan ve sabırla destek olan, görüş ve önerileriyle tezime değer katan sevgili danışmanım **Doç. Dr. Serkan YENAL**'a teşekkürlerimi ve saygılarımı sunarım. Ayrıca, eğitim hayatımda emeği geçen saygıdeğer hocalarım **Doç. Dr. Nihat Ali ÖZCAN, Doç. Dr. Merve SEREN** ve **Doç. Dr. Engin AVCI**'ya, çalışmam süresince desteği ile her an yanımda olan sevgili eşime ve akademik çalışma hayatım boyunca manevi desteğini her an yanımda hissettiğim sevgili **Elif GÜLTEKİN**'e teşekkürlerimi iletirim.

ANKARA, 2023 Mahmut Seçkin ALIŞVRİŞCİ

İÇİNDEKİLER

Sayfa

KISALTMALAR LİSTESİ

ABD	: Amerika Birleşik Devletleri
BM, UN	: Birleşmiş Milletler
CIA	: Merkezi İstihbarat Teşkilatı (ABD)
COG	: Hükümetin Devamı
DEAŞ TÖ	: Irak Şam İslam Devleti Terör Örgütü
ELINT	: Elektronik İstihbarat
GEOINT	: Jeo-uzaysal İstihbarat
IMINT	: Görüntü İstihbaratı
IRA	: İrlanda Cumhuriyet Ordusu
İKK	: İstihbarat Karşı Koyma
İNİS	: İnsan İstihbaratı
KGB	: Rus İstihbarat Teşkilatı
MASINT	: Ölçüm ve İz İstihbaratı
MCDC	: Çokuluslu Yetenek Geliştirme Merkezi
MÖ	: Milattan Önce
NATO	: Kuzey Atlantik Paktı
NSA	: ABD Ulusal Güvenlik Ajansı
ODNI	: ABD Ulusal İstihbarat Direktörlüğü Ofisi
OSINT	: Açık Kaynak İstihbaratı
PYD TÖ	: PYD Terör Örgütü
SIGINT	: Sinyal İstihbaratı
SMO	: Suriye Milli Ordusu
SOCMINT	: Sosyal Medya İstihbaratı
SOI	: Düşmanın İlgi Sinyalleri
SSCB	: Sovyet Sosyalist Cumhuriyetler Birliği
TDK	: Türk Dil Kurumu
TRADOC	: ABD Eğitim ve Doktrin Komutanlığı
UK	: Birleşik Krallık
UNGA	: Birleşmiş Milletler Genel Kurulu
YPG TÖ	: YPG Terör Örgütü

ÖZ

HİBRİT HAREKÂT ORTAMINDA İSTİHBARATIN ÖZELLEŞMESİ: ABD ÖRNEĞİ

Mahmut Seçkin ALIŞVERİŞCİ

Milli Savunma Üniversitesi, Alparslan Savunma Bilimleri ve Milli Güvenlik Enstitüsü
Ankara, Ağustos 2023

Bu tez, günümüz güç mücadelesinin sahaya yansıması olan hibrit harekât ortamında harekât alanının dinamizmi ve çok boyutluluğu ile karar vericinin ihtiyaç duyduğu istihbarat ihtiyacının yeni doktrinel dönüşümünü tanımlarken, bu ihtiyacın karşılanmasında devlet kurumları dışından teminin ne derece etkin bir çözüm olduğunu sorgulamaya odaklanmaktadır.

Çalışmanın birinci bölümünde öncelikle günümüz harekât ortamını daha iyi anlamaya yardımcı olmak üzere savaşın dönüşümü üzerinde durulmuştur. Güç kullanımının günümüz uygulamaları ve bu dönüşümün gerektirdiği doktrinel anlayış değişikliği kavramsal bir çerçevede tanımlanmaya çalışılmıştır.

İkinci bölümde; teknolojik gelişmeler, yeni aktörler ve savaş ile barış arasındaki belirsiz alandaki cereyan eden güç mücadelesinin ortaya çıkardığı daha dinamik, çok yönlü ve daha hızlı karar verme sürecinin gerekliliği ile istihbarat ihtiyaçlarının da değiştiği çalışmanın irdelenmiştir.

Bu belirsizliği artan günümüz mücadele ortamında toplama vasıtaları ile analiz yetenekleri üzerine yatırım yapan özel istihbarat şirketleri, karar vericinin ihtiyaç duyduğu istihbarat ihtiyaçlarının karşılanmasında birçok alanda devlet kurumlarının yeteneklerinin üzerine çıkmıştır.

Değişen istihbarat ihtiyaçlarını karşılamada teknolojilere entegrasyonları, istihdam ve adaptasyon yeteneklerinde çeviklik ile toplama ve analiz yeteneklerini artıran özel sektör istihbaratının ihtiyaçları karşılamada kamu istihbaratını desteklemek üzere mantıklı bir çözüm yolu olup olmadığı ise çalışmanın üçüncü bölümünde incelenmiştir. Doğası gereği muhafazakâr olan istihbarat fonksiyon alanındaki bu devrimsel dönüşüm fayda ve mahsurları ile irdelenmekle kalınmamış, bir zanaat ve akademik bir alan olarak istihbaratın gelişimi ne katkısı ele alınmıştır.

Sonuç bölümünde ise; küçümsenemez avantajları ile öne çıkan istihbarattaki özelleşmenin optimal şekilde kullanımına yönelik çıkarımlarla son görüş oluşturulmuştur.

Anahtar Kelimeler: İstihbaratın Özelleşmesi, İstihbaratın Dışarıdan Temini, Savaşın Dönüşümü, Hibrit Savaş, Hibrit Tehdit, İstihbaratın Dönüşümü,

Bilim Kodu:
Sayfa Sayısı: 131
Tez Danışmanı: Doç. Dr. Serkan YENAL

ABSTRACT

PRIVATIZATION OF INTELIGENCE IN HYBRID WARFARE ENVORONMENT: USA CASE

Mahmut Seçkin ALIŞVERİŞCİ
Turkish National Defense University, Alparslan Defense Sciences and National Security Institute
Ankara, August 2023

This thesis focuses on questioning how effective a solution is the outsourcing of intelligence to fulfill the intelligence requirements of the contemporary decision maker, while defining the doctrinal transformation of the hybrid operational environment with its dynamism and multi-domain characteristics, as the reflection of the great power competition to the modern-day conflict.

In the study initially, the transformation of war is explained to understand the commentary conflict. Within that context, the exercise of using force and the doctrinal transformation, from conventional joint operation approach through irregular operations in the counter-terrorism era then to multi-domain doctrine in today's hybrid operational environment is explained.

The second chapter examines the change in the intelligence requirements due to the new technologies, new actors and the dynamic, multi-domain modern operational environment which dictates prompt decision making a must. Today, the capabilities of the private intelligence companies, which invested on latest collection and analysis technologies, exceeded far beyond the government agencies' in many fields of intelligence.

The third chapter examines; To satisfy the evolving intelligence requirements, with their integration to technologies, employment advantages, agile practices, and adaptation, how logical a solution option is outsourcing intelligence from private intelligence companies? Besides going in details to the pros & cons of this revolutionary evolution in naturally very conservative field, intelligence, the role of private sector intelligence supporting intelligence as academics and as a profession is also looked over.

The final chapter wraps up thoughts about precautions to be taken for the optimal use of private sector intelligence to gain most from its advantages.

Keywords: Intelligence Outsourcing, Privatization of Intelligence, Private Sector Intelligence, Transformation of War, Hybrid Warfare, Hybrid Threat, Intelligence Transformation,

Science Code:
Pages: 131
Supervisor: Assc.Prof. Serkan YENAL

1. GİRİŞ

Devletlerin kendi ulusal çıkarlarını gerçekleştirmek üzere birbirleri üzerinde üstünlük kurma çabaları, diplomatik çözüm yollarının tükenmesi veya uzlaşının sağlanamaması nihai olarak sert güç kullanımını, diğer bir deyişle savaşı doğurmuştur. Sonuçları her ne kadar yıkıcı olsa da modern anlamda savaş, 1648 Vestfalya Antlaşması'ndan günümüze, ulus devlet kavramı çerçevesinde diğer ülkelerin iç işleri ve toprak bütünlüğüne saygı duyma prensibi ile ve sonrasındaki pek çok antlaşma ile kısıtlanmaya çalışılsa da önlenememiştir. Gelişen medeniyet ve teknolojilerin etkisi ile sürekli bir dönüşüm içinde olan bu güç dönemsel olarak doktrinel değişimleri de beraberinde getirmiştir. Bu doktrinel dönüşümün incelenmesi, günümüz güç mücadelesini anlamak ve yakın geleceği yorumlayarak çıkarımlar yapmak için elzemdir. Çalışmanın birinci bölümü giriş bölümünü oluştururken, ikinci bölümünde günümüz harekât ortamını daha iyi anlamaya yardımcı olmak üzere savaşın dönüşümü üzerinde durulmuştur. Güç kullanımının günümüz uygulamaları ve bu dönüşümün gerektirdiği doktrinel anlayış değişikliği kavramsal bir çerçevede tanımlanmaya çalışılmıştır.

Kısıtlı da olsa güç kullanımını, karar vermek için gerekli analiz edilmiş veriyi sağlayan istihbarattan ayrı düşünmek mümkün değildir. Bu bağlamda tezin üçüncü bölümde; teknolojik gelişmeler, yeni aktörler ve savaş ile barış arasındaki belirsiz alandaki cereyan eden güç mücadelesinin ortaya çıkardığı daha dinamik, çok yönlü ve daha hızlı karar verme sürecini gerekli kılan istihbarat ihtiyaçlarındaki değişim irdelenmiştir.

Pek tabiidir ki istihbarat da gelişen teknolojik imkânlar, mücadele ortamından gelen ihtiyaçlar ile zanaat ve disiplin olma yolundaki akademik çalışmalar ile uygulama, toplama, analiz ve düşünsel manada sürekli bir dönüşüm içerisindedir. Karar vericiye ışık tutan istihbarat alanında da yeni bir doktrin ihtiyacı doğmuştur. Bu belirsizliği artan günümüz mücadele ortamında toplama vasıtaları ile analiz yetenekleri üzerine yatırım yapan özel istihbarat şirketleri, karar vericinin ihtiyaç duyduğu istihbarat

ihtiyaçlarının karşılanmasında birçok alanda devlet kurumlarının yeteneklerinin üzerine çıkmıştır.[1]

Değişen istihbarat ihtiyaçlarını karşılamada teknolojilere entegrasyonları, istihdam ve adaptasyon yeteneklerinde çeviklik ile toplama ve analiz yeteneklerini artıran özel sektör istihbaratının ihtiyaçları karşılamada kamu istihbaratını desteklemek üzere mantıklı bir çözüm yolu olup olmadığı ise çalışmanın dördüncü bölümünde incelenmiştir. Doğası gereği muhafazakâr olan istihbarat fonksiyon alanındaki bu devrimsel dönüşüm fayda ve mahsurları ile irdelenmiş, günümüz çatışma ortamındaki dönüşümle birlikte değişen istihbarat ihtiyaçları ile yeni teknolojiler ışığında geliştirilen analitik yöntemleri uygulamaya geçirmiş özel istihbarat şirketleri ile iş birliğinin çağın ihtiyaçlarını karşılamada en etkin nasıl kullanılabileceğine yönelik çıkarımlarda bulunulmaya çalışılmıştır.

Günümüzde istihbarat teşkilatlarının eskiye nazaran çok daha acil ve hassas analiz gerektiren ihtiyaçlarının karşılanmasında özel sektörden destek alması bir norm haline gelmiştir. Şüphesizdir ki bunda yeni teknolojilerin etkisi büyüktür. Bugün istihbarat sektörünü destekleyen birçok şirketin imkân ve teknolojileri devlet kurumlarınınkilerle yarışır seviyededir. Sektöre sağladıkları avantajların detaylı inceleneceği özel istihbarat sektörü için ABD, 2006 yılı için istihbarat bütçesinin %70'ini (yaklaşık 42 milyar dolar) kontrat ödemelerine tahsis ettiğini açıklamıştır.[2] ODNI 2007 yılında özel şirketlere ayrılan bütçeyi ABD ulusal güvenliğini tehdit edeceği gerekçesi ile yayınlamayı reddetmiş ve bu günümüze kadar devam etmiştir. Özel şirketlere verilen projelerin gizliliği de bu alana ayrılan bütçelerinin hesaplanmasının önüne geçmektedir.[3]

Bu dev bütçe, ABD özelinde istihbarat topluluğunun nasıl bir ağırlığa sahip olduğunun basit bir göstergesi niteliğindedir. Gizli casus ağlarının işletilmesinden istihbarat analizine, sinyal istihbaratından örtülü operasyonlara, düşman esirlerinin sorgulanmasına özel istihbarat şirketleri istihbarat fonksiyonunun her alanında önemli görevler üstlenmiş durumdadır. Örneğin; 52,000 güvenlik kleranslı bilgi sistemleri çalışanı, 42 milyar dolar toplam kârı ile Lockheed Martin ABD ve dünyanın en büyük

[1] Shay Hershkovitz, *The Future of National Intelligence: How Emerging Technologies Reshaped Intelligence Communities* (Londra, Rowman & Littlefield, 2022) 71.
[2] Tim Shorrock, *Spies for Hire: The Secret World of Intelligence Outrourcing*, (New York, Simon & Schuster, 2008) 25.
[3] a.g.e., 17.

savunma odaklı şirketi ve istihbarat gücünü oluştururken, diğer yanda Virjinya/ABD merkezli SpecTal şirketi 300'ün üzerinde Çok Gizli kleranslı saha ajanı ile Afganistan ve Irak'ta istihbarat görevleri icra etmektedir.[4] Öte yandan, istihbarat alanında uluslararası bir kurumsallaşma ya da genel geçer bir hukuki çerçeve olmasa bile uluslararası iş birliği mekanizmaları ve bölgesel iş birliklerden bahsedilebilir. İstihbaratın köklü geçmişi, zamanla akademide bir disiplin haline gelmesi ve iş birliği mekanizmaları istihbarat alanında genel geçer kabul görmüş bir hukuk çerçevesi oluşmasa bile teamül ve etik kuralların oluşmasına zemin hazırlamıştır. Devletler için özellikle örtülü faaliyetler çerçevesinde bu etik kurallar ve teamüller bir sınırlılık arz etmekle birlikte bu sınırlamaları esnetmek adına özel şirketlerin imkânlarından faydalanıldığı görülmektedir. Çalışmanın sonuç bölümünde ise küçümsenemez avantajları ile öne çıkan istihbarattaki özelleşmenin optimal şekilde kullanımına yönelik çıkarımlarla son görüş oluşturulmuştur.

1.1. Araştırmanın Amacı ve Problemi

Bu tezin amacı; hibrit harekât ortamındaki değişimin, karar vericiler için elzem olan istihbarat ihtiyaçlarını da değiştirip değiştirmediğini inceleyerek, değiştirmiş ise; istihbarat ihtiyaçlarını karşılamada özelleşmenin etkin bir çözüm yolu olup olmadığını ve özel istihbarat şirketlerinden optimum faydanın elde edilebilmesi için nasıl bir çerçeve oluşturulması gerektiğine yönelik çıkarımlara ulaşmaktır.

Dinamizmi artan, çok aktörlü ve çok tabanlı günümüz çatışma ortamının ihtiyaçlarına çevik çözümler getiren özel istihbarat şirketlerinden en optimal faydanın sağlanabilmesi için hangi çerçevede istifade edilmesi gerektiğini ortaya koymak üzere istihbaratın dışarıdan temininin fayda ve mahsurları incelenmiştir.

Çalışmanın alt amaçları ise;

- Savaşın dönüşümü kapsamında çatışma alanına yansıyan doktrin değişiminin tehdidin değişimi doğrultusunda dönüşümünü açıklamak,
- Bu doktrinel dönüşüm ve güç mücadelesi içerisinde karar vericilerin istihbarat ihtiyaçlarındaki değişimi değerlendirmek,

[4] a.g.e., 24.

- İstihbaratın özelleşmesinin istihbarat ihtiyaçlarındaki değişime ne kadar cevap verebileceğini incelemektir.

1.2. Araştırmanın Önemi

Son dönemin popüler konuları olarak savaşın dönüşümü ve hibrit savaş üzerine pek çok çalışma bulunmakla beraber, savaşın dönüşümü ve bu eksende değişen günümüz çatışma ortamının değişen istihbarat ihtiyaçları, bu ihtiyaçların çözümü bağlamında istihbaratın dışarıdan temininin nedenleri ile yerini irdeleyen az sayıda çalışma olduğu görülmüştür. Tezin ana üç bölümünü oluşturan bu başlıkların pratikte birbirleri ile entegre oldukları dikkate alındığında bu başlıkların neden-sonuç ilişkisi içinde bütüncül incelenmesinin yapılan çalışmanın önemini artırdığı değerlendirilmektedir.

1.3. Araştırmanın Kapsamı ve Sınırlılıkları

Önceleri sadece askerî harekâtı desteklemek üzere düşünülen istihbarat, "Askerî İstihbarat" kimliğinden ayrışmış ve devletin karar vericilerini desteklemek üzere istihbarat teşkilatları olarak sivilleşmiştir. İstihbaratın ağırlık merkezinin askerî istihbaratın dışındaki diğer alanlarda sivil devlet kurumlarına kayması "İstihbaratın Sivilleşmesi" olarak kavramlaştırılmıştır. "İstihbaratın Özelleşmesi" ise gerek toplama vasıtaları gerekse analiz yetenekleri ile devletin istihbarat kurumlarının dışında özel şirketlerce istihbarat üretilmesi ve devletlerin bu şirketlerden bu hizmetleri satın almalarını tanımlamak için kullanılmaktadır.[5]

Çalışma, ülkeler arasında caydırıcılıktan çatışma dahil olmak üzere yürütülen uluslararası güç mücadelesi kapsamında askerî istihbarat odaklı bir incelemeyi esas almıştır. Gerek yakın dönem savaşlarında doktrinin oluşturulmasında gerekse harekâtların icrasını destekleyen istihbaratın şekillendirilmesinde başat rolündeki ABD modeli çalışmada esas alınmıştır.

Araştırmanın sınırlılığı ise istihbaratın gizli doğası ile ilgilidir. Dolayısıyla, çalışma her ne kadar gözlemlere dayansa ve kişisel saha tecrübelerinden faydalanılsa da herhangi bir ülkenin devlet kurum ya da kuruluştan direk olarak bilgi alınamamıştır. Öte yandan, istihbaratta uluslararası bir kurumsallaşma olmadığı için bu konuda net

[5] Simon Chersterman, "The Privatization of Intelligence", EJIL: Talk Blog of the European Journal of International Law, 2009, https://www.ejiltalk.org/privatization_of_intel/ [Erişim Tarihi 20.08.2022].

bir teorik çerçeve çizmek de mümkün değildir. Dolayısıyla çalışmada kullanılan kaynaklar, genellikle açık kaynak niteliği taşımaktadır.

Ayrıca özel istihbarat şirketleri, istihbarat fonksiyonları olsa da özel askerî şirketlerden ayrı tutulmuş ve çalışma istihbarat fonksiyon alanına odaklanmış özel sektör oluşumları ile kısıtlı bir yaklaşımı benimsemiştir.

1.4. Araştırmanın Türü ve Yöntemi

Çalışmanın tamamı kuramsal bir dönüşüm içerisinde birbiri ile bütünleşmiş uygulamalar olan harekât ve istihbaratı neden-sonuç ilişkisi içinde irdelemekte ve son derece muhafazakâr bir alan olan istihbaratta devrimsel bir değişim olarak özelleşmenin kaçınılmaz olarak hayata geçişi açıklanmaya çalışılmaktadır. Bu alanda başat konumda olan ABD modelinin esas alındığı çalışmada, pek çok akademisyen tarafından da eleştirilen bu modelin olduğu gibi kabul edilip edilmemesi gerektiği incelenmiştir. Sürekli sorgulayıcı bir yaklaşımla, fayda ve mahsurları ortaya koyularak, optimum bir fayda için ne tür bir yaklaşımın gerekli olduğu sonucuna erişilmeye çalışan nitel bir araştırmadır.

İncelenen konuya ilişkin altyapı oluşturmak üzere hukuki metinler, uluslararası anlaşmalar, kitaplar, hakemli dergilerde yayımlanan makaleler, düşünce kuruluşlarının rapor, analiz ve görüşleri, basın yayın organları, internetteki diğer açık kaynaklardan faydalanılmıştır. Sadece istihbarat şirketlerinin değil, sivillerin de çatışma alanına açık kaynak istihbaratı katkısını tespit etmek üzere sosyal medya platformlarında inceleme yapılmıştır. Daha aktif kullanılan Twitter üzerinden Ukrayna-Rusya krizine yönelik açık kaynak verileri (uçuş verileri, su üstü vasıtaların rota bilgileri vb.) kullanarak analiz yapan hesaplar tespit edilmiş, kâr amacı gütmeyen sivil kişilerin analiz edilerek açık kaynaktan erişilebilen veriler ile görsellerin coğrafi eşlemeleri ile istihbarat oluşturulduğu ve paylaşıldığı, bu değerlendirmelerin taktik sahaya yansımalarının olduğu tespit edilmiştir.

Çıkarım ve değerlendirmeler için raporlar ve söylemler analiz edilmiştir. ABD istihbarat topluluğu içinde koordinatör role sahip ABD Ulusal İstihbarat Direktörlüğünün her yıl yayınladığı Ulusal İstihbarat Stratejisi Raporları incelenerek ABD istihbaratının 2005'ten itibaren stratejisindeki değişim analiz edilmiştir. Ayrıca savaşın dönüşümünün incelendiği bölümde çatışma trendlerini analiz etmek

maksadıyla Heidelberg Uluslararası Çatışma Araştırmaları Enstitüsü'nün[6] yıllık olarak yayımladığı 1992-2020 yılları arasındaki 'Conflict Barometer' raporları incelenmiş ve çalışmaya veri sağlanmıştır.

Bunların yanında, ABD istihbaratının gelişim ve dönüşümüne ilişkin değerlendirmeler yapmak için ABD İstihbarat Topluluğu yöneticilerinin söylemleri analiz edilmiş, gelişimi işaret edilen alanlar ile çağı yakalamaya yönelik olarak topluluğa gösterilen yön konusunda kıymetli veri elde edilmiştir.

Yazın taraması ile oluşturulan kavramsal çerçeve, raporlardan toplanan veri ve ABD İstihbaratına yön veren yönetici ve akademisyenlerin söylemleri çerçevesinde irdelenmiş, günümüz istihbarat ihtiyaçları ve bu ihtiyaçların karşılanmasında bir çözüm yolu olarak istihbaratın özelleşmesi fayda-mahsur analizi ile desteklenerek incelenmiştir.

[6] The Heidelberg Institute for International Conflict Research (HIIK), Heidelberg Üniversitesi (Almanya) Siyasal Bilimler Enstitüsüne bağlı, dünya çapında siyasal çatışmaları araştırma, değerlendirme ve raporlama görevine odaklı bir çıkar amacı gütmeyken kuruluştur.

2. SAVAŞIN DÖNÜŞÜMÜ VE DEĞİŞEN HAREKÂT ORTAMI

2.1. Modern Anlamda Savaş ve Dönüşümü

Toplumlar kendi çıkarlarını diğerlerine kabul ettirmeleri için, insanın doğası gereği, gücünü artırma ve diğerleri üzerinde hegemonya kurma dürtüsü ile savaşırlar, ki dünya tarihinin savaşlar ile başladığı genel kabul gören bir yaklaşımdır. Tarihin başlangıcından günümüze savaşın doğası değişmese de kullanılan yöntemler zaman içinde insanlığın gelişimi doğrultusunda değişiklik göstermiştir. Modern anlamda savaşın dönüşümünü incelemek istersek, 17'nci yüzyıldan günümüze doğru 18'inci yüzyıl, 19'uncu yüzyıl, soğuk savaş dönemi ve sonrası olmak üzere, pek çok savaş tarihçisi gibi, tarihsel bölümlere ayırarak incelemek mantıklı olacaktır.

İnsanlık, **17'nci yüzyıl**ın başlarından itibaren, Otuz Yıl Savaşları (1619-1648) ile Gutmann'ın hegemonya dönemi diye tabir ettiği, dünya egemen güçlerin etkisi altında kontrolsüz bir şiddetin hüküm sürdüğü bir süreci yaşadı. Gilpin'in ortaya attığı bu "Hegemonik Savaş Teorisi; uluslararası sistemde güç dengelerinin değişiminin önemini ve etkilerini görmemizi sağlamıştır. Gücün bir devletten diğerine geçmesi, bahse konu dönemde savaşı kaçınılmaz kılmıştır. Ayrıca çözümün savaşla aranması ve diplomatik bir uzlaşının hiçbir egemen devletçe tercih edilmemesi, gerçekçi bir barış girişiminde bulunulmaması bu uzun savaş döneminin sebebi ve karakteristiğini oluşturmuştur. Uzun süren savaşın kaynakları tüketmesi ancak barışı mecbur kılmış ve 1648'de Vestfalya konferansları ile ulus devlet anlayışının temellerini atan antlaşma imzalanmıştır.[7] Günümüzün modern politik yapısının temellerini oluşturan Vestfalya Antlaşmasının savaş tarihinde de bir dönüm noktası olduğunu söylemek yanlış olmaz. Ulus devlet ve devletlerin ulusal orduları ile güvenliklerini sağladıkları bir dönemi başlatan anlaşma ile savaş alanlarında paralı askerlerin varlığı ciddi oranda azalsa da varlıkları tamamen ortadan kalkmamıştır.[8]

[7] Myron P. Gutmann, "The Origins of the Thirty Years' War", *The Journal of Interdisciplinary History*, C. 18, S. 4 (1988): 752-767 http://www.jstor.org/stable/204823 [Erişim Tarihi: 15.05.2022].
[8] Ferdi Güçyetmez, "The Changing Concept of War and America's Defence Policy.", *Lectio Socialis*, C. 5, S. 2 (2021): 75–88. https://doi.org/10.47478/lectio.837638 [Erişim Tarihi: 15.05.2022].

18'inci yüzyıla gelindiğinde ise; İngiltere ve Fransa birbirlerine karşı bir güç dengesi oluşturmaya çalışırken savaş, muharebe alanında karşı karşıya gelen ordular ile sınırlı kalmıştır [9]. Avrupa siyasasını domine eden dönemin bu iki hâkim gücünün mücadelesi **19'uncu yüzyıl**da ekonomik, teknolojik ve bunların yanında güç kullanımına yönelik bakış açısı, politika, strateji ve doktrindeki değişim ve gelişim ile savaşın da değişimini, dönüşümünü beraberinde getirmiştir. Artan milliyetçiliğin, ulus bilincinin etkisi ile ülkelerin ordularında daha önceki dönemlerde olağan olan paralı askerlerin artık tercih edilmemesine neden olmuştur. 18'inci yüzyılın sonlarında İngiliz ordusunun neredeyse tamamını gönüllüler oluştururken; Napolyon; Fransız vatandaşıyla ulusal bir ordu oluşturmuş, yeni silahları, doktrini ve askerî dehası ile karada egemen olurken, İngilizler ise denizlere hakimiyetleri ile dengeyi sağlamaya çalışmıştır. Ulus devlet kavramının oluşması ile ulusal orduların oluşması sonucunda savaş toplumun tamamını ilgilendirir hale gelmiştir. Clausewitz'in sıklıkla halk desteğinin önemini vurgulamasının[10] kaynağını da bu oluşturur.

Avrupa'da endüstri devrimine kadar süren iç savaşlar, din savaşları milyonlarca kişinin ölümüne neden olmuştur. Endüstri devrimi ile gelişen sanayi ve teknoloji savaşı ulusların arasındaki bir olgudan küresel bir boyuta taşımış ve **dünya savaşları dönemine** girilmiştir. Milliyetçi yaklaşımlar ve topyekûn savaş ile tüm halkın seferber edildiği dev ordular dönemi dünya savaşları döneminde de devam etmiştir.[11] Tren ve telgrafın kullanılması savaş, tek hatta karşı karşıya gelen orduların mücadelesinden çok daha geniş bir alana yayılmış, çok cepheli ve birleşik/müşterek bir karakter kazanmış, topyekûn savaş konsepti gelişmiştir.[12] Birinci Dünya Savaşında hem keşif hem taarruzi olmak üzere hava gücü kullanımı, motorize hareket yüksek ateş gücü ve zırh koruması ile birleşmiş yeni stratejiler ve parametreler gelişmiştir. Endüstriyel seferberlik ile seri harp silah araç ve gereçlerinin üretilmesi bu alandaki teknolojiyi de ileri sürüklemiştir. Lojistik ihtiyaçlar ile tren ve kamyon gibi ulaştırma yeteneklerinin önemi artmıştır. Statik mevzi muhabereleri çatışmaların temelini oluştururken, manevra yetenekleri ile savaş dinamizm kazanmanın ilk sinyallerini vermeye başlamıştır. Savaş; İkinci Dünya Savaşında yıldırım savaşı doktrini ile mevzi savaşı

[9] Haldun Yalçınkaya, Kadir Tamer Türkeş. "Yirmi Birinci Yüzyılda Çatışma Alanlarında Görülen Yeni Unsurlar", *Güvenlik Stratejileri Dergisi*, C. 4, S. 7 (2008): 60, https://dergipark.org.tr/en/pub/guvenlikstrtj/issue/7536/99214 [Erişim Tarihi: 06.05.2023].
[10] Carl von Clausewitz, *On War*, (Londra: Oxford University Press, 2007), 230-242.
[11] Martin Van Creveld, *Transformation of War*, (New York, The Free Press, 1991), 46.
[12] Colmar von der Goltz, *The Nation in Arms* (Londra: W.H.Allen & Co, 1887), 379.

dönemi sona ermekle birlikte harekât, iki tarafın bir temas hattında çatışmasından çok cepheli, derinliği olan dinamik bir karakter kazanmıştır. Denizlerde mücadele de denizaltıların etkinliği ile kara harekâtından farklı bir derinlik kazanmıştır. Radar gibi teknolojiler deniz ve hava harekâtlarında oyunu değiştiren teknoloji olmuş, harp silah araç ve gereçlerindeki teknolojik gelişmeler savaşın yıkıcılığını artırmış, kimyasal silahlar ve atom bombasının icadı ve kullanılması ile kitle imha silahları kavramı ortaya çıkmıştır.

İnsanlık tarihindeki en çok zayiata sebep olan İkinci Dünya Savaşından sonra savaşın önlenmesi kapsamında Birleşmiş Milletler (BM) Antlaşması 2'nci Maddesinin 4'üncü fıkrası ile, istisnai durumlar kapsam dışında bırakılmak üzere, güç kullanımı ve güç kullanma tehdidi yasaklanmıştır. Yasaklanmış olsa dahi, antlaşma metni içinde 'kuvvet' ve 'kuvvet kullanma tehdidi' terimleri net olarak açıklanmamış olması ülkelerce suiistimal edilebilecek bir durumu ortaya çıkartmaktadır. Ancak bu akde rağmen ülkelerin, politikalarını diğer ülkelere kabul ettirmek üzere askerî güçlerini kullanma yönündeki hırsı devam etmiş, BM antlaşmasındaki istisnai durumları suiistimal edecek metotlar geliştirme çabası içine girmişlerdir.

Dünya savaşlarını takip eden, ABD ve Sovyetler Birliği arasındaki iki kutuplu dönemi sembolize eden **Soğuk Savaş döneminde** ülkeler, bu iki süper gücün çevresinde toplanmış ve bu iki süper gücün çekişmesi kaynaklı sosyo-ekonomik ve politik problemler ile uğraşmak zorunda kalmışlardır. Bu durum karşılıklı ittifakların oluşmasını beraberinde getirmiş ve bunun neticesinde ülkeler savunma ve güvenliklerini kolektif savunma mantığını da kapsayacak şekilde yeniden inşa etmek zorunda kalmışlardır. Bu dönemde iki süper güç ve onlarla ittifak içindeki ülkeler arasında barış, stratejik dengenin muhafazası ile mümkün olabilmiş, nükleer silahların yıkıcı etkisi iki paktın direkt olarak karşı karşıya gelmelerini önlemiştir. Kissinger bu dengeyi; karşı tarafın kabul edilemez seviyede tahribata yol açabilecek misillemesinden çekinilmesi nedeniyle her iki tarafın da elindeki kitle imha silahlarını kullanamayacak olması olarak tanımlamaktadır. 1960'larda "Kısıtlı Kullanım" ilkesi ile olası bir savaşta nükleer silahların kullanımının muharebe sahası ve askerî hedefler ile kısıtlı tutulması konusunda uzlaşılsa da nükleer savaş eşiğinin geçilmesi ile dünyada yıkımın ne seviyeye geleceğinin kaygılarını ortadan kaldıramamıştır.[13]

[13] Henry Kissinger, *World Order* (New York: Penguin Books, 2015), 250.

Caydırıcılık bu dönemde güvenlik politikalarının temelini oluşturmuştur. İki süper güç arasındaki, nükleer başta olmak üzere, silahlanma yarışı bu iki gücün karşılıklı sıcak çatışmaya girmesini engellemiş, güç mücadelesi Vietnam, Afganistan gibi kenar kuşaktaki ülkeler üzerinde dolaylı olarak gerçekleşmiştir. Bu dönemde, küçük ülkeler süper güçlere karşı "Direniş Savaşları" diye de tanımlanan gerilla savaşı tekniklerini temel alan stratejiler uygularken, direnişle birlikte aslında dolaylı olarak diğer süper güçle mücadele eden diğer süper güç yeni teknoloji ve silah sistemlerini harekât alanına sürerek üstünlük kurmaya çalışmıştır. Bu mücadele içinde, değişen ve gelişen savaşlarda klasik topyekûn savaşlara nazaran daha az ve daha nitelikli insan gücüne ihtiyaç duyulacağının ilk sinyalleri verilmiştir. Kullanılan yeni teknolojiler ve yeni sistemler ise; daha çok özel sektörce karşılanan danışmanlık, lojistik ve teknik desteğin harekât alanına girmesine neden olmuştur.

Clausewitz'ci yaklaşım savaşın devletler arasında olduğunu ileri sürmektedir. Bu mantık üzerinden gidildiğinde; çatışan taraf devletler değil ise, yaşanan vahşetin boyutu ne olursa olsun adına savaş diyemeyiz sonucu çıkartılabilir. İki süper güç arasındaki çekişme çevresinde dönen güç mücadelesi ile 1950'lerden itibaren özellikle sömürü rejimleri altındaki üçüncü dünya ülkelerinde dini ya da ideolojik ve çoğunlukla da etnik kökenli yönetime başkaldırı hareketleri gözlenmeye başlanmıştır. Bu **özgürlükçü hareketler döneminde**, çoğunlukla halk ayaklanması, silahlanması ve alışık olunan konvansiyonel taktiklerin dışında gerilla taktikleri uygulayan, kimi zaman hedef seçmede asker sivil ayrımı gözetmeyen, şiddet ve propaganda ile davalarını anlatmaya ve taraftar toplamaya çalışan bir silahlı mücadele türü ortaya çıkmıştır.[14] Mücadele eden ülkelere göre terörist ya da asi olan bu gruplar, kimilerine göre özgürlük savaşçısı olarak kabul edilmiş ve meşru kabul edilmişlerdir. Meşruiyetlerini kabul edenlerin aldıkları dış destek ile çoğunlukla başarıya ulaşan mu mücadelelerin belki de politik olarak önemi uluslararası kamuoyunca sonuçlarının tanınması olarak ifade edilebilir. Tanım itibariyle savaş olarak adlandırılamayan bu yeni silahlı mücadele türü; kısıtlı savaş, gerilla savaşı, ayaklanma ile mücadele, gibi çeşitli isimlerle anılmakla birlikte, genel kabul görmüş terim olarak **düşük yoğunluklu çatışma** terimi tercih edilmektedir. Bu dönemde, konvansiyonel olmayan teknikler uygulayan hasımla silahlı mücadelede devletler, kendi ülkesinde veya kendi ülkesi dışında klasik anlayışla konvansiyonel mücadeleden sonuç alamadıkları, gerilla

[14] Creveld, a.g.e, 57-62

taktik ve teknikleri kullanan düşman ile benzer teknikleri kullanarak küçük birlik harekâtı ile mücadele etmeye çalışan özel birliklerini ön plana çıkartmışlardır. Klasik ordular içerisinde alışılmamış taktik-teknikler ile birlikte, yeni nesil silah, teçhizat ve teknolojiler ile prosedürlerin harekât alanına girmesine öncülük eden bu özel birliklerin desteklenmesi için ise, klasik askerî yetenekler yetersiz kalmış, ihtiyaç duyulan bu desteğin özel şirketlerden karşılanmaya başlanması savaş gibi devlet tekelinde olan bir alanda özelleşmenin yolunu açmıştır.

Ekonomik nedenler başta olmak üzere devlet kurumlarının gelişen teknolojiye adapte olmada hantal kalmasının da etkisi ile bu dönemde kimi devletsel fonksiyonların özel sektöre devredildiği gözlenmiştir. Bu dönemde, sivil şirketlerin askerî alana da nüfuz ettiği görülmeye başlanmıştır. 20'nci yüzyılın ikinci yarısından itibaren başlayan bu durum, özel askerî şirketler ile birlikte güvenliğin ve istihbaratın özelleşmesinin de başlangıcı olmuştur. Batılı toplumlarda tasarruf, daha hızlı ve etkin hizmete erişim vazgeçilmez bir savunma siyasası haline gelmiştir. Bu bağlamda silahlı kuvvetlerin küçültülerek tasarruf sağlanması için özelleşme ve dışarıdan temin önemli bir araç olarak kabul edilmekle birlikte, olumsuz tarafları da eleştirilmektedir.[15]

1989'da **Sovyetler Birliğinin (SSCB) dağılması ve Soğuk Savaş döneminin sona ermesi ile**, eski imparatorlukların yerini almış olan merkezi ideoloji çevresinde federatif yapılanma çözülmeye başlamış, bu çözülme ile pek çok doğu bloğu ülkesinde siyaseten bastırılmış gruplar arasında rekabet yaşanmaya başlamıştır.[16] Bu çözülme ve mevcut siyasi otoriteyi himaye eden süper gücün ortadan kalkmasını, ülkelerin çok daha az karşı karşıya geldikleri, daha çok devlet dışı aktörlerin terörizm ve bölgesel çatışmaların ön plana çıktığı düşük yoğunluklu çatışmaların yaşandığı bir süreç takip etmiştir. SSCB'nin dağılması ile oluşan kaos ve otorite boşluğunun suistimali ile normalde silahlı kuvvetler envanterinde bulunan harp silah, araç ve gereçlerin devlet dışı silahlı yapılanmaların eline geçmesine ve bunların tarihte daha önce rastlanmayan yeteneklere sahip olmalarına olanak sağlamıştır. Bu durum, güç kullanma konusunda bu yeni aktörlerin devletlere alternatif olarak çatışma alanlarındaki ağırlıklarının

[15] Minow, Martha. "Outsourcing Power: Privatizing Military Efforts and the Risks to Accountability, Professionalism, and Democracy." In *Government by Contract: Outsourcing and American Democracy*, ed. Jody Freeman, Martha Minow (Cambridge,MA: Harvard University Press, 2009), 125-127. https://doi.org/10.2307/j.ctv22jnrsb.9. [Erişim Tarihi: 15.05.2022].

[16] Erhan Büyükakıncı, "Yeni Savaşlardan Savaşın Dönüşümüne: Uluslararası Sistem ve Aktörlerde Değişimin Sürekliliği", *Savaşın Dönüşümü; Yeni Dinamikler, Aktörler ve Araçlar,* der. Erhan Büyükakıncı, (Ankara: Adres Yayınları, 2021), 39.

artmasına yardımcı olmuştur.[17] Bu dönemde sadece mücadele eden iki tarafın da devlet olduğu sadece on savaşın yaşanması, devletlerin birbirleri ile olan sorunlarını savaştan başka yöntemlerle çözme, bir diğeri üzerinde politikalarını dikte etmek için daha farklı yöntemleri tercih etmeye başladıklarını göstermektedir. Artık çatışmalarda en az bir taraf devlet dışı hal almış, mutemet kuvvetler de dahil olmak üzere çatışmaların aktörlerinde çeşitlilik artmış, ulusal çıkarları için devletler birbirleri ile farklı aktör ve vasıtalar ile farklı harekât ortamlarında karşı karşıya gelmeye başlamışlardır. 1991 yılını Soğuk Savaş döneminin sonu olarak kabul edecek olursak, 2021 yılına kadar geçen 30 yılda iki devletin karşı karşıya geldiği 11 savaş gerçekleşmiştir.[18] Devletler arası savaşlar azalırken, iç savaşlar ve çatışmaların artış gösterdiği gözlenmektedir. Bu bağlamda günümüzde devletler arası savaşların istisnai bir hal aldığını, çatışmaların taraflarından en az birini devlet dışı aktörlerin oluşturduğu söylenebilir.

Tüm bu anlayış değişimi ile; teknolojik gelişmeler, ekonomik kısıtlamalar ve ABD başta olmak üzere lider ülkelerin her alanda özelleşmeye yönelik politikaları doğrultusunda 1991 Körfez Savaşında tarihte hiç rastlanmadığı ölçüde özel sektöre bağımlığı ve karar vericilerin (askerî istihbarat da dahil olmak üzere) kimi askerî alanlarda özelleşmenin kaçınılmaz olduğu görüşünde oldukları gözlenmiştir.[19] Özellikle 11 Eylül 2001 saldırılarını takip eden, terörizm çağı olarak da tanımlanan dönemde asimetrik savaş stratejileri ön plana çıkarken, güvenlik politikaları soğuk savaş dönemi caydırıcılığından, terörizm çağının güvenlik politikası olan 'önleme'ye dönüşmüştür. Ülke sınırlarını aşan ve küresel bir tehdit halini alan terörizm döneme damgasını vurmuş ve bu dönemde silahlı çatışmaların çoğunluğunu oluşturmuştur. Bölgesel değil, küresel bir tehdit halini alan terörizmle çokuluslu bir mücadele ve eşgüdüm sağlamak üzere ABD öncülüğünde "Küresel Teröre Karşı Savaş" ilan edilmiştir. Her ne kadar bu dönemde küreselleşen teröre karşı verilen mücadele "Terörle Savaş" olarak lanse edilmiş olsa da bu tanımın terörist örgütlere bir politik statü, belki de ulaşmayı amaçladıkları meşruluğu kazandıracağı nedeniyle

[17] Mary Kaldor, *New and Old Wars: Organized Violence in a Global Era*. (Stanford: Stanford University Press, 2006) 4.
[18] Heidelberg Institute for International Conflict Research, *Conflict Barometer Reports*. (Heiderberg, 2020).
[19] Güçyetmez, a.g.m., 82.

eleştirilmektedir.[20] Amerikalı stratejist Luttwak, bu dönemde terörizmle mücadelenin bu derece öne çıkmasının nedenini Sovyetler Birliğinin dağılması sonrasında tek kutuplu hal alan dünyada geçici bir süre için büyük güç mücadelesinin olmayışına bağlamaktadır [21].

Sınırları aşan, bölgeselin ötesine geçmiş terörizme karşı yapılan mücadelelerde tek ülke yerine ülkelerce oluşturulan Koalisyon Kuvvetlerinin oluşturulduğu ve ülkelerin aynı amaç çevresinde kolektif hareket ettiği gözlenmektedir. Bu durum her ne kadar Yalçınkaya tarafından artık savaşların milli çıkarlar doğrultusunda yapılmadığı çıkarımı yapılmış olsa da[22], kolektif mücadele ile birlikte ulusal yapılara rastlanması[23], ortak bir düşmana karşı yapılan mücadelede iş birliğinin yanında ulusal kaygı ve farklı çıkarların da olduğunu göstermektedir. Ülkelerin aynı tehdide farklı yaklaşımları, bölgesel veya yöntemsel olarak ortak hareketten ayrışan uygulamaları, ulusal politikaların hâlâ güç kullanımda etkin olduğunun ispatı olarak karşımıza çıkmaktadır. Burada dikkatten kaçırılmaması gereken bir husus ise kolektif hareket etmenin yapılan silahlı müdahalelerin meşruiyetini artırmak için başvurulan bir yöntem olarak kullanıldığıdır.

Düşük yoğunluklu çatışmaların konvansiyonel savaşın yerini alması ile bu yeni tip tehditler ile mücadelede ülkeler daha hafif, küçük ve esnek silahlı kuvvetler yapılanmasına ihtiyaç duymuşlardır. Batılı ülkelerin küresel terörizmle mücadelesi sürerken güçlenen ve uluslararası arenada giderek etkisini artıran Rusya Federasyonu ve Çin Halk Cumhuriyeti, ABD'nin düzensiz savaş (Irregular Warfare) stratejisi gibi devlet dışı aktörlerin, vekil unsurların, tüm devlet kurumları ve çatışma ortamına dolaylı veya direkt olarak etki edecek tüm milli güç unsurlarını ulusal menfaatleri doğrultusunda kullandıkları yeni strateji ve metotlar geliştirmiştir. Kaldor'un da belirttiği gibi; bu, aslında yeni olmayan, savaş tarihi boyunca pek çok kez baş vurulmuş yöntemlerin günümüze adaptasyonu ile geliştirilmiş 'yeni savaş', devletler aslında o kadar da yeni değildir.

---

[20] Mary Kaldor, "Old Wars, Cold Wars, New Wars, and the War on Terror", International Politics, Volume 42, 2005, 498.

[21] Edward N. Luttwak, "A Brief Note on 'Fourth-Generation Warfare", *Contemporary Security Policy*, C. 26, S. 2 (2005): 227. https://doi.org/10.1080/13523260500211009 [Erişim Tarihi: 15.05.2022]

[22] Haldun Yalçınkaya, "Savaşın Değişimi ve Savaş Çalışmalarında Farklı Disiplinler", *Savaş: Farklı Disiplinlerde Yeni Yaklaşımlar*, der. Haldun Yalçınkaya (Ankara: Siyasal Yayın-Dağıtım, 2010), 22.

[23] Afganistan'da uluslararası ISAF harekâtının yanında ABD'nin tamamen ulusal komutanlığı çatısı altında yürüttüğü ayrı bir terörle mücadele harekâtı ve Suriye'de DEAŞ'a karşı mücadelede oluşturulan Koalisyonun yanında ülkelerin milli olarak da yürüttükleri harekâtlar örnek olarak gösterilebilir.

Günümüzün yeni savaşını farklı kılan; bu çatışmalarda devletlerin karşı karşıya gelmeyerek, kendi politikalarını diğerlerine kabul ettirmek ve bir bölgede hakimiyet kurmak için uluslararası bağlantıları olan devlet ya da devlet dışı ağları, kompleks legal veya illegal organizasyonları, diasporalar, şirketler, paralı askerler, gönüllüler, hükumet dışı organizasyonlar, dini veya etnik gruplar, uluslararası organizasyonlar gibi küresel aktörlerin rol almalarıdır.[24] Bu devlet dışı aktörler silahlı olabildikleri gibi sadece askerî değil, diğer fonksiyon alanlarında etkinlik göstererek harekât alanına tesir edebilecek sivil gurupları da içerebilmektedir.

Münkler ise bu yeni savaşın pek çok açıdan aslında yeni olduğunu savunmaktadır. Bu kapsamda söylemini; devletlerin artık baskın aktörler olmaktan çıktığına, stratejinin kesin sonuçlu muharebe ile bir an önce galip gelmekten düşmanı tüketerek pes ettirmeye doğru kaydığına, sivillerin artık asıl hedefi oluşturduğu üzerinde durarak savaşın icrasına yönelik normların değişime uğradığına, katliamlara varan aşırı şiddetin artık olağanlaştığına dayandırmaktadır. Asimetrik çatışmaların devletler arasındaki savaşların önüne geçtiğini ve yirmi birinci yüzyılı bu yeni çatışma anlayışının şekillendireceği çıkarımında bulunmaktadır.[25] Yeni savaşlar konusundaki argümanını da 1. Savaşların özelleşmesi, 2. Ticarileşmesi ve 3. Asimetrikleşmesi kriterleri üzerinden savunmakta; devlet dışı aktörlerin artması neticesinde devletlerin savaş çıkarma tekelini kaybetmeleri, yani savaşın özelleşmesi, ekonomik kaygı ve hedeflerin savaşların sebebini oluşturma konusunda etkisinin artması ve savaşların düzensizleşmesi neticesinde risk faktörlerinin tahmininin güçleşerek çatışma ortamının karmaşık ve çok katmanlı hal alması gibi dönüşümlere dikkat çekerek açıklamaya çalışmaktadır.[26]

Yeni savaşlar üzerine çalışmaları incelerken, dördüncü nesil savaşlar olarak literatüre katkı sağlayan William Lind'in yaklaşımının da değerlendirilmesi gerekir. Lind, kronolojik bir inceleme içerisinde nesillere ayırdığı savaşın değişimi kapsamında günümüz çatışma ortamını tanımladığı 4'üncü nesil savaş kavramında geleneksel savaş stratejilerinin yetersiz kaldığını ve bu evrim sürecinde belirleyici etkenin ise teknoloji olduğunu öne sürmektedir. Bu yeni nesil güç çekişmesinde savaş ile barış arasındaki kesin çizginin bulanıklaştığını, mücadelenin belirli bir alanın dışına

[24] Kaldor, a.g.m., 499-501.
[25] Herfried Münkler, *The New Wars* (Oxford: Polity Press, 2004), 135.
[26] Herfried Münkler, *İmparatorluklar: Eski Roma'dan ABD'ye Dünya Egemenliğinin Mantığı* (İstanbul: İletişim Yayınları, 2009), 220-227.

taştığını, çatışan taraflara askerlerin yanında sivillerin de dahil olduğunu, asimetrik özellik taşıyan askerî, yarı askerî veya sivil gayretlerin günümüz çatışmalarının ana unsurlarını oluşturduğunu ileri sürmektedir.

Klasik anlayışta devlet tekelinde olan şiddet, teknolojik gelişmelerin de etkisiyle devletin kontrolünden devlet dışı aktörlerin ilgi alanına doğru kayma göstermiştir. Bu bağlamda devlet otoritesine karşı ayaklanan gruplardan suç örgütlerine, dini yapılanmalardan terör örgütlerine çeşitli gruplar kendi otoritelerini kurdukları bölgelerde beka ve yapılanma stratejileri oluşturarak küresel güvenliği tehdit etmeye başlamışlardır. Bu yapılanmaların etkisi ile, karşıt birey ve gruplar da güvenlik endişeleri ile savunma mekanizmaları oluşturma gayretleri içine girmiş, bu da bireysel silahlanma ve başka devlet dışı silahlı yapılanmaların oluşumunu ortaya çıkartmıştır. Güvenlik sağlama yeni bir endüstri halini almış, özel şirketlerin güvenlik pazarında yaygınlaşmaları ile ticari, hukuki ve beşerî alanda güvenlik farklı boyut kazanmaya başlamıştır.[27]

Savaşın taraflarını "… devlet veya devler grubunun diğer bir devlet veya devletler grubuna karşı …" ifadesi ile tanımlayan Clausewitz'ci bakış açısı ile günümüzdeki savaşın geçmişteki savaşlarla bir tutulması, günümüzün gerçeklerinin ve tehditlerinin üstesinden gelmemizi engelleyecektir. Uygulanan teknikler her ne kadar savaş tarihinde ilk olmasalar da günümüz çatışma ortamının, uygulanan metot ve stratejilerin 2'nci Dünya Savaşı, Soğuk Savaş veya Teröre Karşı Savaşa nazaran çok farlı olması 'yeni savaş' olarak tanımlanmasını sağlamaktadır.[28] Savaşı yeni yapanın; güç mücadelesine dahil olan yeni aktörler, ekonomik rekabetin çatışmanın ana nedenleri arasında yer alması ve kullanılan araçların asimetrik kullanımı neticesinde mücadelenin karmaşıklaşması olarak gösterilmektedir. Bu karmaşıklık ile etkilenen sivillerin sayısı artmış, yerinden edilenler ile mülteciler yerel bir sorun olmanın ötesine geçerek küresel bir problem halini almış, çatışan taraflar arasında asker sivil ayrımının güçleşmesi yanında yer yer kadın ve çocukların da dahil olduğu görülmeye başlanmış, suç örgütleri, isyancı milisler ve savaş beyleri gibi devletlere alternatif silahlı unsurlar gözlenmeye başlanmıştır.[29]

---

[27] William S. Lind, "Understanding Fourth Generation War." *Military Review*, 2014, https://www.hsdl.org/?view&did=482203 [Erişim Tarihi: 15.05.2022].
[28] Kaldor, a.g.m., 498
[29] Büyükakıncı, a.g.e., 27-29.

Özetlemek gerekirse; soğuk savaş sorasında ülkelerin karşı karşıya gelmekten kaçınmaları ve bu güç mücadelesini farklı coğrafyalarda farklı aktörler üzerinden farklı silahlı müdahale gerekçeleri ile gerçekleştirmeleri, silahlı kuvvetlerde küçülme, düşük yoğunluklu çatışmalardaki artış, silah ve istihbarat toplama vasıtalarındaki teknolojik gelişmeler, bilgi teknolojilerinin giderek daha önemli hale gelmesi, siber ortamın bu mücadelelerde kullanımının artması gibi nedenlerle özel şirketlerin özellikle 2003 Irak savaşından itibaren harekât alanındaki varlığının ve etkinliğinin arttığı ifade edilmektedir.[30] İncelediğimiz birkaç yüzyıllık dönemde sosyal, kültürel, politik, endüstriyel ve teknolojik gelişmelerin etkisi ile savaşın tarafları, emelleri, stratejileri ve belki de en önemlisi icra ediliş şeklinin önemli ölçüde değişmiş olduğunu görmekteyiz. Önceden sadece devletler arasında bir hükümranlık mücadelesi olan savaşa devlet dışı aktörler de zaman içinde dahil olmuşlardır.

Güçyetmez'in İngiltere'nin 19'uncu yüzyıl başlarında yaptığı gibi günümüzde ABD'nin hegemonyası ile uluslararası sistemde güç kullanımını yeniden yapılandırma, yönetme, Vestfelya sisteminin prensip ve normlarını yeniden uluşturma gayreti içinde olduğu görüşüne[31] Rusya ve Çin'in de bu bağlamdaki yaklaşımlarını eklemek konuya çok yönlü bakmak adına yerinde olacaktır. 1999 Irak Savaşı ile gündeme gelen ve konvansiyonel kuvvetlerin müşterek birleşik/harekâtını mümkün kılan ağ tabanlı harekâtın, terör saldırıları sonrasında ABD'nin Afganistan'ı işgali ardından gündeme gelen asimetrik savaş anlayışına, 2003'te başlayan Irak savaşı, Kırım'ın ilhakı, devamında Suriye iç savaşı ile vekalet savaşları stratejisini de kapsayacak şekilde genel kabul görmüş adı ile Hibrit savaşa dönüştüğü söylenebilir. Bununla birlikte büyük güç yarışı[32] içinde Çin'in uyguladığı gri alan faaliyetlerini kapsayan Kısıtsız Savaş (Unrestricted Warfare) doktrinin uluslararası ortamda ulusal politika hedeflerine ulaşılmak üzere kullanıldığı gözlenmektedir.

Tarih boyunca uluslar arasında ilişki savaş ve diplomasi olmak üzere iki temel kavram üzerinden yürümüştür. Ülkelerin ulusal çıkarlarının barışçıl bir yaklaşımla sağlanması

---

[30] Deborah Denise Avant, *The Market for Force The Consequences of Privatizing Security* (New York: Cambridge University Press, 2005), 9.
[31] Güçyetmez, a.g.m, 80.
[32] Büyük Güç Yarışı (Great Power Competition); Çin'in yükselişi, Rusya'nın tekrar gücünü toparlaması ver ABD'nin göreceli olarak düşüşte olması algısına dayalı küresel politik bir yaklaşımı ifade eder. Jonathan M. DiCicco, Tudor A. Onea, *Great Power Competition* (Londra: International Studies and Oxford University Press, 2023, https://oxfordre.com/internationalstudies/display/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-756 [Erişim Tarihi 23.08.2023].

olarak tanımlanan diplomasi tıkandığında anlaşmazlıkların güç kullanarak, savaş yoluyla çözümü yoluna gidilmiştir. Topyekûn savaşın yıkımı ve nükleer silahların gücünün dünyada hayatı sonlandıracak kudrete erişmelerinden duyulan kaygılar ülkeleri savaştan uzaklaştırsa da ulusal politikalar doğrultusunda diğer ülkeler üzerinde baskı unsuru oluşturmaya yönelik ihtiras son bulmamıştır. İkinci Dünya Savaşından sonra barışın sürdürülmesine yönelik güç kullanımına koyulan kısıtlamalar ile diplomasiye alternatif çözüm yolunun değiştiği ve dönüştüğü gözlenmektedir. Günümüzde politik hedefleri desteklemek üzere kuvvetli bir silahlı kuvvetler ile caydırıcılığın sağlanmasıyla beraber, problem sahalarına müdahalenin mecburiyet ve meşruiyetinin uluslararası kamuoyuna ispatlanması ve sunulan gerekçelerin kabul görmesi hiç olmadığı kadar önem kazanmıştır. Bu bağlamda savaş ile diplomasi arasında gri bir bölge oluşmuş, bu belirsiz alanda BM antlaşması ile güç kullanımına koyulan kısıtların etrafından dolaşmaya yönelik uygulamalar hayata geçirilerek günümüz güç mücadelelerini şekillendirmiştir.

2.2. Kavramsal Çerçeve

Hibrit savaş terimi ilk olarak Hoffman tarafından "Suç ve terörizm unsurları ile, konvansiyonel ve konvansiyonel olmayan kuvvetlerin sinerji yaratacak şekilde birlikte kullanılması" olarak tanımlanmıştır.[33] Ayrıca başka bir eserinde; emekli bir asker olan McCuen'in asimetrik bir savaş olan hibrit savaşın; çatışma alanında yaşayan halk, uluslararası toplum ve savaş uygulayan ülkede yaşayan halk olmak üzere üç insan grubu arasındaki bir mücadele olduğu ve hibrit savaşın odak noktasının bu üç insan grubunun algısı üzerinde yöneltilmiş modern bilgi teknolojilerinin kullanımını içerdiği tespitine yer vermiştir.[34] Hoffman'ın yaklaşımı; daha önceden farklı karakteristiklere sahip olan farklı harekât çeşitlerinin birlikte ve diğer bileşenleri ile daha bulanık bir şekilde icrası[35] olarak özetlenebilecek olsa da, savaşın dönüşümü konusunda bahsedilen Çin'in sınırsız savaş konsepti, Lind'in dördüncü nesil savaş teorisi, konvansiyonel ve düzensiz silahlı unsurların savaşta birlikte kullanımını tanımlayan bütünleşik savaş (Compound Warfare) ve ABD Savunma Bakanlığının; 21'inci yüzyılın konvansiyonel olmayan tehditlerle mücadele ve stratejik belirsizliği ile

[33] Hoffman, a.g.m., 29.
[34] Frank G. Hoffman, "Hybrid Warfare and Challenges." *Joint Forces Quarterly*, S. 52 (2009): 275, https://apps.dtic.mil/sti/pdfs/ADA516871.pdf [Erişim Tarihi: 15.05.2022].
[35] Frank G. Hoffman, "'Hybrid Threats': Neither Omnipotent nor Unbeatable" *Orbis*, C. 54, S. 3 (2010): 443, https://doi.org/10.1016/j.orbis.2010.04.009 [Erişim Tarihi: 15.05.2022].

mücadele etmek üzere Savunma Bakanı Donald Rumsfeld tarafından kaleme alınan 2005 tarihli Ulusal Savunma Stratejisini[36] bir potada eriten bir bakış açısını yansıttığı söylenebilir.[37]

Sinerjik etki yaratmak üzere taktik ve operasyonel askerî faaliyetlerin koordine ve yönetilmesi odaklı incelediği hibrit tehditleri konvansiyonel silahlar ile düzensiz taktikleri, terörizmi ve suç unsuru içeren faaliyetleri siyasi hedefe ulaşmak üzere harekât alanında eş zamanlı (senkronize) ve çatışma ortamının şartlarına uygun şekilde uygulayan hasım olarak tanımlamaktadır.[38] Bu taktik ve operatif seviye, yani daha icraya yönelik yorumlaması ile stratejik seviyede uygulamaları içeren Çin'in Sınırsız Savaş konseptinden hibrit tehditleri, dolayısıyla hibrit savaşı ayırmaktadır.[39]

Hoffman ayrıca hibrit savaşı da konvansiyonel yetenekleri, düzensiz taktik ve formasyonları kapsayan farklı savaş türlerini, ayrım gözetmeyen şiddet ve baskıyı da kapsayan terörist faaliyetleri ve suç örgütlerinin faaliyetleri bütünleştiren silahlı mücadele ile eşgüdüm içinde yürütülen dikkatlice planlanıp sosyal ağları kullanarak icra edilen bilgi harekâtı ile toplum algısının yönetilmesi neticesinde istikrarsızlaşma faaliyetleri, en baştan itibaren direkt çabaları destekleyen stratejik seviyede yürütülen ekonomik, enerji, dış politika yaptırımları ve tümünü destekleyen siber gayretlerin bütünü olarak tanımlamaktadır.[40] Toplum algısı üzerine yürütülen bilgi harekâtı ile özellikle hassasiyet içeren grupların manipülasyonu ile yönetime karşı gösteri ve toplumsal olaylar teşvik edilirken hükumetin yıpratılması hedeflenmekte, toplumsal olayların şiddetinin artırılması ile hedef devletçe alınan tedbirlerin sertleşmesi sağlanarak ve sosyal medya üzerinden uygulanan şiddetin paylaşılması ile uluslararası kamuoyu nezdinde hedef ülke hükumeti üzerinde baskı oluşturulmaktadır. Burada hedeflenenlerden biri mevcut mücadele edilen hedef ülke hükumetinin düşürülmesi ve yerine yandaş kukla hükumetin getirilmesi ve dolaylı olarak yönetimin kontrol altına alınması iken, bunun gerçekleşmemesi durumunda yaratılan uluslararası algı ve kendisine yandaş (çoğu örnekte hasım ülkede yaşayan çift vatandaşlık sahibi ya da çift

[36] Donald Rumsfeld, *The National Defense Strategy of the United States of America*. Washington DC: 2005, V.
[37] Ofer Fridman, *Russian Hybrid Warfare: Resurgence and Politicization* (Londra: Oxford University Press, 2018), 82.
[38] Frank, G. Hoffmann, *Conflict in the 21st Century: Rise of Hybrid Wars* (Arlington: Virginia, 2007), 14.
[39] Fridman, a.g.e., 84.
[40] Hoffman, a.g.m., 2010, 444.

vatandaş yapılmış kendi ulusu kökenli halk) topluma karşı uygulanan şiddet bahane edilerek silahlı müdahalenin meşrulaştırılması gayreti olarak ifade edilmektedir [41].

Hibrit savaş konusunda pek çok akademisyen Hoffman'ın çalışmalarına sıklıkla değinmiş, bir çıkış, referans noktası olarak faydalanmış ve kendi bakış açıları ile yorumlamış, farklı faktörlerin günümüz güç mücadelesine etkilerini değerlendirmişlerdir. McCulloh ve Johnson da Müşterek Özel Harekât Üniversitesi (Joint Special Operations University – JSAU) bünyesinde yaptıkları çalışmada; konvansiyonel ağırlıklı hasma karşı spesifik ve sinerjik bir etki yaratmak üzere konvansiyonel ve konvansiyonel olmayan unsurların birlikte kullanımına sahip olunan kültürün getirdiği etkiyi de dâhil etmişlerdir.[42] Güncel bir tanımlamada ise Tokmakoğlu hibrit savaşı stratejik bir yaklaşımla; "Bir devletin veya gücün, yüksek çıkarlarını geliştirmek amacıyla, politik, askerî, diplomatik, ekonomik ve teknolojik araçları bir araya getirerek, belli coğrafyalarda her türlü yolu izleyerek, uzun süreli uygulayacağı kasıtlı çabalarını içeren plan ve politikaların bütünüdür." şeklinde ifade etmektedir.[43] Amacı bir bölgeyi ele geçirmekten öte, hedef ülkenin savaşma azim ve iradesini yok etmek üzere hibrit savaşta gayretler askerî hedeflerin yanında sivil altyapıyı da hedef alarak politik hedefini kabul ettirmek, kabul etmeye mecbur bırakmaktır.[44] Caşın ise hibrit savaşı; savaş ve barış durumları arasındaki belirleyici unsurları bulanıklaştırma / belirsizleştirme üzerinden, alışılagelmiş konvansiyonel savaş metotlarına ek olarak farklı harekât nevilerinin ve sistemlerinin eşzamanlı uygulanmasını kapsayan bir silahlı mücadele türü ve stratejisi olarak tanımlamıştır.[45]

Evrensel olarak üzerinde mutabakat sağlanmış bir tanımı olmasa da[46], akademisyenlerin yanında, askerî doktrin ve siyasa yazını ilk bahsedilmeye başlandığı yıllardan itibaren hibrit savaş kavramını tanımlamaya çalışmıştır. Zamanın ABD Genelkurmay Başkanı Org. Casey 2008 yılında, Hoffman'ın tanımını anımsatacak

[41] Hoffman, a.g.e., 2007, 29-30.
[42] Timothy McCulloh, Richard Johnson. *Hybrid Warfare-JSOU Report 13-4*, (McDill AFB: Joint Special Operations University, 2013), 17, https://jsou.libguides.com/ld.php?content_id=2876897 [Erişim Tarihi: 19.04.2022].
[43] Gürsel Tokmakoğlu, "Hibrit Savaş", 2021 https://politikmerkez.com/konular/guvenlik/hibrit-savas/ [Erişim Tarihi: 06.05.2023].
[44] Salih Bıçakcı, "Hibrit Savaş.", Uluslararası İlişkiler Konseyi Güvenlik Yazıları Serisi 33(8), Kasım 2019, s.3. https://doi.org/10.13140/RG.2.2.32236.10883 (Erişim Tarihi: 16.01.2023)
[45] Mesut Hakkı Caşın, "Modern Harbin Doğasında Değişim Modeli Olarak Hibrit Savaş", *Savaşın Dönüşümü: Yeni Dinamikler, Aktörler ve Araçlar*, der. Erhan Büyükakıncı (Ankara: Adres Yayınları, 2021) 208.
[46] David McFarland, *Understanding Hybrid Warfare: Navigating the Smoke and Mirrors of International Security*, (Las Vegas: David McFarland, 2021), 8-9.

şekilde hibrit savaşı konvansiyonel, düzensiz, terörist ve suç örgütleri faaliyetlerinin politik hedeflere ulaşılmak üzere dinamik bir şekilde birlikte kullanılması olarak tanımlamıştır.[47] ABD Kara Kuvvetleri ise hibrit savaşı 3 yıl sonra; düzenli ve düzensiz kuvvetler, suç örgütleri veya bu kuvvetlerin etki oluşturmak üzere kombine bir şekilde ortak bir çıkar elde etmek üzere çeşitli ve dinamik bir şekilde birlikte faaliyet göstermeleri olarak doktrininde dahil etmiştir. İngilizler ise; hibrit savaşı bir nevi düzensiz savaş olarak görmekte ve asimetrik taktikleri uygulayan düzensiz veya gerilla kuvvetlerinin harekâtından çok da farklı bir tanımlama yapmayarak Hoffman'ın görüşü doğrultusunda tanım geliştiren ABD'li müttefiklerinden kavramsal olarak ayrışmaktadırlar. Hibrit savaşı, genellikle düzenli ordular tarafından kullanılan sofistike silahlar ve sistemleri kullanan düzensiz kuvvetler tarafından icra edilen, şartlar ve kaynaklara göre biçimlenebilen ve uyum sağlayan uygulamalar olarak tanımlamaktadır. İsrail askerî teorisyenleri ise daha farklı bir yaklaşım ile hibrit savaşı sosyal kısıtlamalardan etkilenmeyen sosyal bir savaş metodu olarak tanımlamaktadır. Hibrit savaşın, konvansiyonel teknolojiler ve konvansiyonel olmayan taktik ve uygulamaların birlikte kullanımının sağladığı fiziksel üstünlüğün yanında, konvansiyonel bir devlet gücünün tabi olduğu Cenevre Sözleşmesi, Harp Hukuku ve angajman kuralları gibi hukuki ve sosyal sınırlılıklara tabi olmayarak kavramsal bir üstünlük de sağladığı tespitinde bulunmaktadır. Bu çifte avantaj ile, toplum algısını şekillendirmede sosyal ağları kullanarak daha çevik ve etkin olabildiğini ileri sürmektedir. İsrail bakış açısı, hibrit tehditlere daha etki odaklı anlayışı ile, kavrama fonksiyon odaklı bakan ABD anlayışından farklılık göstermektedir.[48]

NATO tarafından ilk olarak 2014 Galler Zirvesi sonuç bildirgesinde "Açık ve örtülü askerî, paramiliter ve sivil tedbirlerin/yöntemlerin oldukça entegre bir şekilde uygulanması" olarak tanımlanmıştır. Tanımlanmaya çalışılan yeni nesil savaşın metotlarını oluşturan; siber savaş, küresel terörizm, korsanlık/deniz haydutluğu, asimetrik çatışmalar, bunlarla sınırlı kalmamak üzere, Hibrit Tehditler olarak tanımlanmaktadır. [49]

---

[47] George W. Casey, "America's Army In an Era Of Persistent Conflict", *Army Journal* C. 58, S. 1 (2008): 24. https://www.ausa.org/sites/default/files/Casey_1008.pdf [Erişim Tarihi: 16.01.2023].

[48] Timothy B. McCulloh, *The Inadequacy of Definition and the Utility of a Theory of Hybrid Conflict: Is the 'Hybrid Threat' New?*, (Fort Leavenworth/Ka: 2012), 14-15, https://www.hsdl.org/?view&did=758318 [Erişim Tarihi: 19.04.2022]. Görüş, atıf yapılan eserin yazarının İsrail Savunma Güçlerinden emekli generallerle ve İsrail askerî teorisyenlerle Tel Aviv'de Mart 2012'de yaptığı mülakatlara dayanmaktadır.

[49] North Atlantic Council, *Wales Summit Declaration* (Cardiff, 2014), 13.

İlk tanımlanmaya başlandığı tarihlerden sonraki gelişmeleri ve uygulamaları da çalışmalarına dâhil ederek hibrit harekât konseptini anlama ve mücadele yöntemleri bulmayı amaçlayan daha güncel ve kapsamlı bir proje olarak karşımıza çıkan Çokuluslu Yetenek Geliştirme Merkezi (MCDC)[50] Hibrit Tehditlerle Mücadele Projesi hibrit harekâtın batılı perspektiften tanımını; "Askerî, politik, ekonomik, sivil ve bilgi gibi güç enstrümanlarının askerî alanın çok ötesinde sosyal fonksiyonlar yelpazesinin tamamındaki hassasiyetler üzerinde senkronizasyon ile sinerjik etkiler yaratacak şekilde kullanılması" olarak yapmaktadır. Bu tanıma kullanılan enstrümanların derinliğini etki ettikleri ortamların çeşitliliğine de dikkat çekmek adına 'çok tabanlı (multi domain)' ifadesini de biz ekleyebiliriz. Bahse konu raporda Cullen ve Kjennerud ayrıca bu faaliyetlerin seviye ve ağırlıklarının, birlikte veya ardışık icrasının elde edilmek istenen etki ve uluslararası kamuoyunun tepkisine göre artırılıp azaltılabileceğini belirtmektedir. Bu çok tabanlı ve değişik seviyelerde eşgüdüm içinde uygulanan enstrümanlar, uygulayan aktörün yetenekleri, hasmın suiistimal edilecek hassasiyetleri, ulaşılmak istenen politik hedefler ve bu hedeflere ulaşmak için uygulanacak yönteme göre şekillenebilmektedir.[51]

Hirbrit savaş stratejisi, hasım ülkenin karşılık vermesine imkân tanıyacak bir eşiğin altında uygulanan faaliyetler yolu ile icrayı esas almaktadır. Burada hukuki ve siyasi eşiklerin birbirinden farklı özellikler göstermesi, hukuk fonksiyon alanını da değerlendirilmesi gereken bir husus olarak ortaya çıkartmaktadır.[52]

2.3. Uluslararası Hukukta Savaş'ın Yeri

Birleşmiş Milletler Antlaşması, barışı korumak adına güç kullanımı ve güç kullanma tehdidini 51'inci maddesinde açıklanan iki istisnai durum dışında yasaklamıştır. Bu iki istisnai durumun ilki Birleşmiş Milletler Güvenlik Konseyi'nin belli bir durumda güç kullanımına karar vermesi ve ikincisi ise bir ülkenin öz savunma maksadı ile güç kullanımıdır. Aslında 51'inci madde öz savunma hakkını genel uluslararası hukuktan almaktadır. Silahlı saldırı durumunda geçerli olacak öz savunma hakkından bahsedilirken, antlaşma öz savunmanın kapsamını açıklamadığı gibi, kendisine

[50] Multinational Capability Development Campaign (MCDC).
[51] Patrick J. Cullen, Erik Reichborn-Kjennerud, Understanding Hybrid Warfare, (Oslo: Norwegian Institute of International Affairs, 2017), 8-9. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf [Erişim Tarihi: 16.01.2023].
[52] McFarland, a.g.e., 10.

yöneltilmiş silahlı saldırının kapsamını, ölçüsünü veya şeklini de tanımlamamıştır. Pek çok açıdan net bir tanıma bağlanmamış olan 'silahlı saldırı' ve 'öz savunma hakkı' kavramları barışın sürdürülmesine yönelik önemli bir alanda tartışmalı, farklı bakış açılarına ve yorumlamalara imkân tanıyan bir durum oluşturmuştur.

Ulusların birbirleri ile güç kullanımı dışındaki dostane ilişkilerinin ve iş birliğinin çerçevesini ise Birleşmiş Milletler Genel Kurulu'nun 24 Ekim 1970 tarihli "Devletler arasında dostane ilişkiler ve iş birliği prensipleri üzerine Uluslararası Hukuk Deklarasyonu" çizmektedir. Bu deklarasyona göre;

> "Hiçbir devlet direkt ya da dolaylı, her ne sebeple olursa olsun diğerinin iç veya dış işlerine karışamaz. … Hiçbir devlet ekonomik, politik veya herhangi bir başka vasıta ile diğerinin bağımsızlığından doğan haklarını kullanmasını engelleyemez ve yahut baskı yapamaz. Bununla birlikte hiçbir devlet diğerinin yönetimini devirmeye yönelik şiddet uygulayan, terörist veya silahlı bir oluşumu organize edemez, bu amaçla ortaya çıkmış böyle bir oluşumu destekleyemez, finanse edemez, yönlendiremez ve faaliyetlerine göz yumamaz. Başka bir ülkede ortaya çıkan bir sivil kalkışmayı destekleyemez." [53]

Genel kurulda kabul edilen bu deklarasyonda üzerinde uzlaşılan prensiplerin, genel kurul kararlarının bağlayıcı olmaması nedeniyle, günümüz güç mücadelelerinde sıklıkla göz ardı edildiği görülmektedir. Görülmektedir ki, devletler uluslararası hukukun belirsizliklerini ve bağlayıcı olmayan kurallarını suiistimal etmektedirler.[54] Kimi zaman hedef ülkedeki soydaşlarının haklarını korumak, kimi zaman hedef ülke hükumetinin otorite boşluğundan faydalanan terör örgütleri ile mücadelede kapasitesiz ya da isteksiz olması neticesinde terörle mücadele sebebiyle, kimi zaman ise hedef ülkenin manipüle edilen hükumetinin daveti üzerine iç karışıklıklara müdahale etmek üzere diğer devletlerin topraklarında güç kullandıkları gözlemlenmektedir. Kimi zaman da Amerikalı askerî stratejist Luttwak'ın savaştan barışa geçişin engelleyicisi olarak gördüğü barışı destekleme harekâtları[55], 2001'de yazdığı görüşlerini haklı çıkartırcasına günümüzde de hedef ülkede istihbarat teşkilatları ve özel kuvvetler

[53] UNGA, *The United Nations General Assembly Resolution 2625, The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States*, (New York: Pub. L. No. Resolution 2625, 1970), https://www.un.org/ruleoflaw/files/3dda1f104.pdf [Erişim Tarihi: 06.05.2023].
[54] McFarland, a.g.e., 73.
[55] Edward N. Luttwak, *Strategy: The Logic of War and Peace* (Londra: The Belknap Press of Harva, 2001), 61.

vasıtasıyla yaratılan iç karışıklık veya ayaklanmayı yatıştırmak üzere hedef ülkeye barış gücü adı altında silahlı kuvvetler ile müdahale etmek için kullanılmaktadır.

2.4. Hibrit Harekât Ortamı ve Hibrit Tehdit

Günümüz çatışma ortamı, konvansiyonel savaş, düzensiz savaşın (hatta zaman zaman terörizm ile) basit ve sofistike teknolojilerin yenilikçi bir anlayışla karışık şekilde uygulanması, âdem-i merkeziyetçi planlama ve icra ile devlet dışı aktörlerin varlığı ile karakterize edilmektedir. Uluslararası bir ortamda hibrit savaş teriminin ilk telaffuz edildiği çalışmasında Hoffman bu evrimleşmiş savaş ortamını; "Devletler veya devlet dışı aktörlerce icra edilebilen bu yöntem ile, harekât alanındaki konvansiyonel unsurlar ile koordine içinde muharebenin fiziki ve psikolojik boyutların etkileyecek şekilde taktik ve operasyonel seviyede sinerji yaratılmaktadır." tespiti ile açıklamaktadır.[56] Hatta Hoffman'ın tanımladığı bu ortam içinde bölgedeki hâkim otoritenin zayıflatılması için suç örgütlerinden dahi istifade edilerek, muhalif unsurlara gerekli kaynaklar sağlanarak iç çatışma ortamı yaratılarak hedef ülkedeki istikrarın bozulması ve müdahaleye meşruiyet kazandırılması söz konusu olabilmektedir.

Adeta günümüz çatışma ortamını tanımlamak için kullanılmaya başlayan 'hibrit harekât' terimi, her ne kadar örneklerine daha önce de rastlanılmış olsa da Rusya Federasyonu Genelkurmay Başkanı V. Gerasimov'un 2013 yılında Rusça yayın yapan Askerî Endüstri Kuryesi Dergisinde yayımlanan makalesi ile batının dikkatini çekmiştir. Gerasimov makalesinde; Rus, politik ve stratejik hedeflerine ulaşmak üzere dış siyasetini destelemede askerî olmayan yöntemlerin silahlı gücün yanında, hatta zaman zaman önünde rol alması gerektiğini vurgulamaktadır. Bahsettiği askerî olmayan metotlara, siyasi hedef doğrultusunda toplumun yönetime baş kaldırma potansiyelini de dahil eden Gerasimov, özel kuvvetlerin kullanımı, bilgi harekâtı, elektronik savaş gibi gizlice sağlanan askerî yöntemlerin de belli safhalarda, tercihen başarının elde edileceği son safhada dâhil edilebileceğini ifade etmektedir.[57]

---

[56] Hoffman, a.g.m., 2007, 8.

[57] Valery Gerasimov, "The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations." *Military Review*, (Washington DC: 2016). https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf [Erişim Tarihi: 15.05.2022]. Atıf yapılan yayın V. Gerasimov'un 2013 yılında yayımlanan makalesinin 2016 yılında yayımlanan tercümesidir. Makalenin 2013 yılında General V.Gerasimov tarafından yazılan orijinali için; (Ценность науки в предвидении**;** Новые вызовы требуют переосмыслить формы и способы ведения боевых действий) https://vpk-news.ru/articles/14632 [Erişim Tarihi: 15.05.2022].

Gerasimov tarafından ortaya atılmış olduğu düşünülen bu doktrin, aslında batılı devletlerin örtülü müdahalelerinin de olduğu iddia edilen Arap Baharı kalkışmaları ile Ukrayna ve Gürcistan gibi Rusya'nın yakın kuşak (Near Abroad) ülkelerindeki renkli toplumsal olayların sentezine dayanmaktadır.[58] Bu husus çoğunlukla batılı taktisyenler tarafından göz ardı edilmektedir.[59]

McFarland, Gerasimov'un günümüzde hayata geçirdiği stratejilerini şekillendirmede tarihten örnekleri analiz ettiği ve bunları günümüze uyarladığını iddia eder.[60] Örneğin; İkinci Dünya Savaşı öncesi 1938'de Nazi Almanya'sı Çekoslovakya'yı işgal için önce Sudentenland bölgesinde yaşayan Alman kökenli halkı ayaklandırmış, Çekoslovak yönetiminin ayaklanmayı bastırmak üzere sert tedbirler alması neticesinde Hitler, Çekoslovak yönetimini terörizm uyguladığı ve Almanca konuşanları infaz ettiğini gerekçe göstererek Çekoslovakya'da yaşayan Alman halkını koruma maksadı ile Sudentenland bölgesini işgal etmiştir. Fransa ve Birleşik Krallık ordularını seferber etse de bu açık askerî hazırlıklar caydırıcılık etkisi yaratmamış, Almanya'nın bu askerî manevrayı "barışçıl nedenlerle icra ettiği" savının uluslararası kamuoyunda kabul bulması (ki baştan beri plan budur) Fransa ve Birleşik Krallık savaş kararı almaktan çekinmiştir. Hiçbir direniş ile karşılaşmadan Çekoslovakya'nın en önemli savunma hattını ele geçiren Almanya bu hamlesinin ardından Çekoslovak hükumetinin değişmesini sağlamış ve Mart 1939'da ülkenin geri kalanında da kontrolü ele geçirmiştir.

Komünist hükumet yönetiminde bir sosyalist özgür ülke olan Çekoslovakya'da 1968'de iktidardaki Komünist Partisinin başına geçen Alexander Dubcek ve hükumetteki bir grup liberal üye, medyada sansürün kaldırılması, ülke dışından radyo yayınlarının serbest bırakılması, ifade özgürlüğü gibi bir takım demokratik reformu hayata geçirmişlerdir. Bu demokratik açılımı sisteme tehdit olarak gören başta Sovyet Rusya olmak üzere Varşova Paktının diğer ülkeleri Çekoslovakya'ya bahse konu demokratik reformların durdurulması yönünde ültimatom vermiş, Mayıs 1968'de bir baskı unsuru olarak sınıra yakın bölgelere asker sevk etmişlerdir. Haziran ayında ise,

[58] Alexander D. Chekov, Anna V. Makarycheva, Anastasia M. Solomentseva, Maxim A. Suchkov ve Andrey A. Sushentsov. "War of the Future: A View from Russia", *Survival*, C. 61, S. 6 (2019): 29, https://doi.org/10.1080/00396338.2019.1688563 [Erişim Tarihi: 16.01.2023].
[59] Charles K. Bartles, "Getting Gerasimov Right." *Military Review*, (Ocak-Şubat 2016): 37 https://www.researchgate.net/publication/329933852_Getting_Gerasimov_Right [Erişim Tarihi: 30.05.2022].
[60] McFarland, a.g.e., 2021, 32.

Çekoslovak, Doğu Almanya, Polonya ve Sovyet Rusya birliklerinin katılımı ile, hatta ilki Çekoslovakya içinde olmak üzere tatbikatlar icra etmişler, bu tatbikatları bölgede hazır askerî kuvvetlerin yığınaklanmasını meşru göstermek üzere kullanmışlardır.

Yaptırımların ve diplomatik zorlamaların sonuç vermemesi üzerine Danube Harekâtı açık bir şekilde icra edilmiştir. Operasyonla; Sovyet Rusya özel kuvvelerinin (Spetnatz) öncülüğünde Prag havalimanın kontrol altına alınması, müteakiben Prag'daki medya, radyo, televizyon ve iletişim istasyonlarının kontrol edilmesi, hükümetteki reformist üyelerin 21 Ağustos 1968'de yakalanması ve yönetimin kontrol altına alınması ile 24 saatten kısa bir sürede sona ermiştir. Bir grup ülkenin[61] ; bu askerî müdahalenin uluslararası hukuka aykırı olduğu çağrısı ile acil toplanan Birleşmiş Milletler Güvenlik Konseyinde Sovyet temsilcisi; Varşova Paktı askerlerinin Çekoslovakya'ya tanımlanamayan yabancı ve yerli aktörlerin oluşturduğu tehdide karşı Çekoslovak Hükumetinin daveti üzerine girdiğini, bu uygulamanın bölgesel antlaşmalar, BM Antlaşması ile öz savunma hakkı ve kolektif savunma kapsamında Uluslararası Hukuka da uygun olduğunu iddia etmiştir.

ABD'nin Vietnam'a müdahalesini ve İsrail'e yardımını da benzer uygulama olarak referans göstermiştir. Yapılan oylamada Konseyin 15 üyesinin 11'i olumlu, 3 üye çekimser, 2 üye ise olumsuz (SSCB ve Macaristan) oy kullanmış, daimî üye SSCB'nin olumsuz oyu ile BM Güvenlik Konseyi kararı veto olmuştur. Bu toplantılarda ABD temsilcisinin günümüz hibrit savaş anlayışı ile ilişkilendirilebilecek tespiti "İstilayı gizleme gayreti içinde dahi bulunmadılar" tespiti dikkate değerdir.[62]

Nikaragua'da 1981'de Marksist Sandanista Cuntası'nın yönetimi ele geçirmesi ile Başkan Reagan Merkezi Haber Alma Teşkilatına (CIA) yönetime karşı silahlı mücadele veren ve Kontralar (Contras) olarak bilinen ve çoğunlukla eski Ulusal Muhafızlardan oluşan grubun örtülü desteklenmesi talimatı vermiştir. İlk başlarda CIA tarafından finanse edilen ve Arjantinli subaylar üzerinden yürütülen eğitim desteği yerini kısa zamanda CIA personelince direkt olarak verilmeye başlanmıştır. Sandinista yönetimine askerî caydırıcılık maksadıyla komşu Honduras ile Nikaragua sınırına yakın bölgelerde ABD askerleri ile tatbikatlar icra edilmiş, bu çabalar Nikaragua'ya mali yardımların kesilmesi, ekonomik ve ticari yaptırımlar uygulanması, uluslararası

[61] Kanada, Danimarka, Fransa, Paraguay, Birleşik Krallık ve ABD
[62] McFarland, a.g.e., 2021, 38-39.

bankaların diplomasi baskısı ile Nikaragua'ya kredi vermesinin engellenmesi gibi ekonomik yaptırımlarla desteklenmiştir.

1983 sonlarına doğru Nikaragua limanları, köprüleri, silah ve yakıt depolarını hedef alan saldırılar CIA'in direkt desteği ve katılımı ile artmış, 1984 ocak ve şubat aylarında kritik tesislere hava taarruzları ve hava sahası ihlalleri ile perdelenerek ABD gemilerinden çıkan botlar ile limanları mayınlanmıştır. Nikaragua yönetiminin Birleşmiş Milletler Güvenlik Konseyinde ABD müdahalelerinin görüşülmesi için girişimlerde bulunmuş önce 1983'te sorunların diplomatik yollarla çözümlenmesine yönelik bir karar çıkmıştır. Güç kullanımı ve limanların mayınlanmasının gündeme getirildiği diğer bir toplantıda ise 13 üye ülke temsilcisinin mayınlamanın uluslararası hukukun ihlali yönünde verdiği oya rağmen Birleşik Krallık çekimser oy kullanmış, ABD olumsuz oy kullanarak kararı veto ederek kararın onaylanmasını engellemiştir. Contra'lara silah ve mali desteğin İran üzerinden yapılması, bu fonların oluşturulmasında özel organizasyonların faaliyetlerinde bağış toplanması, bu fonların aktarılmasında İsviçre bankaları ve off-shore hesapların kullanılması ise günümüzdeki benzeri uygulamalara örnek teşkil etmiştir. Bu uluslararası hukuka aykırı yardımlar en nihayetinde Uluslararası Adalet Divânı tarafından incelenmiş ve Divân ABD'yi haksız bulmuştur.[63]

Aslında yürütülen bu örtülü faaliyetler, ABD yasaları kapsamında suç teşkil etmemekte ve CIA bu kapsamda yetkiyi 1948 yılında Başkan Truman tarafından onaylanarak yürürlüğe giren Ulusal Güvenlik Konseyi Direktifinden almaktadır. İstihbarat Teşkilatı Yapılanması kapsamında Özel Projeler Ofisinin yetki ve sorumluluklarını belirleyen 292 Numaralı kanunun 5'inci maddesinde istihbarat teşkilatının; propaganda, ekonomik savaş, önleyici direkt görev harekâtı (sabotaj, tahrip ve kaçırma), hasım ülkeye yöneltilmiş yıkıcı faaliyetler (direniş kuvvetlerinin, gerilla ve özgürlükçü gruplar ile anti-komünist yerel grupların desteklenmesi) yeteneklerine sahip olması gerektiği tanımlanmıştır.[64] Bu kapsamda yasa ile

[63] International Court of Justice, "Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)", *Merits, Judgment. I.C.J. Reports 1986*, (1986), 14. https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf [Erişim Tarihi: 15.05.2022].

[64] National Security Council, *National Security Council Directive on Office of Special Projects (1948)*, (1948). https://history.state.gov/historicaldocuments/frus1945-50Intel/d292 [Erişim Tarihi: 19.04.2022].

tanımlanan özel aktiviteler ve örtülü faaliyetlerin açık olarak günümüzde karşı karşıya kaldığımız Hibrit Harekât kapsamına girdiği açıkça ifade edilebilir.

Örneklerde açıkça görüldüğü ve Irak (1991, 2003), Yugoslavya (1999), Haiti (1994, 2004), Afganistan (2001) müdahaleleri gibi birçok sıcak çatışmanın alt yapısını oluşturan nedenler, yakın dönem harp tarihinde benzer öğeler barındırmaktadır. Bu konseptin; hassas planlama gerektirdiği, askerî olmayan unsurlar ile muhtemel harekât ortamın şekillendirmeyi kapsadığı, hasım ülke ve tarafların savaş ilanına yol açmayacak politik ve askerî eşiği aşmayacak seviyede açık veya örtülü güç kullanımını içerdiği, tüm devlet kurumlarının senkronizasyonunu gerektirdiği, ekonomik, diplomatik, sosyo-politik ve pek çok alanı güç unsuru olarak kullandığı, özellikle büyük devletlerin BM Güvenlik Konseyindeki veto haklarını da gerektiğinde kullanarak çeşitli gerekçelerle güç kullanımını engellemek üzere oluşturulmaya çalışılan uluslararası hukuk kurallarını esnettikleri gözlemlenmektedir. Bu kapsamda; politik veya stratejik hedeflere ulaşmak maksadıyla askerî yöntemlerin yerine veya desteğinde askerî olmayan yöntemlerin açık veya örtülü kullanılması konsepti, görüldüğü üzere ne yeni ne de tek bir bölge, politik ideolojiye veya askerî olarak zayıf olana ait değildir çıkarımı yapılabilir.

Günümüzde güç mücadelesinin harekât alanında icrasını tanımlamak üzere kullanılan pek çok terimin belki de en popüler olanı, hibrit savaşın tanımlanmasına yönelik Galeotti[65], Fridman[66], Renz[67], Lanoszka[68] gibi akademisyenlerin Rus odaklı yaklaşımlarıyla sıkça karşılaşılmakla beraber kavramı daha evrensel yorumlayanların, bahse konu günümüz güç mücadelesinin sahaya yansıyan icrasını tanımlanmasında daha objektif bir bakış açısını ortaya koydukları görülmektedir. Lakin savaşın dönüşüm sürecinde gerek batı gerekse doğu bloğu güç odaklarının tarih boyunca benzer stratejiler doğrultusunda benzer hibrit uygulamalara başvurdukları görülmektedir, ki üzerinde uzlaşıya varılan husus, konvansiyonel ve düzensiz unsurların, savaşın çeşitli uygulama yöntemleri ile topyekûn bir mücadele olan savaş

[65] Mark Galeotti, "Hybrid, Ambiguous, and Non-Linear? How New Is Russia's 'New Way of War'?", *Small Wars and Insurgencies*, C. 27, S. 2 (2016): 296-297. https://doi.org/10.1080/09592318.2015.1129170 [Erişim Tarihi: 15.05.2022].
[66] Fridman, a.g.e., 2018, 21.
[67] Bettina Renz, "Russia and 'Hybrid Warfare", *Contemporary Politics*, C. 22, S. 3 (2016): 283–300. https://doi.org/10.1080/13569775.2016.1201316 [Erişim Tarihi: 10.04.2022].
[68] Alexander Lanoszka, "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe", *International Affairs*, C. 92, S. 1 (2016): 175–195. https://doi.org/10.1111/1468-2346.12509 [Erişim Tarihi: 15.05.2022].

için yeni bir kavram olmadığıdır. Yeni ve eski savaşları karşılaştırarak inceleyen Karaosmanoğlu da Clausewitz'in tanımladığı klasik savaş tanımını içeren kavramsal çerçevenin günümüzde de büyük oranda geçerli olduğu, yeni savaş diye tanımlanmaya çalışılan olgunun, ki hibrit savaş da bu kapsamda değerlendirilmelidir, savaş kavramının doğasını değiştirecek ölçüde olmadığı sonucuna varmıştır.[69]

2.4.1. Gri Alan Aktiviteleri ve Şiddet Eşiği Kavramı

Ülkeler yüzyıllardır inkâr edebilecekleri ölçüde birbirlerinin iç işlerine karışmışlardır. İkinci Dünya Savaşı sonrasındaki soğuk savaş döneminde bu faili veya eylemin kendi inkâr edilebilen faaliyetlere "gizli veya örtülü faaliyetler" denmiştir.[70]

Özellikle soğuk savaş sonrası dönemde hasım ülke üzerinde baskı unsuru oluşturarak hedeflenen politik hedeflere ulaşmak maksadıyla uluslararası hukukun boşluklarının suiistimal edilmesi ile sıkça karşılaşılmaya başlanmıştır. Devletler Arasında Dostane İlişkiler ve İş Birliği Prensipleri Üzerine Uluslararası Hukuk Deklarasyonu ile tanımlanmaya çalışılan prensiplerin, çoğu kez inandırıcılığı şüpheli olsa da inkâr edilerek bir baskı unsuru olarak uygulandığına şahit olunmaktadır. Liderler zaman zaman inandırıcılığın dışına çıksa da inkâr ettikleri faaliyetleri diğer ülke üzerinde etki oluşturmak üzere kullanmaya devam etmektedirler. Gizli veya örtülü faaliyetlerin saf dışı bırakmayan bu inkâr edilebilen faaliyetler, gizli ve açık icra arasındaki bu gri alanda uygulayan devlete, silahlı çatışmaya varmayacak seviyede güç kullanarak politikalarını dikte etme bağlamında önemli avantajlar sağlamaktadır. Taraflar birbirlerini itham etseler de Rusya Federasyonu'ndan ABD'ye, Çin Halk Cumhuriyeti'nden İran İslam Cumhuriyeti'ne pek çok ülke politik hedefleri doğrultusunda bu yolla diğer ülkelerin iç işlerine müdahale etmiştir.[71]

Bahse konu uluslararası hukuk prensiplerin hilafındaki bu uygulamalar çoğunlukla hedef ülke tarafından hoş karşılanılmayıp tedbir getirilse de uygulayıcı ülke tarafından bu saldırıların dozu politik veya askerî olarak tepki verme için yeterli hukuki meşruiyeti oluşturacak eşiğinin altında tutulmaktadır. Dikkatli planlama ile uygulanan

---

[69] Ali L. Karaosmanoğlu, "Yirmibirinci Yüzyılda Savaşı Tartışmak: Clausewitz Yeniden", *Uluslararası İlişkiler Dergisi*, C. 8, S.29 (2011): 24-25. http://www.uidergisi.com/wp-content/uploads/2013/02/21st-yuzyilda-savasi-tartisma.pdf [Erişim Tarihi: 15.05.2022].

[70] Rory Cormac ve Richard J Aldrich. "Grey Is the New Black: Covert Action and Implausible Deniability." *International Affairs* C. 3 (2018): 477–478. https://doi.org/10.1093/ia/iiy067 [Erişim Tarihi: 16.01.2023].

[71] a.g.m., 493.

bu faaliyetler BM Güvenlik Konseyince yaptırım uygulama kararı almaya yetmeyecek seviyede tutulmaktadır. Rusya'nın Kırım'ın ilhakında uyguladığı, Çin Halk Cumhuriyeti'nin Güney Çin Denizi'nde uyguladığı faaliyetler bu kapsamda örnek teşkil edebilirler. Özellikle bu faaliyetleri uygulayan ülke, Birleşmiş Milletler Güvenlik Konseyinin 5 Daimî Üyesinden biri ise karar alınmasını veto hakkı ile de desteklenerek uluslararası kamuoyunun gerilime müdahalesinin de önünü tıkamaktadır.

Bu dışarıdan müdahalelerin ölçüsü makul inkâr edilebilirlik (plausible deniability) kapsamında planlanmakta ve dikkatle icra edilmektedir.[72] Bu kavram uluslararası hukuk kapsamında dostane ilişkiler ve iş birliği deklarasyonu kapsamında diğer ülkelerin bağımsızlıklarından doğan haklarına saygı gösterilmesini tanımlayan prensiplerin hilafında icraatları perdelemek üzere yapılan açıklama ve inkârları ifade etmek için kullanılmaktadır. Buna, Kırım'ın ilhakı ve Donbas/Luhansk bölgelerinde silah sevkiyatlarının Rus ordusu ile ilişkisinin olmadığı, çatışanların ayrılıkçı sivil milisler olduğu, Rus ordusunun bu faaliyetlere destek sağlamadığı yönündeki deklarasyonlar örnek olarak gösterilebilir. Hatta ele geçirilen kimi 'milis' diye tanımlanan kişilerin Rus ordusu veya askerî istihbarat teşkilatı mensubu oldukları ispat edilse dahi bunların izinde kendi iradeleri ile bahse konu bölgedeki çatışmalara katıldıkları iddiaları, aşikâr gözüken müdahalenin nasıl inkâr edilebildiği konusunda zaman zaman şaşkınlığa düşürecek seviyede gerçekleşebilmektedir.[73]

Hasım ülkenin krizi savaşa taşıyacak şekilde siyasi ve/veya askerî karşılık verme eşiğinin altında faaliyet göstermek için sıklıkla; düzensiz unsurlar veya gizlilik içinde faaliyet gösterebilecek oldukça yetkin özel birlikler, yetkin vekil kuvvetler (istihbarat teşkilatları veya özel kuvvetlerce eğitilmiş milisler, gönüllüler vb.) gibi inkâr edilebilir kuvvetler kullanılır. Bu tip inkâr edilen saldırılarla ve bunları icra edenlerle mücadelede de genellikle paramiliter veya eski askerlerden oluşan kuvvelerle

[72] Maciej Bartkowski, "Nonviolent Civilian Defense to Counter Russian Hybrid Warfare", (Johns Hopkins University Krieger School of Arts and Sciences, 2015), 8. https://www.nonviolent-conflict.org/wp-content/uploads/2018/12/GOV1501_WhitePaper_Bartkowski.pdf [Erişim Tarihi: 30.05.2022].

[73] Eli Lake, "U.S. Eyes Russian Spies Infiltrating Ukraine", Daily Beast, 2014. https://www.thedailybeast.com/us-eyes-russian-spies-infiltrating-ukraine [Erişim Tarihi: 15.05.2022].; Oussama Romdhani, "Tunisia, the West, and the 'Arab Spring.' " *The Atlantic Council*, (2017). https://www.atlanticcouncil.org/blogs/menasource/tunisia-the-west-and-the-arab-spring/ [Erişim Tarihi: 10.04.2022].

uygulanan tehdide benzer metotlar tercih edilmektedir.[74] Lakin konvansiyonel kuvvetlerle açıktan yapılacak müdahaleler, karşı tarafın; sivillere veya ayaklanan ırkdaşlara karşı aşırı güç kullanımı propagandasını destekleyeceğinden, haksız duruma düşülerek, barış gücü kisvesi altında da olsa olası bir askerî müdahale için zemin hazırlayacağından dolayı tercih edilmediği gözlemlenmektedir.

Savaş durumu ile barış durumu arasında kalan bu alanda vuku bulan devletler arası ya da devlet ile devlet dışı aktörler arasındaki bu güç çekişmesine 'gri alan faaliyetleri' denilmektedir. Düzensiz savaş, düşük yoğunluklu çatışma, asimetrik savaş, savaş dışı askerî harekât ve küçük savaş terimlerinin yerine kullanılan Gri Alan Faaliyetleri savaş ile barış durumu arasında cereyan eden güç mücadelelerini ifade etmek üzere, hibrit savaş gibi, yeni bir terim olarak kullanılmaktadır.[75] Hibrit savaş vasıtalarının da kullanıldığı bu faaliyetlerin genellikle daha stratejik seviyede ve nispeten daha az şiddet içeren uygulamalar olduğu yönünde genel bir çıkarım yapmak mümkündür.

Mazarr, süper ya da bölgesel güç olarak ulusal politikaları doğrultusunda çevrelerindeki statükoyu değiştirmek üzere hedef ülke veya bölgedeki diğer güçler ile savaş seviyesine taşımadan silahlı ve/veya silahsız mücadele içine giren ülkeleri 'değişimci (revisionist)' ülkeler olarak isimlendirmekte, bu gibi ülkelerin durumlarından memnuniyetsizliklerinin neticesi olarak mevcut şartları değiştirmeye yönelik güç mücadelesi içine girerek hegemonyalarını kabul ettirme gayreti içine girdiklerini iddia etmektedir. Gelişen ve güçlenen ülkelerin bu tür güç mücadeleleri içinde daha çok yer aldıkları tespitinde de bulunan Mazarr, Çin Halk Cumhuriyeti'nin son dönemde Güney Çin Denizindeki yayılmacı politikasına karşı çıkılması ile silahlanmasının artması, bölgedeki diğer ülkeler üzerinde yaptırım ve tanımlamaya çalıştığımız gri alan faaliyetleri uygulamaya başlaması örneği ile desteklemektedir.[76] Mazarr; Shelling'in "Arms and Influence" eserinde kullandığı "salam dilimleme" metaforu üzerinden gri alan aktivitelerini açıklamakta, devletlerin de, Shelling'in metaforundaki suya girmemesi öğütlenen çocuğun önce ayaklarını sokması, sonra

---

[74] Antulio J Echevarria II, *Operating in the Gray Zone An Alternative Paradigm for U.S. Military Strategy*, (Carlisle: Strategic Studies Institute and U.S. Army War College Press, 2016): 12. https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1424&context=monographs [Erişim Tarihi: 16.01.2023].

[75] Philip Kapusta, "The Gray Zone." *Special Warfare*. (2015): 20. https://www.soc.mil/SWCS/SWmag/archive/SW2804/GrayZone.pdf [Erişim Tarihi: 15.05.2022].

[76] Michael J. Mazarr, "Mastering the Gray Zone", *Understanding a Changing Era of Conflict*, (Carlisle, PA: U.S. Army War Collage US Army Publication, 2015), 14-16. https://publications.armywarcollege.edu/pubs/2372.pdf [Erişim Tarihi: 19.04.2022].

biraz daha girmesi, sonra biraz daha derken tamamen yüzen çocuğa ebeveynlerinin en son "göremeyeceğimiz kadar açılma" diyerek durumu kabullenmeleri gibi, tehdit eden ülkelerin önce küçük müdahaleleri zaman içinde yavaş yavaş artırarak hedef ülkeye bu müdahaleleri kanıksatan bir metodoloji izledikleri tespitinde bulunmaktadır.[77]

Hoffman hibrit tehditlerin tanımının şiddet içermeyen yaptırımları kapsayan gri alan faaliyetlerini açıklamada yetersiz kaldığını kabul etmiştir. Ekonomik ve finansal yaptırımlar, ticaret sendikaları ya da Devlet Dışı Organizasyonlar kurmak veya örtülü olarak finanse ederek hükumeti yıpratmak üzere kullanmak, sahte örün (Web) siteleri kurarak bu siteler üzerinden ya da sahte hesaplar üzerinden dezenformasyon içeren paylaşımlar yaparak bilgi harekâtı yürütmek, örtülü ve politik yıkıcı eylemler, medyanın manipüle edilmesi, yolsuzlukların suiistimal edilmesi günümüzde güç mücadelesi içindeki büyük devletlerin kullandıkları yeni gri alan aktiviteleri olarak sayılabilir.[78]

Barış durumu ile savaş arasındaki bulanık ortamda yürütülen ve bir tür yumuşak güç kullanımı olan bu terim; politik hedefe ulaşabilmek üzere geniş bir yelpaze oluşturan araç ve eylemlerin hasım ülke üzerinde uygulanması olarak tanımlanmaktadır. Tüm gri alan faaliyetlerinin aslında bir nevi politik savaş vasıtası olduğu söylenebilir. Diplomatik, politik, ekonomik ve daha geniş bir çerçevede ulusal güvenlik stratejisi politik savaşın vasıtaları olarak sayılabilir. Rusların 'aktif tedbirler' olarak tanımladığı ve soğuk savaş döneminden itibaren uyguladıkları politik, ekonomik ve sosyal baskı oluşturarak batılı ülkeleri zayıflatmayı amaçlayan politikalarına günümüzde siber saldırıları ve enerjinin bu maksatla kullanımını da eklemek mümkündür.[79]

2.4.2. Sınırsız Savaş Konsepti (Unrestricted Warfare)

Stratejik görüşü Sun Tzu doktrinine dayanan Çin, günümüz mücadelesinde sürpriz ve aldatmayı esas almakla birlikte, sivil teknolojisi ile desteklediği askerî yeteneklerinin caydırıcılığı ile demokratik toplumların değerlerini de hedef alarak savaşma azmini kırmaya yönelik, eski ve yeniyi birleştirdiği, daha önceden savaş için kullanılmayan

[77] a.g.r., 34-35.
[78] Frank G. Hoffman, "On Not So New Warfare: Political Warfare Vs Hybrid Threats", *War on the Rocks*, (2014). https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/ [Erişim Tarihi: 15.05.2022].
[79] Mazarr, a.g.r., 48-50.

metotları güç mücadelesine dahil ederek savaş konseptini genişleten bir stratejiyi uygulamaktadır.[80]

Qiao ve Wang küreselleşen ve gelişen savaşı birbiri ile ilişkili fakat farklı iki gelişmeye bağlamaktadır. Bunların ilkinin gelişen bilgi teknolojilerinin güç mücadelelerindeki rolünün artışı, diğeri ise; profesyonel olmayan savaşçıların (milisler vb.) veya devlet dışı organizasyonların giderek devletlere karşı daha fazla tehdit oluşturmaları, her geçen gün ordulara karşı daha ciddi bir rakip olmaya başlamaları olduğunun ileri sürmektedir. Yazarlara göre bu iki gelişme, sınırsız savaş teorisi kapsamında bahsedilen, terörizm, siber suçlar, mali manipülasyonlar/yaptırımlar gibi askerî olmayan yöntem ve metotların güç çekişmesindeki rolünü artırmaktadır. Teknik, bilimsel, teorik, psikolojik, etik, geleneksel veya diğer sınırların modern savaş anlayışı ile bulanıklaştığı, bu bulanıklık içinde neresi çatışma alanı neresi değil, kim asker kim değil, kullanılan yaptırım unsurunun hangisi silah hangisi değil fark edilmesinin güçleştiği ileri sürülmektedir.[81] Teoriyi ortaya koyan yazarlar; günümüz güç mücadelesinde dört çeşit unsurun kombine şekilde kullanılmasın gerektiğini vurgularlarken bunları;

1. Ulusal, uluslararası ve devlet dışı organizasyonların birlikte kullanımını ifade eden ulus-üstü Supra-national) kombinasyon,

2. Harekât tabanlarının, yani kara, deniz, hava, bilgi, uzay tabanlarının yanında, finans, ticari ve psikolojik savaşın de günümüz harekât ve güç çekişmelerinin bir parçası olduğu iddiasıyla tüm bu fonksiyon alanlarının eşgüdüm içinde kullanılmasını ifade eden harekât tabanı-üstü (Supra-domain) kombinasyon,

3. Askerî veya değil, yaptırım için kullanılabilecek tüm yöntemlerin birlikte kullanılmasını ifade eden yöntem-üstü (Supra-means) kombinasyon,

4. Politik, stratejik, operasyonel ve taktik seviyeler arasındaki farklılıkların da günümüz çekişmelerinde bulanıklaştığı tespitine dayanarak, her seviyede bakış açısı, yöntem ve eylemlerin mevcut çekişme ortamına yansıtıldığı seviye-üstü (Supra-tier combination) kombinasyon yaklaşımı olarak sıralamaktadırlar.[82]

[80] Liang Qiao ve Xiangsui Wang, *Unrestricted Warfare*, (New Delhi: Natraj Publishers, 2007), 42-43.
[81] a.g.e., 10-36.
[82] a.g.e., 155-171.

Tüm bu unsurların ulusal politik hedefleri desteklemek üzere birlikte kullanılması üzerine kurulan bu sınır aşan savaş teorisinin uygulamasında 8 prensibe dikkat çeken yazarlar bunları;

- Çok yönlülük – çok tabanlı harekât uygulamalarını vurgulamakla birlikte mücadelenin askerî, yarı askerî veya sivil, şiddet içeren ya da içermeyen, askerlerin ya da konusunun uzmanı sivillerin rol alabileceği tüm milli güç unsurları ile icra,
- Senkronizasyon – Farklı harekât tabanlarında ve coğrafyada sürdürülen mücadelenin birbirleri ile eşgüdüm ve zaman uyumlu olarak icrası,
- Kısıtlı hedeflilik – Kullanılacak metotlara göre erişilebilir, etki altına alınabilir belli miktarda hedefe yönelinmesi,
- Metotlarda kısıtsızlık – Belirli miktardaki hedeflere karşı uygulanacak metotların kısıtsızlığı,
- Asimetri – Beklenmeyen yerde beklenmeyen ve mücadele edilen unsurlar ile büyüklük, kapasite veya tür olarak zıt unsurlarla tesir yaratmayı,
- Tüketimde tasarruf – mücadelenin sürdürülebilmesi için mantıklı bir icranın esas alınması; mantıklı hedef seçimi ve mantıklı bir kaynak kullanımı ile kaynak kullanımında ekonomiyi,
- Çok yönlü koordinasyon – farklı harekât alanlarında ve tabanlarında görev alan farklı kuvvetlerin hedefe ulaşılması için koordine içinde faaliyetleri icrası,
- Sürecin tamamının kontrol ve düzenlenmesi – Dinamik günümüz mücadele ortamında planın hedeflenen şekilde yürütülmesi maksadıyla gelişmelere adaptasyonu ve işleyişin sürekli kontrolü olarak sıralamaktadırlar.[83]

Özellikle Çin'in günümüzdeki güç çekişmelerinde uyguladığı, çok yönlü, çok tabanlı, kapsamlı, coğrafi sınır tanımayan ve nispeten caydırıcılıkla birlikte daha az şiddet içeren, yumuşak güç kullanımı ile daha çok bağdaştırabileceğimiz stratejisini açıklayan bu kavram, tanımlamaya çalışılan günümüz savaş ve güç çekişmelerinde kendine has özellikleri ve bakış açısı ile, gri alan faaliyetlerine daha yakın bir konumda yer almaktadır. Sorunların sadece askerî olarak çözülemeyeceğinin bilincinde

[83] a.g.e., 175-188.

geliştirilen ve daha çok güçlü olunan ekonomik, ticari, teknolojik ve endüstriyel alanlardaki üstünlüklerin güç yarışına yansıtıldığı bir yaklaşımın benimsendiği, ideolojinin de kullanılmakla beraber terör örgütleri de dahil olmak üzere devlet dışı örgütlerin fikir ile yönlendirilmesinin de bir mücadele metodu olarak kullanabilecek ölçüde farklı bakış açısına sahip olduğu çok yönlü, kapsamlı bir stratejiyi tanımladığı söylenebilir.

2.4.3. Bilgi Harekâtı

ABD askerî doktrini bilgi ortamının bileşenlerini kişiler, organizasyonlar ve sistemler olarak listelemektedir. Komuta kontrol sistemleri, kritik karar vericiler ve kişiler ve organizasyonların etki yaratmasını destekleyen tesisleri bilgi ortamını fiziksel bileşenleri olarak tanımlamaktadır. Bu ortamın bilgi boyutunda toplama, işleme, saklama, yayımlama ve koruma fonksiyonlarının birbirleri ile etkileşimli döngüsünü anlatılırken; bilgi ortamının kavramsal boyutu ise, bahse konu bilginin yayılması, hedef tarafından alınması, buna göre bir tepki oluşması ve algısı doğrultusunda eyleme dönüştürülmesi olarak açıklanmaktadır. Bilgi harekâtı ise, tanımlanan bu bilgi ortamında karar vericileri ve karar vericiler üzerinde baskı oluşturan topluluğun algısı üzerinde etki oluşturarak, ulusal stratejiyi destekleme doğrultusunda tesir yaratmak olarak tanımlanmaktadır.[84]

Ruslar ise; "Hasmın askerî ve/veya politik liderleri, askerleri ve halkı üzerinde gelişmiş bilgi teknolojileri vasıtası ile bilgi ve algıya dayalı psikolojik baskı oluşturarak hasmın kritik askerî, endüstriyel ve idari yapı ve sistemlerinin işleyişini bozmak" olarak tanımlamaktadırlar.[85] Doğu ve batı bloklarının bilgi alanının stratejiyi desteklemek üzere kullanımı konusunda doktriner olarak oldukça benzeştikleri, her iki bakış açısının da farklı, yeni bir yaklaşım ortaya koymadığı söylenebilir.[86]

Bu kapsamda günümüz güç çekişmesinde; hedef ülkeye dolaylı müdahalede algının şekillendirilmesine yönelik, özellikle istihbarat teşkilatları ve özel kuvvetler üzerinden yürütülen, iletişim teknolojilerindeki gelişmeler neticesinde siber alandan da

[84] US Department of Defence, *JP 3-13 Information Operations*, Washington DC: Joint Publication Series, 1(1), 2014, 1–3.
[85] Alina Prelipcean, Andrei Albert "Landmarks of Russia's Use of Information Warfare." *Strategies XXI- Security and Defense Faculty*, C. 17, S. 1 (2021): 140–144. https://doi.org/10.53477/2668-2001-21-16 [Erişim Tarihi: 10.04.2022].
[86] Sandor Fabian, "The Russian Hybrid Warfare Strategy–Neither Russian nor Strategy", *Defense and Security Analysis*, C. 35, S. 3 (2019): 308–325. https://doi.org/10.1080/14751798.2019.1640424 [Erişim Tarihi: 16.01.2023].

desteklenen bilgi harekâtı faaliyetleri önemli rol oynamaktadır. Bu çabalar sosyal hassasiyetleri suiistimal ederek toplumsal olaylar çıkartmaktan, seçimlere müdahaleye kadar geniş bir yelpazede seyredebilmektedir (Rusya'nın 2016 ABD Seçimlerine müdahale iddiaları vb.).[87] Batı doktrini ile oldukça örtüşen, Panarin'in sistematik bir şekilde icrasını tanımladığı bilgi harekâtı çerçevesinde açık/yarı açık/gizli olmak üzere propaganda faaliyetleri, sosyal ve klasik medya üzerinden dezenformasyonu da içerecek şekilde algı operasyonları ile bu faaliyetlere karşı hasmın gayretlerini bastırmaya yönelik sistemlerin baskılanması faaliyetleri sayılabilir.[88]

Berzins'in ifade ettiği gibi, artık günümüzde harekât alanı toplulukların beyinleridir. Bu sebeple, iletişimin gelişmesi ve manipüle edilebilirliğinin artması ile, dezenformasyon da dahil olmak üzere algıyı yönetmek üzere bilgi harekâtı ve psikolojik harekât uygulamalarının önemi her geçen gün artmakta ve hibrit savaşın temel araçları halini almaktadır.[89] Bu araçlar, hedef ülkede, özellikle etnik ve kültürel bağlantı veya yakınlığı bulunan halka yöneltilmekte, bu toplulukların belirlenen plan doğrultusunda genel stratejiyi destekleyecek şekilde hareketlendirilmek üzere hayata geçirilmektedir. Bu bağlamda hedef ülkede etnik ve kültürel yakınlığı olan bir nüfusun bulunması, bu kapsamda uygulanacak hibrit tehditlere karşı hassasiyeti artıracak bir faktör olarak değerlendirilmelidir.[90]

Gelişen iletişim teknolojileri ve elektronik sistemlerin karar mekanizmaları da dahil olmak üzere hayatın her alanındaki artan kullanımı nedeniyle tüm bu çabalar siber yeteneklerle desteklenmekte, kitlelere erişim ve etkiler artırılmaktadır. Siber yetenekler hedef ülkenin halkını etkilemek üzere bilgi harekâtını desteklemede yumuşak güç unsuru olarak kullanılabildiği gibi, o hedef ülkedeki kimi kritik tesislerin komuta tesislerine zarar vererek ya da işlevsiz hale getirerek bir bombardımandan daha çok zarar yaratacak bir etki oluşturulabilir. Buna metropolleri besleyen elektrik santralleri, nükleer reaktörler gibi tesislerin işleyişini tehdit edecek siber saldırıları

[87] McFarland, a.g.e., 119.
[88] Jolanta Darczewska, "The Anatomy of Russian Information Warfare", Point of View, Derleyen: Anna Łabuszewska, (Warsaw: Centre for Eastern Studies, C. May 14, 2014), 15. http://www.osw.waw.pl/en/publikacje/point-view/2014-05-22/anatomy-russian-information-warfare-crimean-operation-a-case-study [Erişim Tarihi: 16.01.2023].
[89] Jānis Bērziņš, "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy," Nisan, 2014, 5. https://sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf [Erişim Tarihi: 16.08.2023].
[90] Ali Nedim Karabulut, "Eski Savaş, Yeni Strateji: Rusya'nın Yirmibirinci Yüzyıldaki Hibrit Savaş Doktrini ve Ukrayna Krizi'ndeki Uygulaması", *Uluslararası İlişkiler Dergisi*, C. 13, S. 49 (2016), 38.

örnek olarak verebiliriz ki bu da siber yeteneğin sert güç kullanımı olarak ifade edilmektedir. Nye ayrıca; kompleks bir siber sistemin desteklediği askerî ve ekonomik tesislere bağımlılığı olan büyük devletlerin, siber saldırı ile bu hassasiyeti suiistimal edebilecek devlet dışı aktörlere karşı zafiyet yaşayabileceğini belirtmektedir [91]. Konvansiyonel bir saldırı ile sağlanmasının çok zor ve maliyetli olacağı bu gibi durumların, çok boyutlu (multi-domain) günümüz savaşında devlet dışı aktörlerin kendi başlarına veya devletlerin vekili olarak siber alanda icra edilecek saldırılarla hasım ülkeye genel strateji doğrultusunda diğer alanlarda yürütülen çabalarla eş güdüm içerisinde hatırı sayılır etki yaratabileceğini söylemek yanlış olmayacaktır.

Devlet dışı aktörlerin veya diğer devletlerin hedef ülkeye karşı şiddet, terörist eylemler, harekâtın desteklenmesi gibi kinetik metotlarla veya baskı, provokasyon, dezenformasyonu da içerecek şekilde algı üzerine faaliyetler, siber saldırılar gibi kinetik olmayan metotları patron ülke adına yani vekil olarak gerçekleştirebildikleri görülmektedir. Vekil olarak icra edilen bu faaliyetlerin günümüz güç mücadelesinde kullanımı vekâlet savaşları olgusunu ortaya çıkartmıştır.

2.5. Hibrit Savaş Belli Bir Ülkeye mi Ait?

Hibrit savaş konseptinin Rusya odaklı yeni savaş konsepti olduğunu belki de en kuvvetli şekilde eleştiren akademisyenlerden olan Galeotti, "Geresimov Doktrini" ifadesini ilk kez Gerasimov'un 2013'te yayınlanan yazısını yorumladığı blogunda[92] kullanmasının niyetinin dışında farklı algılandığını belirtmektedir. "Lineer olmayan savaş" olarak tanımlamayı tercih ettiği açıklamakta olduğumuz genel kabul görmüş terim olarak "Hibrit Savaş"ın yeni bir Rus kapsamlı savaş yaklaşımı olarak anlaşıldığını, ancak blogunda yazdığı gibi Gerasimov'un da Arap Baharı ve dönemin diğer gelişmeleri ekseninde geleceğin çatışmalarının nasıl gerçekleşebileceğine yönelik görüşlerini yazdığını ifade etmekte, kendi açıklamalarının Rusya'nın takip eden dönemde Kırım'ı ilhakı ile Gerasimov'un açıklamalarının yerine kendisinin

[91] Joseph S. Nye, *Cyber Power*, (London: Belfer Center for Science and International Affairs of Harvard Kennedy School, 2010), 4-6. https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf [Erişim Tarihi: 20.05.2022].
[92] Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War", *In Moskow's Shadows,* 2014. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/ [Erişim Tarihi: 16.12.2022].

isimlendirdiği yeni bir savaş nevi, bir doktrin olarak algılandığını belirtmektedir.[93] Hibrit savaşın Rusya Federasyonu'na özgü bir strateji ve uyguladığı doktrin olmadığını Fridman da çalışmasında derinlemesine incelemiş; Lind tarafından ortaya atılan 4'üncü Nesil Savaş, Liang ve Xiangsui tarafından geliştirilen ve Çin Halk Cumhuriyeti'nin güç mücadelesindeki strateji ile özdeşleştirilen "Sınırsız Savaş" doktrininden, NATO tarafından yeniden konseptleştirilen "Hibrit Savaş"tan, Çekinov ve Bogdanov tarafından formüle edilmeye çalışılan "Rus Yeni Nesil Savaş"ının aynı genel konsepte işaret ettiğini belirtmiştir.[94] En nihayetinde bahsi geçen tüm stratejik konseptler askerî ve askerî olmayan metot ve unsurların politik hedefe ulaşmak üzere senkronize bir şekilde kullanımına işaret ederken, savaşın tanımı içinde yer alan "politik hedefe ulaşmak için tüm milli güç unsurlarının seferber edilmesi" tanımının kavramsal olarak ötesine geçmemektedir.[95] Bunun yanında; güç çekişmesinin hayata geçirilmesi, harekât alanına yansıması olarak yorumlayabileceğimiz Hibrit Savaşın herhangi bir ülke veya bölgeden bağımsız olarak doğu veya batının değil, günümüzün mücadelesi olduğu tekrar vurgulanmalıdır.

Araştırmamızın ortamını oluşturan, anlamaya ve tanımlamaya çalışılan günümüz güç mücadelesinde kullanılan strateji, popüler ifade şekli ile Hibrit Savaş Luttwak'ın paradoksal strateji fikrine uyum göstermektedir.[96] Uygulanışına ilişkin konseptsel parametreler konusunda evrensel bir uzlaşıya varılmamış olsa da kompleks, düzensiz, doğrusal olmayan, farklı alanlarda eş zamanlı uygulamalar, kinetik ve kinetik olmayan unsurları barındıran konvansiyonel ve düzensiz unsurların birlikte kullanımını ile karakterize edilen hibrit savaş; kompleks, genellikle mantık ötesinde işleyen, tek düze olmayan ve durumsal olarak çelişken yapısı ile karakterize edilen ve Luttwak'ın "Tüm stratejiler paradoksaldır" yaklaşımı ile özdeşleştirebileceğimiz strateji ile uyumludur. Kırım'ın ilhakı örneğine bakacak olursak, belirsizliğin hâkim olduğu oramda gerçekleşen istila, karşı çıkanların tepki olarak neredeyse hiçbir şey yapmamaları ve durumun bir şekilde kabullenilmesi ve her geçen gün eskiye dönüşün imkânsızlaştığı, hibrit savaşın stratejik paradoksun merkezinde yer aldığı bir durum oluşturmuştur.

---

[93] Mark Galeotti, "I'm Sorry for Creating the 'Gerasimov Doctrine.'" *Foreign Policy*, 2018. https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/ [Erişim Tarihi: 16.01.2023].
[94] Fridman, a.g.e., 403-405.
[95] Fabian, a.g.m., 315.
[96] Luttwak, a.g.e., 2001, 261.

Bilindiği üzere; hükumetlerce belirlenen politikalar ulaşılmak istenen son noktayı tanımlarken "Ne?" ve "Neden?" sorularına cevap olurken, izlenecek politikaların "Nasıl?" hayata geçirileceğinin cevabını strateji, stratejik seviye belirler. Operasyonel ve taktik seviyeler ise icra ederler.[97] Operasyonel ve taktik seviyelerde icra edilen faaliyetler sadece askerî gibi düşünülmemeli, bilgi, ekonomi, sosyal, diplomasi, enerji gibi pek çok yan alanda icra edilen faaliyetlerin senkronizasyonu ile hedefe ulaşılmasının bu stratejinin kalbini oluşturduğu unutulmamalıdır. Bu bağlamda, yukarıda da doğu ve batı bakış açısı ile tanımlanmaya çalışılan günümüzün savaş stratejisinin, tüm ulusal güç unsurlarının askerî ve askerî olmayan yöntemlerin senkronize bir şekilde hasım ülkenin ve uluslararası ortamın zafiyetlerini suiistimal edecek şekilde kullanarak hedeflere ulaşılma gayretlerinin bir politika ile desteklenmiyor olması düşünülemez.

Rus örneği üzerinden gidecek olursak; Gerasimov'un bahsettiği stratejik/operatif seviyede güç kullanma modeli, 1996'da zamanın Dış İşleri Bakanı Primakov'un Rusya'nın tek kutuplu ABD hegemonyasındaki dünya düzenine karşı duruşunu oluşturan dış politikası doğrultusunda, uluslararası ilişkilerde dönemin gelişmelerini sentezleyerek savaş ve diplomasi arasındaki gri alanı suiistimal ederek sert güç kullanımın yöntemini açıkladığı bir yaklaşımı tanımlamaktadır. ABD hegemonyasında tek kutuplu bir dünyanın kabul edilemez olduğu görüşünde olan Primakov Rusya'nın dış politikasını; ABD'nin gücünü dengelemek için güçlenme, Sovyet Rusya'dan kopan bölgelerde Rus hakimiyetinin yeniden tesisi, ayrılan ülkelerin Rusya ile entegrasyonunun yeniden sağlanması, NATO'nun Varşova Paktından ayrılan, "Yakın Kuşak (Near Abroad)" olarak nitelendirilen çevre ülkelere genişlemesine karşı çıkma ve ABD'ye karşı dengeyi sağlayabilmek için Çin ile birlikte hareket etme prensipleri çevresinde şekillendirmiştir.[98]

Primakov'un prensipleri doğrultusunda sürdürülen Rus dış politikasının sert kuvvet kullanımının rolü ile doğrudan ilintili olduğu görülmektedir. Dış politikanın hayata geçirilmesinde bir metot olan ve Gerasimov tarafından bir gereklilik olarak açıklanan hibrit savaşta risk analizi yapılarak askerî metotların kullanımının çok riskli olduğu

[97] Murat Çalışkan, "Hybrid Warfare through the Lens of Strategic Theory", *Defense and Security Analysis*, C. 35, S. 1 (2019): 40–58, https://doi.org/10.1080/14751798.2019.1565364 [Erişim Tarihi: 16.01.2023].
[98] Eugene Rumer, "The Primakov (Not Gerasimov) Doctrine in Action." *Carnegie Endowment for International Peace*, C. June 2019, (2019), 5.

durumda askerî olmayan unsurlar ile sonuca gidilirken sert güç unsurları her zaman destekte olmuş, nükleer kabiliyetleri ülkenin güvenliğinin ve stratejik bağımsızlığının güvencesi, temelini oluşturmuş, 2008 Gürcistan müdahalesi, 2014 Ukrayna'ya ait olan Kırımın ilhakı ve Donbask ve Luhansk bölgelerinin bir bölümünün milislerce işgali ve 2015'den beri de Suriye'de atılan adımlar çok dikkatli hesaplanmıştır. Ancak Moskova; Suriye'de sert güç kullanımı ve icra edilen hibrit harekât zirve noktasına ulaşmış olmasına rağmen Kremlin arzu ettiği şekilde barışı sağlayamamış, Ortadoğu'da egemen olmak için ekonomik ve askerî güç olarak yetersiz kaldığını fark etmiştir.[99] Bu durumda vekil kuvvetler üzerinden ABD ile, bölgesel güç olarak da Türkiye ile mücadele içinde olmasının etkisi vardır ve bu durum da günümüz harekât alanının en önemli gerçeklerinden biridir.

Benzer şekilde ABD'nin NATO üzerinden Rusya üzerinde baskı kurma ve Ukrayna krizi temelinde güç mücadelesi içine girmesi, Çin'in sınırlarının ötesinde güney Pasifik, Afrika, hatta endüstri ve teknolojisini kullanarak Avrupa üzerinde bir nüfuz yaratma gayreti içerisinde olduğu görülmektedir. Küresel ve bölgesel güçlerin, politikalarını dikte etmek adına askerî veya sivil caydırıcılıklarını kullanarak, uluslararası hukukun boşluklarını da suiistimal ederek, ilgi alanlarındaki diğer ülkelere karşı, maruz kalan ülkenin askerî veya politik olarak karşılık verebileceği eşiğin altında tutularak zorlayıcı faaliyetler yürüttükleri gözlenmektedir. Hatta normalde hegemonya mücadelesi içinde rakip olan güçlerin, Lutwakk'ın "stratejinin paradoksallığı" yaklaşımını hatırlatırcasına, ortak hasma karşı ittifak içine girdikleri görülmektedir.

Toparlamak gerekirse; Bettina Renz; Pukhov'un "Hibrit Savaş Efsanesi" [100] adlı makalesinde; hibrit savaşın bir propaganda malzemesi olarak kullanıldığı, savaşın bir türünü ifade eden bir sınıflandırma olmadığı kanaatine vardığını, bu kanaate varmada hibrit savaş olarak nitelendirilen olgunun savaşa dair çok da yeni bir şey ortaya koymadığının belirleyici olduğunu ifade etmektedir.[101] Savaşın veya çatışmanın ana yapısında bir değişiklik olmamakla birlikte, güç mücadelesi içinde uygulanışına yönelik değişiklikler olduğu aşikardır.

[99] a.g.m., 1-5.
[100] Piotr Pukhov, "Миф о 'гибридной войне'. Независимое военное обозрение", 29 Mayıs 2015.
[101] Renz, a.g.m., ss.14-15

Günümüz çatışma ortamını tanımlamak üzere kullanılan popüler bir terim olarak Hibrit savaşın savaş kavramına getirdiği değişimi Newman'ın savaşın değişen doğasını açıklamakta kullandığı altı değişken faktör üzerinden değerlendirerek konuyu toparlayabiliriz. Newman bu değişken faktörleri 1. Taraflar, 2. Çatışmanın temel nedenleri, temel motivasyon unsuru, 3. Coğrafyası ya da çatışma alanı, 4. Uygulanan yöntem ve silahlar, 5. Sosyal, yapısal ve insani etkileri ve 6. Politik ekonomi ve sosyal yapısı olarak sıralamaktadır.[102] Newman'ın altı değişken faktörlerine göre incelendiğinde;

(1) Taraflar: Günümüz çatışma ortamında her ne kadar devletlerin devletlerle çatışmalarında azalma, iç savaş, silahlı devlet dışı aktörler, paramiliter gruplar, özel askerî şirketler, terör ve suç örgütleri, ayaklanan milis güçler üzerinden devletlerin diğer silahlı unsurlar ile veya başka devletlerin bu diğer silahlı unsurları vekil olarak kullanarak çatışmalarda rol aldığı örneklerde artış gözlenmekte ise de 2022'de Rusya Federasyonu'nun Ukrayna'yı işgali devletler arası savaşın da halen devam eden bir olgu olduğunun ispatı olarak tarih sahnesinde yerini almıştır. Savaşan taraf olmasalar da günümüz çatışmalarından en çok etkilenenlerin siviller olduğunu söylemek yanlış olmaz. Chesterman günümüzde savaş zayiatının %80'ini sivillerin oluşturduğunu söylerken gerek mağduriyete gerekse bu zayiatın neden olduğu mülteci sorunlarına da çatışma alanının dinamikleri içinde dikkat çekmektedir.[103] Çatışma alanı içinde silahlı veya silahsız mücadele eden unsurların yanında, politik çıkarlar ve bölge üzerindeki emelleri gereği çatışan taraflara destek sağlayan diğer ülke, örgüt veya diasporanın rolüne de makro çerçevede göz ardı edilmemelidir.

(2) Çatışmanın temel nedenleri, temel motivasyon unsuru: Belli bir ideolojiyi yaymanın ötesinde, günümüzde çatışmanın ana nedenini hegemon devletlerin başka bir coğrafyada kendi politik hedeflerini dikte etme gayreti temel motivasyon unsuru olarak gözlemlenmektedir. Hedef alınan ülkede yönetimi ele geçirme ya da kendi politikalarını kabul ettirecek şekilde baskı altına alma

[102] Edward Newman, "The 'New Wars' Debate: A Historical Perspective Is Needed", *Security Dialogue*, C. 35, S. 2 (2004): 173–89, https://doi.org/10.1177/0967010604044975 [Erişim Tarihi: 19.04.2022].

[103] Simon Chesterman ve Angelina Fisher, "Introduction", *Private Security, Public Order The Outsourcing of Public Services and Its Limits*, der. Simon Chesterman, London: Oxford University Press, 2009, 2.

günümüzde ön plana çıkmaktadır. Hedeflenen ülkede, iktidarı bu kapsamda yönlendirmek üzere istihbarat teşkilatları ve özel kuvvetler gibi örtülü faaliyet gösterebilen unsurlarca desteklenen muhalif unsurların kışkırtılmasından, sivil itaatsizlik ve gösteriler ile silahlı direnişe kadar varabilen halk hareketleri organize edilebilmekte ve örtülü şekilde desteklenebilmektedir. Hatta, politik hedeflere ulaşmak üzere hedef ülkedeki iç karışıklık ve savaş bahane edilerek terörle mücadele, davet üzerine hâkim otoritenin desteklenmesi veya barış gücü kisvesi ile silahlı güç kullanmak da dâhil olmak üzere askerî müdahalede bulunulabilmektedir. Hedef ülkenin yönetimi üzerinde söz sahibi olunmasının yanında, etnik veya dini bağlar gerekçe gösterilerek belirli coğrafi bölgelerin de ilhakının amaçlanabildiği gözlemlenmektedir.

(3) Çatışmanın coğrafyası ya da çatışma alanı: Günümüzde çatışma savaş meydanlarından insan unsurunun bulunduğu tüm coğrafyaya yayılmıştır. Kara, deniz ve hava olmak üzere üçe ayrılan harekât alanları, uzay, bilgi, siber alanları da kapsayacak şekilde insan odaklı bir şekilde çok tabanlı bir hal almıştır. Silahlı mücadele arazi ve tahkim edilmiş mevzilerden, meskûn mahaller de dahil olmak üzere insanın bulunduğu her alana sirayet etmiştir. Çatışmanın belli bir bölge veya ülke ile sınırlı kalma kısıtı olmaksızın etkilerinin bölgesel ve hatta küresel boyutlara ulaşabildiğine sıkça şahit olunmaktadır.

(4) Çatışmada uygulanan yöntem, silah ve teknolojiler: Çoğunlukla konvansiyonel olmayan düzensiz unsurlar ile mücadelede konvansiyonel unsurlar desteğinde yine düzensiz savaş stratejileri ön plana çıkmakta olsa da 2022 Ukrayna-Rusya çatışmasında son noktanın yine sert güç kullanımının uluslararası ilişkilerde daima bir seçenek olduğu gözler önüne serilmiştir. Günümüz güç mücadelesi her ne kadar asimetrik, düzensiz, mahdut veya kısıtsız stratejiler üzerinden yürütülmeye çalışılsa da son noktada mekanize/zırhlı birlikler, yüksek ateş gücü ve kan ile sonuçlandığına tanık olunmaktadır.[104] Devlet dışı silahlı unsurların, çeşitli şekillerde temin ettikleri normalde silahlı kuvvetler envanterinde bulunan yüksek hassasiyet ve ateş gücüne sahip silahlar ile siber, elektronik harp vb. diğer teknolojik yetenekler ile kullandıkları bombalı araç,

[104] Seth Cropsey, "Wither Hybrid War", *Real Clear Defence*, 2022, 3.

el yapımı patlayıcılar, modifiye edilmiş dronların kullanımı gibi taktikler ile çatışma ortamında asimetrik etki yarattıkları gözlenmektedir.

(5) Çatışmanın sosyal, yapısal ve insani etkileri: Düzensiz unsurlara karşı yürütülen mücadelelerde bu unsurların uyguladıkları taktik ve teknikler doğrultusunda gizlenmek, yüksek ateş gücüne sahip orduları yan hasar riski kaygısını kullanarak kısıtlamak maksadıyla sivil varlığı ile kendini perdelemeye çalışması günümüz çatışmalarını meskûn mahallere taşımıştır. Sivil varlığı ile kendini perdelemeye çalışan düzensiz unsurları sivillerin çatışma alanını terk etme çabalarını engellemeye çalıştıkları çokça rastlanan bir durumdur. Bununla birlikte; güvenliğini tehdit altına gören toplulukların çatışma alanlarından göçleri de yerinden edilmişler veya mülteciler sorunu olarak günümüz çatışma alanının ve bu alanı çevreleyen bölgelerin önemli bir sorunu haline gelmiştir. Kontrolünün zorluğu nedeniyle bu mülteci grupların barındığı kamp alanlarının terör örgütlerince kullanılması, sınır geçen mülteciler arasında örgüt mensuplarının da sınırlardan geçmeleri, yine günümüz çatışma ortamının dinamikleri içinde ayrı bir soru alanını oluşturmaktadır. Meskûn mahallere taşınan çatışmalar, harp hukuku ile bağlı düzenli orduları istihbarat, gözetleme ve keşif yetenekleri ile desteklenen hassas hedefleme kabiliyetlerine mecbur bırakmaktadır. Tüm bunların yanında, aşırı şiddet kullanımı ile korku yaratarak topluluklar üzerinde otorite oluşturmak üzere gerek terör örgütleri gerek otoriter rejimler gerekse işgalci güçlerce sivillere karşı bilinçli olarak güç kullanılması günümüz çatışmalarının bir karakteristiği olarak karşımıza çıkmaktadır [105]. Sivil halk, barınma alanları ve şehir alt yapısına yöneltilen bu tür güç kullanımı ise, etkisi çatışma/savaşın çok daha sonrasına uzanacak yıkımı beraberinde getirerek sivil mağduriyetini artırmaktadır.

(6) Çatışmanın politik, ekonomik ve sosyal yapısı: Uluslararası hukuk ile yasaklanan güç kullanma ve güç kullanma tehdidine rağmen, uluslararası hukukun bu konuda tanıdığı istisnai durumlar ile boşlukların suiistimali ile hegemon ülkelerin etki alanı içindeki diğer ülkeler üzerinde savaş ilanına varmayacak ölçüde şiddet eşiğini aşmadan güç kullanması, yaratılan politik

[105] Mary Kaldor, "Wanted: Global Politics." The Nation, no. Kasım 2001, 99.

> baskının hedef ülke halkının ve uluslararası kamuoyunun algısını şekillendirecek dezenformasyon ve propagandaları kapsayan bilgi harekâtı ile desteklenmesi sıkça karşımıza çıkmaktadır. Algı üzerine yoğunlaştırılan çabalar ile hedef ülkenin diplomasi alanında yalnız bırakılması, bununla birlikte enerji, ticaret gibi alanları da kapsayacak şekilde ekonomik yaptırımlar ile yürütülen politikaların desteklenmesi günümüz güç mücadelesinde norm oluşturmaya başlamıştır. Silahlı güç kullanımı veya caydırıcılığını tüm milli güç unsurları ile destekleyen tüm bu unsurların birlikte kullanımdan isim bulan 'Hibrit Savaş', sert ve yumuşak güç kullanımı arasında köprü oluşturmaktadır.[106] Günümüz güç mücadelesinin ana eksenini tanımlamaya çalışan ve güç mücadelesini savaş ilanı eşiği altında tutarak yürütme odaklı hibrit savaşın bu seviyede kalmak zorunda olmadığı hatırdan çıkartılmamalıdır. Rusya'nın Ukrayna'ya askerî müdahalesi ile; çatışmayı destekleyen bileşenlerin melezliği, hibritliği, detaylı planlama ile politik hedefleri destekleyecek şekilde eşgüdüm içinde icrası savaşın karakteristiğini değiştirmemiş, sert güç kullanımı savaş/çatışma kavramı içinde baskın yerini koruduğunu göstermiştir.[107]

Günümüz savaşı; çatışmanın belli bir bölgeden küresel bir niteliğe kavuşmasına, klasik uygulamalardan daha modern teknolojilerin de etkisi ile daha çağdaş bir anlayışa, devlet tekelinden devlet dışı aktörler üzerine ağırlığın kaymasına, asker odaklı uygulamalardan sivilleşmeye, hukukilikten uluslararası hukukun boşluklarını suiistimal ile hukuk dışılığa, farklı harekât ortamlarında eşgüdüm içerisinde ve tüm aktörlerin birlikte detaylı bir planlama, risk analizi ile senkronize bir şekilde icrası ile kompleksleşen melez, hibrit bir güç mücadelesine dönüşmüştür. Hibrit savaş terimi ile kavramlaştırılmaya çalışılan çatışma tipinde aktörler, kullanılan araçlar ve tarafların politikaları doğrultusunda uyguladıkları stratejiler son derece durumsal ve netlikten uzaktır. Bu bağlamda Münkler'in asimetrikleşmeyi merkeze koyan değerlendirmesi, uygulayan devletten bağımsız olarak, tüm büyük güç odaklarının mücadelesinin temelini oluşturması bakımından öne çıkmakta ve gününüz çatışma ortamının odak noktasını ortaya koymaktadır.[108] Dördüncü nesil savaş kavramı ile düzensiz, gayrı

[106] Diego A. Ruiz Palmer. Back to the Future? Russia's Hybrid Warfare, Revolutions in Military Affairs, and Cold War Comparisons. (Research Paper-NATO Defense College, Sayı: 120, 2015), 2. https://www.files.ethz.ch/isn/194718/rp_120.pdf [Erişim Tarihi: 23.05.2022].
[107] Cropsey, a.g.e., 1.
[108] Münkler, a.g.e., 2005, 224.

nizami silahlı mücadeleleri ön plana çıkartan Lind'in yaklaşımlarına da günümüz çatışma ve güç mücadelesini tanımlamakta kullanılan hibrit savaş kavramını anlamada sıklıkla baş vurulmakta ve tartışılmaktadır.[109]

Bileşenlerine bakıldığında politik-stratejik seviye bir mücadele olduğu aşikâr olan hibrit savaşta yöntem ve kullanılan araçlar yerine hasmın amaçlarına odaklanmak, düşmanın niyetini, hedeflerini tespit ederek, bunları kullandığı araçlar ile ilişkiyi anlamak ana stratejiyi oluşturmalıdır.[110] Bu alandaki savaşın sisini stratejik istihbarat kaldırmaya çalışırken, saha da yürütülen mücadeleyi anlamaya yönelik olarak operatif ve taktik istihbarat faaliyetleri eşgüdüm içerisinde yürütülmelidir.

2.6. Değişen Harekât Ortamının Getirdiği Yeni Doktrin İhtiyacı

Sebepleri politik ve stratejik olan hibrit tehditlerle mücadele, yine sebeplerinin sosyal ve beşerî şartların analizi ile oluşturulacak politikalar ile yapılmalıdır. Ancak günümüzde çözüm arayışlarının güç kullanımını gerekli kılan durumlarla karşı karşıya kalındığı da ortadadır. Bu mücadeleler, düzensiz unsurlarla birlikte bileşik harekât kabiliyetine sahip düzenli birliklerce icra edilecek yeni nesil bir teşkilatlanma, zihniyet ve müşterek harekât doktrinini gerekli kılmaktadır.[111]

Tarihsel süreç içerisinde değişen ve gelişen savaş, tarafların mücadeleyi icra ediş şekillerini belirleyen doktrinleri de tehdidin şekline ve uyguladığı taktik ve tekniklere göre değiştirmiştir. Çok tabanlı yeni muharebe ortamı ile önümüzdeki dönemde de karşılaşılacak olması, konvansiyonel muharebeler için tasarlanmış ordular, komuta kontrol ve karar destek sistemleri (istihbarat da dahil olmak üzere karar verme sürecini destekleyen tüm sistemeler) başta olmak üzere tüm fonksiyon alanlarının her seviyede (taktik, operatif ve stratejik) yeni doğan harekât ihtiyaçlarını karşılamada yeterli kalamayacağı değerlendirilmektedir.[112]

Son derece dinamik günümüz harekât alanında; organizasyonel ataletini yenen, yüksek uyum kabiliyetine sahip, değişen harekât ortamı içinde değişen askerî ihtiyaçlara

---

[109] William S. Lind, *On War: The Collected Columns of 2003-2009,* London: Castalia House, 2009.
[110] Robert Johnson, "Hibrit Tehdidin Tarihsel Evrimi", *Hibrit Savaş; Savaşın Değişen Modeli* (İstanbul: Milli Savunma Üniversitesi Basımevi, 2018), 1.
[111] Gültekin Yıldız, "Hibrit Savaş Ne Kadar Post-Moderndir? Avrasya Askerî Tarihine Yeniden Bakış", *Hibrit Savaş; Savaşın Değişen Modeli* (İstanbul: Milli Savunma Üniversitesi Basımevi, 2018), 26.
[112] Ali Bülent Uşaklı ve İrfan Hasan Alper. "Teknolojik Gelişmelerin Savaşları Dönüştürmesi ve Gelecekteki Savaşlara Hazır Olmak", *Savaş: Farklı Disiplinlerde Yeni Yaklaşımlar*, der. Haldun Yalçınkaya, (Ankara: Siyasal Kitap Yayın-Dağıtım, 2010), 43.

yenilikçi çözümler getirebilecek, diğer kurum ve kuruluşlarla iş birliği içinde çalışabilen silahlı kuvvetlerin başarı sağlayabileceği öngörülmektedir.[113] Tarihsel gelişim içinde incelediğimiz gibi, teknolojik gelişimin öncülük ettiği değişim ve siyasal konjonktür çerçevesinde değişen savaş ile döneme göre uygulanan strateji ve doktrin de değişiklik göstermiştir. Birçok kaynakta son konvansiyonel savaş olarak gösterilen 1991 Körfez savaşında geliştirilerek hayata geçirilen "Etki Odaklı Harekât" ve birbirleri ile ağ üzerinden haberleşen kuvvetlerin müşterek harekât doktrini tanımlayan "Ağ Merkezli Harekât" öne çıkmış, savaşın değişimi çerçevesinde devlet dışı tehditlerin çatışma ortamına damga vurması ile "Düzensiz Savaş", diğer devlet kurumlarının da çatışma alanına desteğini içeren "Tüm Devlet Yaklaşımı" ve çok katmanlı hale gelen günümüz harekât alanının tüm boyutlarında mücadeleyi esas alan "Çok Tabanlı Harekât" yaklaşımlarını sırasıyla incelemekte fayda vardır.

2.6.1. Etki Odaklı Harekât (Effect Based Operation) ve Ağ Merkezli Harekât (Network Centric Warfare)

1990-1991 Körfez Savaşında ortaya atılan ve takip eden dönemde doktrinel çerçevesi çizilen Etki Odaklı yaklaşım, karşı tarafta oluşturulmak istenen etkinin belirlenmesini müteakip bu etkiyi oluşturacak en uygun aracın kullanılmasını öngörmektedir. Arzu edilen stratejik sonuç veya etkiyi elde etmek üzere askerî veya askerî olmayan (Politik, ekonomik, sosyal, vb.) imkânların askerî çabaları destekleyecek şekilde etkileşim içinde sinerji oluşturacak şekilde kullanımı amaçlanmaktadır. Daimî bir durumsal farkındalık sağlamak üzere sürekli harekâtı takip eden bir değerlendirme mekanizması ile elde edilmek istenen etki, istenmeden oluşan ve olumsuz etki doğuran sonuçlar ve istenilen etkiyi oluşturmaya yönelik taktik faaliyetlerin tespiti amaçlanmaktadır. Klasik yaklaşıma göre harekâta farklı bir bakış açısı getiren bu doktrin, düşmana zayiat veya fiziki tahribat yerine etki odaklı harekât anlayışı elde edilmek istenen sonuca odaklanmaktadır. Örneğin psikolojik harekât, elektronik harp, düşman lojistik sisteminin sekteye uğratılması gibi diğer ölümcül olmayan uygulamalarla düşmanın moralini bozarak, savaşma azim ve iradesini kırarak mağlup etmeyi amaçlarken sivil zayiatı ve savaş tahribatını da asgariye indirmeyi amaçlamaktadır.[114] Etki odaklı harekât doktrini kesin sonuçlu ölümcül muharebeyi ortadan kaldırmadan, komutanlar

[113] a.g.e., 39.
[114] Edward Smith, *Effect Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War*, (Washington DC: CCRP Publication, 2002), 25.

için bir seri farklı seçeneği ortaya koyan daha bütüncül bir bakış açısını muharebe sahasına taşımıştır. Konseptin dikkat çekici noktası, barış, kriz dönemi, harekât ve harekât sonrası dönemleri kapsamasıdır. Gerek savaş öncesi ve sonrasındaki savaş dışı dönemleri kapsaması, gerekse askerî unsurlarla birlikte, stratejik hedefe ulaşmak üzere askerî olmayan fonksiyon alanları ve aktörlerin de kullanımına değinmesi günümüzün çatışma ortamında rastladığımız uygulamaların ilk örnekleri olarak dikkat çekmektedir.[115]

Bir arazi parçasının ele geçirilmesinin ötesinde politik hedefi elde etmeye yönelik etki üzerine odaklanan bu yeni anlayış, muhabere ve komuta kontrol sistemleri ile müşterek durumsal farkındalık sağlayarak, bilgi tabanı üzerinden harekât resmini oluşturarak harekât alanında kara, hava, deniz ve özel kuvvetlerin eş güdüm ve müşterek harekâtına imkân sağlayan Ağ Merkezli Harekât doktrini ile kullanılmaya başlanmıştır. Ağ merkezli harekât yaklaşımı, düşmanı da iç içe geçmiş sistemler bütünü olarak görmekte, düşmanın etkin muharebesini sekteye uğratmak adına komuta kontrol sistemlerini de öncelikli etki altına alınacak hedefler arasında önceliklendirmiştir.[116] Askerî ve askerî olmayan metotların kinetik harekât anlayışı ile sınırlı kalmayacak şekilde senkronize ve hedefe ulaşmak için istenen etkiyi yaratmaya yönelik kullanımını temel alan yönüyle düşünüldüğünde etki odaklı ve ağ merkezli yaklaşımın hibrit savaş anlayışının erken versiyonunu oluşturduğu yorumunu yapmak yanlış olmayacaktır.[117]

2.6.2. Düzensiz Harekât (Irregular Warfare)

Savaşın gelişimi ve dönüşümü içerisinde doktrinel gelişim ve dönüşüm de birbirinin üzerine inşa edilerek devam etmiştir. Öncesinde de var olsa da özellikle Körfez Savaşını takip eden dönemde terör örgütlerinin çatışma alanındaki artan varlığı, özellikle de 11 Eylül 2001 saldırısı sonrasında ilan edilen küresel terörle savaş kapsamında düzensiz unsurlar ile mücadele etmede, müşterek harekât icra etme yetenekleri ile desteklenen özel kuvvetler odaklı bir doktrin öne çıkmıştır. ABD

---

[115] Allen Batscheley, *Effects-Based Operations: A New Operational Model?*, (US Army War Collage: US Army Publication, 2002), 2-4. https://web.archive.org/web/20070927213243/http://www.iwar.org.uk/military/resources/effect-based-ops/ebo.pdf [Erişim Tarihi: 16.01.2023].

[116] Paul T. Mitchell, "Network Centric Warfare and Coalition Operations: The New Military Operating System", *Routledge*, (2009): 34-39, https://doi.org/10.4324/9780203881163 [Erişim Tarihi: 19.04.2022].

[117] Karabulut, a.g.m., 29.

Savunma Bakanlığı'nın Kongre'ye sunduğu 2006 tarihli Savunma Raporunda; Konvansiyonel ordular dışındaki düzensiz örgütler ile mücadelenin yeni çatışma modeli olduğu ve bu bağlamda silahlı kuvvetlerin bu tip konvansiyonel olmayan ve dolaylı yaklaşımlar ile arzu edilen stratejik hedefe ulaşmak üzere etki odaklı bir yaklaşımı bütünleştiren yeni doktrini benimsemenin yeni çatışma ortamı içinde bir gereklilik olduğu vurgulanmaktadır.[118]

Rapor; ABD Silahlı Kuvvetlerinin düzensiz savaş ortamına adaptasyonu için kurumsal ve yönetimsel reform, düzensiz harekât doktrininin adaptasyonu, bu stratejiyi hayata geçirmek üzere bölgesel partnerlerin oluşturulması, toplum ve uluslararası kamuoyu algısını şekillendirmek üzere "Stratejik İletişim" ve bu unsurlara gerekli desteğin sağlanabilmesi için istihbarat yapılanmasının şekillendirilmesinin yol haritasını ortaya koyan ve Savunma Bakanlığına dönüşüm için direktif veren kilit bir doküman niteliğindedir. Ayrıca; düzensiz unsurların küresel güvenliği tehdit ettiği dönüşen güvenlik ortamında ABD Silahlı Kuvvetlerinin, istihbarat teşkilatları ile sinerji içerisinde; terörist ağları ile mücadelesini, ülke savunmasının tehdit ana kıtaya varmadan uzaktan sağlanmasını, (Siyasi ve) stratejik dönüm noktasında bulunan ülkelerin seçeneklerinin yönlendirilmesini, hasım ülke ve devlet dışı aktörlerin kitle imha silahlarını kullanımlarının engellenmesini stratejik hedef olarak koymaktadır.[119] Bu bağlamda, istihbarat teşkilatları ile özel kuvvetler üzerinden gerek devlet dışı düzensiz tehditlerle kinetik mücadele ederken, gerekse ilgi alanındaki bölgelerde ülkelerin siyasi tercihlerini kendi politikaları doğrultusunda şekillendirmeye yönelik kinetik olmayan çabaları hedefleyen bir politikayı ortaya koymaktadır. Bu faaliyetlere örnek olarak; terörle mücadele kapsamında Afganistan, Irak ve Suriye'de devam eden terörle mücadele koalisyon harekâtları ile, Kuzey Afrika ve Ortadoğu coğrafyasında batı yanlısı yönetim ve ulusal politika değişikliklerini beraberinde getiren renkli devrimler gösterilebilir.

ABD politikalarının, başat rolü oynadıkları ittifaklardan güç aldığı, NATO başta olmak üzere bölgesel ve ikili iş birliği içinde olunan ülkelerin de bu yeni doktrinel yaklaşımı benimsemelerinin önemine değinilmektedir.[120] ABD ile eş eksenli güvenlik

[118] US Department of Defense, "Quadrennial Defense Review Report", *Quadrennial Defense Review: Assessing U.S. Defense and Security*, (Washington DC: 2006): 1-3. https://www.airforcemag.com/PDF/DocumentFile/Documents/2006/QDR2006_020606.pdf [Erişim Tarihi: 06.05.2023].
[119] a.g.r., 19.
[120] a.g.r., 6.

politikaları yürüten diğer batılı devletlerin de ittifak içerisinde ya da ulusal olarak benzer bir doktrin benimsedikleri ve bölgesel ya da koalisyon içinde bu doktrini özellikle 11 Eylül saldırılarını takip eden dönemde hayata geçirdikleri gözlemlenmiştir. Ayrıca ilgilenilen bölgelerde insani yardımlar ile yazılı ve görsel medya, son dönemde ise sosyal medya aracılığıyla halkın algısının şekillendirilmesi ile hedeflenen politikaların dolaylı yaklaşım ile kabul ettirilmesi yolu düzensiz harekât yaklaşımının sıklıkla gözden kaçırılan ancak önemli bir unsurunu oluşturmaktadır.

2.6.3. Bütüncül Devlet Yaklaşımı (Whole of Government Approach)

Bu doktrinel dönüşüm ile özellikle terörle mücadelede bütün devlet kurumlarının iş birliği, iletişim ve eş güdüm içerisinde sinerjik etki sağlayacak şekilde çalışmasını amaçlayan Bütüncül Devlet Yaklaşımı (Whole of Government Approach) benimsenmiştir. İstihbarat teşkilatları ile desteklenen özel kuvvetler ağırlıklı bu düzensiz harekât doktrininin devlet kurumları ve bu bağlamda milli güç unsurları ile desteklenmesi, günümüze kadar gelişmiş ve açıklamaya çalıştığımız günümüz çatışma ortamı ya da popüler tabiri ile hibrit harekât ortamını şekillendirmiştir. İstihbarat teşkilatları ve özel kuvvetler üzerinden icra edilen gizli/örtülü kinetik veya kinetik olmayan faaliyetler, günümüzde makul inkâr edilebilirlik kapsamında gri alan aktiviteleri olarak icra edilmeye devam etmektedir.[121]

2.6.4. Çok Tabanlı Harekât Doktrini (Multi Domain Operations)

Büyük güç mücadelesi içinde çekişmenin sadece askerî boyuttan askerî olmayan alanların da dahil olması ile genişlediği ve derinleştiğini, mücadelenin farklı fonksiyon alanlarında olduğu gibi farklı boyutlara taşındığını görmekteyiz. Özellikle teknolojik gelişmelerin değişim ve gelişimi sürüklediği günümüz çatışma/mücadele ortamında bilgi işleme gücü, otomasyon, kuantum hesaplama (Quantum computing), makine öğrenmesi ve yapay zekâ yeni silah sistemlerini mümkün kıldığı gibi harekâtın yeni şekillerde icrasına da imkân sağlayacaktır. Çok büyük miktarlardaki verinin işlenmesine imkân sağlayarak, ortak harekât resminde dünyanın neresinde olursa olsun askerî yeteneklerin gizlenmesini zorlaştıracaktır. Bu teknolojik gelişmelerle insansız sistemlerin otonom veya insanlı sistemlerle entegre şekilde uygulamaya geçmesi, hipersonik yeteneklerin, uzun menzilli balistik sistemlerin ve uzaya konuşlu

[121] Cormac ve Aldrich, a.g.m., 493.

sistemlere karşı geliştirilen sistemlerin mücadele ortamına dahil olması beklemektedir. Çatışmaların yaşam alanlarına yaklaşması, insan faktörünün gerek taktik seviyede gerekse stratejik seviyede harekâta etkisinin artması, harekât alanının tecridini sağlayan sistemlerin hayata geçmesi ise modern silah ve sensör sistemlerinin hassas vuruş kabiliyetlerinin ve menzillerinin geliştirilmesini zorunlu kılmıştır. Silah sistemlerinin hız ve menzillerinin artması, atıldıkları platformların deniz altında uzaya kadar çeşitlenmesi, çatışma alanına kinetik olmayan vasıtalarla da etki edilebilmesi sınırların bulanıklaşmasını sağlamıştır. Sadece harp silah, araç ve gereçlerinin değil, bilgi işlem kapasitesinin de son derece hızlanması zamanda hassasiyeti zorunlu kılmış, muharebenin ritmi ve karar verme – icra arasındaki süre kısalmış, daha dinamik, ön alıcı (pre-emptive) ve gereken yerde gerekli yetenekleri hazır bulundurmak günümüz çatışma alanının gerekliliği olarak ön plana çıkmıştır.[122]

Bir bölgede nüfuzunu artırma çabasındaki küresel veya bölgesel güçlerin, o bölgedeki istikrarı bozmaya yönelik olarak ekonomiyi, politik ve sosyal yapıyı bozmaya, ulusal birliği zayıflatmaya yönelik askerî olmayan gayretleri kullandığı, bu faaliyetleri savaş ilanına sebep olmayacak seviyede şiddet organize ederek iç karışıklık çıkartarak ve bu iç karışıklıklara alınan tedbirleri suiistimal ederek güç kullanımına temel oluşturma gayreti içinde oldukları gözlemlenmektedir. Bunları yaparken askerî caydırıcılığın azami kullanıldığı, inkâr edilebilir seviyede gri alanda müdahaleci ülke adına faaliyet gösteren örtülü ve/veya devlet dışı silahlı aktörlere destek sağlanmakta, hedef bölgeye diğer ülkelerin nüfuz etmesini engellemeye yönelik olarak da bölge hava savunma, elektronik harp ve diğer vasıtalarla tecrit edilmektedir. Örneğin Rusya tarafından literatüre ve uygulamaya sokulan; harekât alanının kara, hava ve denizden tecridine dayalı bir bölge kontrol konsepti olan Erişimi Engelleme ve Bölge Tecridi (Anti Access Area Denial – A2AD)[123] benimsenmektedir. Çok ortamlı bir tecrit anlayışını ifade eden bu yeni strateji, hasmın kontrol edilen bölgenin dışında tutulmasını ve müdahalesini kısıtlamayı hedeflemektedir. Rusya kaynaklı bir doktrin olmakla beraber, belli bir ülkeden bağımsız olarak harekât alanın tecridi, günümüz çatışmalarının temel öğesini oluşturmaktadır.

[122] Development Concepts and Doctrine Centre, "UK Multi-Domain Integration - Joint Concept Note 1/20", (London: UK Ministry of Defence, 2020): 6-7. https://www.gov.uk/government/publications/multi-domain-integration-jcn-120 [Erişim Tarihi: 16.01.2023].

[123] Anti Access – Area Denial – A2AD konsepti için; https://warontherocks.com/2019/09/its-time-to-talk-about-a2-ad-rethinking-the-russian-military-challenge/

Tüm bu teknolojinin sürüklediği gelişmeler ve muhtemel hasım ülkelerin güç mücadelesi içinde değişen ve gelişen stratejileri ile konvansiyonel savaştan düzensiz savaşa evrilen askerî doktrinin, müşterek yetenekleri kaybetmeden, partner unsurlar ve diğer ülkelerle ittifak içinde birleşik harekâtı yeteneklerinin geliştirilmesi ihtiyacı ortaya çıkmıştır. İnsan faktörünün artan rolü ve gelişen teknolojiler neticesinde daha önce güç mücadelesinde rol almayan alanların kinetik mücadeleleri desteklemekte kullanılmaya başlanması klasik kara-deniz-hava harekât tabanlarına yenilerinin eklenmesini zorunlu kılmış, çağın gerekliliklerini karşılayacak yeni nesil bir teşkilatlanma, zihniyet ve müşterek harekât doktrini ihtiyacı doğmuştur [124].

Gelişmeler ışığında günümüz güç mücadelesinin yürütüldüğü ortamların, harekât tabanlarının (Operational Domains) tanımlanması ve sınıflandırılması ihtiyacı ortaya çıkmıştır. İstihbaratı destekleyen gözetleme sistemleri atmosferin dışına taşmış ve uzay; güç ve nüfuz mücadelesi içinde olan büyük devletler için harekâtlarını destekleyecekleri yetenekleri konuşlandırabilecekleri bir diğer harekât ortamı olarak 2019 yılı haziran ayında icra edilen NATO Savunma Bakanları toplantısında üzerinde uzlaşılan NATO Uzay Siyasası ile bir harekât tabanı olarak kabul edilmiştir.[125] İnsanın artan önemi ve etkisi neticesinde bilgi, bilgi teknolojilerinin insan hayatı ve karar destek sistemleri ile iletişim üzerindeki artan ağırlığı neticesinde siber, iletişim ve istihbarat toplama yeteneklerinde artan önemi ile elektromanyetik harekâta katkı sağlayan alanlar olarak doktrine dahil edilmiştir. NATO Müttefik Müşterek Harekât Doktrini harekât tabanlarını fiziki (kara, deniz, hava ve uzay) ve fiziki olmayan (bilgi, elektromanyetik, siber, zaman) olarak sınıflandırmaktadır.[126] Birleşik Krallık harekât tabanlarını deniz, kara, hava, uzay, siber ve elektromanyetik olmak üzere altı alanda incelemektedir.[127] Bunlara ilave olarak, kitleleri etkileyen bilginin (Information) ve günümüz muharebe sahasının önemli aktörlerinden devlet dışı silahlı örgütlerin çatışma içinde oldukları yüksek teknoloji ve yıkım gücüne sahip ülke ordularının

[124] Yıldız, a.g.e., 26.
[125] NATO, "NATO's Approach to Space", North Atlantic Treaty Organization, 2021, https://www.nato.int/cps/en/natohq/topics_175419.htm [Erişim Tarihi:17.05.2022].
[126] NATO, "Allied Joint Doctrine for the Conduct of Operations (AJP-3)", *NATO Standardization Office* (Brussels: NATO Standardization Office, North Atlantic Treaty Organization, 2019), 1-3. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/797323/doctrine_nato_conduct_of_ops_ajp_3.pdf [Erişim Tarihi:17.05.2022].
[127] UK Ministry of Defence, "UK Terminology Supplement to NATOTerm (2019 Edition)." (London: Joint Doctrine Publication 0-01.1, 2019), 43. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1138055/20230220-JDP_0_01_1_2023_Edition_A.pdf [Erişim Tarihi: 06.05.2023].

gözünden ve etkilerinden korunmak için kullanmaya başladıkları yer altı [128] ve askerî olmayan unsurların güç çekişmesinde ağırlığının artması ile önemi artan 'insan ve algı' faktörünün[129] de yeni bir harekât ortamı/tabanı olarak kabul edilmesi gerektiği tartışılmaya başlanmıştır.

Farklı askerî ve sivil, devlet ve özel aktörleri ile çeşitlenen harekât ortamlarında müştereklik ve silahlı kuvveler ile diğer devlet kurumları arasında eş güdüm sağlamak çeşitlenen harekât tabanlarında sinerji yaratacak, müttefik veya partner diğer ülkeler ile entegre edilebilecek Çok Tabanlı Harekât Konsepti ilk olarak 2016 yılında ABD Kara Kuvvetleri tarafından gündeme getirilerek geliştirilmeye başlanmıştır. Müşterek kara-hava/deniz-hava müşterek harekât anlayışının zihni bir halefi olarak ortaya çıkan yaklaşım, 2018 yılında ABD Savunma Bakanlığınca doktrinel bir ulusal savunma konsepti olarak telaffuz edilmeye ve geliştirilmeye başlanmıştır.[130] Önce eleştirilen ve günümüz harekât alanında önemi azaldığı düşünülen konvansiyonel kara kuvvetlerinin bilgi çağında umutsuz bir girişimi olarak eleştirilen bu konsept, zamanla önce ABD Savunma Bakanlığı, sonrasında da Birleşik Krallık, ardından NATO bünyesinde diğer ittifak ülkelerince kabul gören ve geliştirilmeye devam edilmektedir. Bu yeni doktrin; günümüz çatışma ortamında tüm devlet kurumları ile eşgüdüm ve sinerji içerisinde, tüm harekât tabanlarında müştereklik ve diğer ülkeler ile birleşik harekât icra edecek şekilde birlikte çalışabilirliğe uyumlu günümüz çatışma ortamında karşılaşılacak tehdit ve gereklilikleri karşılayacak, askerî ve sivil çabaları tüm alanlarda bütünleştirecek bir bakış açısını yansıtmaktadır.

Çok tabanlı harekâtın tüm savunma bakanlığı bağlılarını kapsayan konsepti niteliğindeki giren yeni Müşterek Savaşma Konsepti (Joint Warfighting Concept) Haziran 2021'de ABD Savunma Bakanı tarafından imzalanarak yürürlüğe girmiş, yayınlanan stratejik direktif ile kuvvet komutanları bileşenleri ile, 2013 tarihinde yazılan ve 2017'de güncellenen müşterek harekât doktrinin yerini alacak yeni doktrini oluşturma çalışmalarına başlamışlardır.[131] ABD'nin Çok Tabanlı Harekât Doktrinini

[128] Patrick Tucker, "'Underground' May Be the U.S. Military's Next Warfighting Domain", *Defense One*, (2018). https://www.defenseone.com/technology/2018/06/underground-may-be-us-militarys-next-warfighting-domain/149296/ [Erişim Tarihi: 16.08.2023].
[129] François du Cluzel, "Cognitive Warfare", *Innovation Hub*, (2020), 25-28. https://www.innovationhub-act.org/content/cognitive-warfare#:~:text=Cognitive [Erişim Tarihi: 16.01.2023].
[130] Andrew Feickert, "Defense Primer : Army Multi-Domain Operations (MDO)", *Focus*, (2021). https://sgp.fas.org/crs/natsec/IF11409.pdf [Erişim Tarihi: 15.05.2022].
[131] A.g.ç., tekrar bkz.

2022 yazında onaylayarak yürürlüğe geçirmesi beklenmektedir.[132] Birleşik Krallık Silahlı Kuvvetleri de benzer çok tabanlı bir müşterek konsepti onaylama 2020 yılında ortaya koymuş ve hayata geçirmeye yönelik çalışmaları halen sürdürmektedir.[133]

Günümüz güç mücadelesini barış döneminde devam eden çekişme (Compete), çatışma dönemi içinde sızma, savunmayı çözme, başarıdan faydalanma (Penetrate, Dis-integrate, Exploit) ve çatışma sonrası barışın yeniden sağlanması ile yeniden çekişme (Re-compete) olarak üç ana dönemdeki mücadeleleri kapsaması ön görülmektedir.[134] Bu üç ana dönemde ise mücadelenin; (1) Söylem mücadelesi, yani silahlı kuvvetlerin sadece caydırıcılık ile destekleyeceği, ülkenin uluslararası kamuyu nezdinde itibarı, gücü, saygınlığı, güvenilirliğini destekleyecek politikalar ile gerçekleştirilecek mücadele, (2) Doğrudan mücadele, yani silahlı unsurlar ve tüm yetenekler ile düşük yoğunluklu savaş eşiğinin altındaki faaliyetlerden, top yekûn savaşa kadar uzanan bir yelpazede kinetik ve kinetik olmayan unsurlar ile mücadele, (3) Dolaylı mücadele, yani hedefin avantajlı durum elde etmek (hasmı bundan mahrum bırakarak) üzere düzensiz unsurlar başta olmak üzere gerekli tüm yeteneklerden istifade ile, vekil kuvvetler ve dolaylı yaklaşımlarla politika yapıcılara seçenekler sunacak olmak üzere düşük ve orta yoğunlukta güç kullanımı ve risk ile mücadele olmak üzere üç şekilde gerçekleşeceği değerlendirilmektedir.[135]

Bu yeni müşterek harekât konseptinde;

- Barış ve kriz döneminden itibaren süregelen "Çekişme (Compete)",
- Hasım sistemlerine ve kontrol ettiği harekât alanına "Sızma (Penetrate)",
- Bu alanı kontrol eden ve savunan sistemlerin işleyişini aksatarak dost unsurların manevrasına imkân sağlayan 'Çözme (Dis-integrate)',
- Bu sayede ortaya çıkartılan açıkların suiistimal edilerek sağlanan hareket serbestisi ile düşmanın her harekât ortamında/tabanında yenilerek operatif ve stratejik hedeflerin ele geçirildiği 'Suiistimal (Exploit)',

[132] Jen Judson, "Multidomain Operations Concept Will Become Doctrine This Summer", *Defense News*, (2022). https://www.defensenews.com/land/2022/03/23/multidomain-operations-concept-will-become-doctrine-this-summer/ [Erişim Tarihi: 15.05.2022].
[133] Development Concepts and Doctrine Centre, a.g.r., 2-5.
[134] TRADOC, *The U.S. Army in Multi-Domain Operations 2028- TRADOC Pamphlet 525-3-1*, (Washington DC: U.S. Army Training and Doctrine Command, 2018), 24-25. https://api.army.mil/e2/c/downloads/2021/02/26/b45372c1/20181206-tp525-3-1-the-us-army-in-mdo-2028-final.pdf [Erişim Tarihi: 06.05.2023].
[135] Andrew Feickert, a.g.m., 1.

- Zaferle elde edilen kazanımların her bir ortam/tabandaki kabiliyetleri geliştirmekte kullanıldığı 'Mücadelenin Devamı' (Re-Compete) safhalarını içeren yeni bir müşterek harekât konsepti üzerinde durulmaktadır.[136]

Günümüzde muharebe gücünün temelini oluşturan Tugay Muharebe Grubu yapısından, çok tabanlı harekât konsepti kapsamında fiziki harekât tabanlarının yanında, bilgi tabanlarının (bilgi, siber, elektromanyetik) müşterek diğer yetenekleri ve diğer kamu kurum/kuruluşları ile eş güdüm sağlamak üzere irtibat hücreleri ile desteklenen Tümen ve Kolordu karargâhlarının tarihte olduğu gibi muharip rollerine yeniden kavuşmaları değerlendirilmektedir. Tehdit algısının bölgelere göre farklılık göstermesi nedeniyle ABD silahlı kuvvetleri bu doktrini küresel sorumluluk sahalarını bölüştürdüğü beş Bölgesel Komutanlık (Theater Command) bünyesinde oluşturulacak Çok Tabanlı Görev Kuvveti (Multi-Domain Task Force) yapılanması ile hayata geçirmeyi planlamaktadır [137]. Bahse konu çok tabanlı doktrinin diğer ülkelerce benzer bir mantık ile, etki ve ilgi alanlarına göre farklılıklar gösterecek, ittifak ülkeleri ile uyumlu ancak milli yapılarda teşkil edilmeleri beklenmektedir. Örneğin; Hindistan'ın tehdit algısı doğrultusunda Çin'e karşı, Çin tarafından benimsenen "Kısıtsız Savaş Doktrini" odaklı bir yaklaşım ile çok tabanlı harekât doktrinini şekillendirmesi, ancak ABD Pasifik Komutanlığı ile olası iş birliğini de sağlayacak şekilde birlikte çalışabilir olması batılı yaklaşımlardan farklı bir uygulama olarak değerlendirilebilir.[138]

Bu çok tabanlı harekât ortamına yönelik çalışmalar, ilk ABD tarafından kodifiye edilmiş olsa da bugünü değil, geleceği düşünen tüm ülkelerce incelenmekte ve geleceğin muharebe sahasında başarıyı vaat edecek konsept ve müşterek harekât doktrininin oluşturulmasına yönelik çalışmalar yapılmaktadır. Günümüz muharebe sahasındaki gelişmelerden yola çıkarak, takip eden 10-20 yıllık geleceğe çıkarım yapan bu yeni müşterek harekât anlayışının genel esasları dikkate alındığında harekâtın ne kadar teknoloji ile entegre hale geldiğini, bu entegrasyonun artarak devam edeceğini, hasım kontrolündeki harekât bölgesine sızma, hasmın savunma yeteneklerinde gedik açmak ve bu gedikleri başarı için suiistimal etmek için hangi

[136] TRADOC, a.g.r., 25.
[137] Feickert, a.g.m., 2.
[138] Manabrata Guha, "Multi-Domain Warfare: Waging Unrestricted Warfare", (2019), 7-13. https://www.researchgate.net/publication/331771727_Multi-Domain_Warfare_Waging_Unrestricted_Warfare [Erişim Tarihi: 15.05.2022].

seviyede bir durumsal farkındalık sağlamak için nasıl bir istihbarata ihtiyaç uyulacağı konusunda düşünmemek mümkün değildir.

Bu doktrinel değişim sürecinin teknolojik gelişmeler ışığında yeni yetenekler ve yenilikçi bakış açıları ile gelişmeye devam etmesi beklenmelidir. Bu yenilikçi bakış açısı ile, geliştirilen konseptlerin yeni teknolojilerin kaynaştırılması ile mevcut kabiliyetleri geliştirecek, sürekli bir değişim içinde olan günümüz mücadele ortamının gereksinimlerini karşılayabilecek, hatta şekillendirecek seviye yakalanması hedeflenmelidir.[139] Bu bağlamda karar vericilerin durumsal farkındalığını sağlama, sürprizleri önleme, hasmın savaşma azim ve iradesini kıracak hareket tarzlarının üretilmesinde önemli bir role sahip olan istihbarat alanının da incelediğimiz günümüz harekât alanının ihtiyaçlarını karşılayacak şekilde dönüşüm içinde olması beklenmelidir.

[139] Uşaklı ve Alper, a.g.e., 49.

3. İSTİHBARATIN DÖNÜŞÜMÜ

3.1. İstihbaratın Tarihsel Süreçte Gelişimi ve Dönüşümü

Büyük güç çekişmesi ve uluslararası çatışma ortamı bağlamında askerî istihbarat ve onu destekleyen disiplinler çerçevesinde sınırlandırdığımız çalışmada, savaşın değişen karakteri ile şekil değiştiren çatışma ortamında derinleşen ve genişleyen güç kullanımı ve onu kodifiye eden doktrinel gelişmeler öncelikli olarak incelenmiştir. Güvenlik ortamı ve çok tabanlı, askerî / sivil çok bileşenli günün güç mücadelesini destekleyen unsurların başında şüphesiz karar alma sürecine önemli katkı sunan istihbarat gelmektedir. Tarihi süreçte değişimi ve dönüşümü incelenen çatışma ortamı ile stratejiye yön veren istihbarat da çağın ve çatışma ortamının gereksinimleri karşılamak üzere dönüşüm içerisindedir.

Napolyon döneminde zorunlu askerlik ve seferberlik sisteminin hayata geçirilmesi ile millileşen ordular, ülke kaynaklarından daha fazla istifade ile, daha uzun soluklu ve daha fazla cephede muharebe etme imkânı sağlamaya başlamış ve modern anlamda savaş anlayışının başlangıcı kabul edilmiştir.[140] Bu dönemde istihbarat ise; casusluk ile hasmın harekât planlarını ele geçirmek ve liderlerin kendileri ile aile bireylerinin korunmasına yönelik çabaların ötesine geçmemiştir. İstihbaratın önemli bileşenlerinden olan ve bilgi güvenliğini esas alan İstihbarata Karşı Koyma (İKK), ancak İngilizlerin 1889'da yürürlüğe koyduğu, askerî bilgileri sızdıranlara karşı cezai yaptırımlar hükmeden 'Resmî Gizlilik Yasası' ile istihbarat kavramı içinde yer bulmuştur. Modern savaş istihbaratının bu erken döneminde veri/bilgi toplama vasıtaları da bu bağlamda casuslar, diplomatlar ve gazeteci gibi açık kaynaklarla sınırlı kalmıştır. İngiltere ile Güney Afrika'yı kolonileştiren Boer'ler arasındaki ikinci Boer Savaşı ise istihbarat servislerinin oluşumu için önemli bir kilometre taşını oluşturmaktadır. Daha önce harekât alanındaki komutanlara ihtiyaç duydukları bilgiler çeşitli askerî fonksiyonlarca sağlanmaktayken, bu savaş sürecinde birliklere 'savaş

[140] Owen Comelly, Blundering to Glory: Napoleon's Military Campagins (Lanham, MD: Rowman & Littlefield, 2006).

istihbaratı subayları', karargâhlara ise 'istihbarat subayları' atanmıştır. İngiliz deniz ve kara kuvvetleri arasında kablosuz iletişimin kullanılmaya başlaması ve bu sinyallerin bazılarının Boer'lar tarafından yakalanarak kullanılması ise sinyal istihbaratının ilk örneklerini oluşturmuştur. Savaş süresince bu yeni istihbarat teşkillerince toplanan bilgilerin miktarındaki artış, bu bilgileri analiz etmek ve ihtiyaç sahiplerine dağıtmakla görevli oluşumları ortaya çıkartmıştır. Savaşın sonrasında bu ihtiyaç ortadan kalksa da İngilizler Savunma Bakanlığı bünyesinde küçük bir İstihbarat Departmanını hayatta tutmayı başarmışlardır. Britanya adasında Alman casusluk tehdidinin artması ile; yabancı istihbarat çabaları ile mücadele ve Birleşik Krallığın potansiyel düşmanları hakkında bilgi toplamak üzere, MI5 ve MI6'nın temellerini oluşturacak Gizli Servis Bürosu'nu kurmuş ve bu alanda dev bir adım atılmıştır.[141]

ABD Ulusal İstihbarat Konseyi eski başkanı Treverton; istihbarattaki ilk büyük dönüşümü Jomini ve Clausewitz'in tanımladığı yeni askerî anlayış kapsamında değerlendirir.[142] Birçok akademisyen tarafından tüm milli güç unsurlarının seferber edildiği, savaş alanının pek çok teknolojik yenilikle (Uçakların, gelişmiş muhabere vasıtaları, şifre sistemleri ile bu gizli muhaberelerin dinlenmesi ve şifre çözme yetenekleri v.b.) tanıştığı, Birinci Dünya Savaşı istihbarat alanındaki en büyük atılımların yapıldığı mihenk taşı olarak kabul edilmektedir.[143]

İkinci Dünya Savaşı ise tüm istihbarat çabalarının tek bir çatı altında birleştiği Ulusal İstihbarat Sistemi'nin ilk uygulamaya geçirildiği modern istihbarat anlayışının başlangıcı olarak kabul edilir. Bu modern istihbarat anlayışının;

(1) Toplama yeteneklerinde, özellikle muhabere istihbaratı (COMINT) ve radar ağırlıklı elektronik istihbarat (ELINT) de dahil olmak üzere sinyal istihbaratı (SIGINT) yeteneklerindeki gelişmeler,
(2) Savaşan unsurların başındakiler de dahil olmak üzere karar vericilerin istihbarat ile desteklemesine imkân sağlayacak şekilde organizasyonel yapıların gelişmesi,
(3) İstihbarat disiplinine yönelik bilgi birikiminin artması ile karargâhlara verdikleri desteğin organizasyon içinde kabul görmesi,

[141] Herskovitz, a.g.e., 3-4.
[142] Gregory F. Treverton, "The Future of Intelligence: Changing Threats, evolving methods". *The Future of Intelligence Challenges in the 21st Century*. ed. Isabelle Duyvesteyn, Ben de Jong ve Joop van Reijn. New York: Routledge, 2014, 33.
[143] Herskovitz, a.g.e., 5.

(4) İstihbarat anlayışının sadece durumsal farkındalık sağlamanın ötesinde, psikolojik harekât, ekonomik harp ve sabotaj gibi harekât ortamını değiştirecek şekilde genişlemesi olarak sıralanabilecek dört ana alanda gerçekleştiği söylenebilir.

Modern istihbarat anlayışının genişlemesi ve harekâta sağladığı desteğin artması kapsamında dikkat çekici uygulamalar arasında ABD'nin 1941'de Bilgi Koordinasyon Ofisini (Office of Coordination of Information) Almanya'nın Sovyetler Birliğini işgaline yönelik olarak bir istihbarat, dezenformasyon ve propaganda ajansı olarak kurması örnek olarak gösterilebilir. ABD Bilgi Koordinasyon Ofisi; ortak nihai hedefe yönelik olarak görev tanımı net olarak oluşturulmuş ilk istihbarat teşkili olması nedeniyle önemli bir adım olarak gösterilmektedir. İlk etapta harekâta yönelik istihbarat ihtiyaçlarını koordine etmek üzere kurulan oluşum, 1942'de; daha sonra Merkezi İstihbarat Ajansı (CIA)'na dönüşecek olan Stratejik Hizmetler Ofisi (OSS) ve daha sonra ABD Bilgi Ajansı (USIA)'na dönüşecek Savaş Bilgi Ofisi olarak ikiye bölünmüştür.[144] ABD Bilgi Ajansı propaganda ve dezenformasyon odaklı çalışırken, Stratejik Hizmetler Ofisi (OSS); casusluk, sabotaj, yıkıcı faaliyetler ve propaganda ile ABD'nin askerî gayretlerini desteklemekle memur edilmiştir.[145]

İstihbaratın gelişiminde teknolojik gelişmelerin rolünü tabiki göz ardı etmek mümkün değildir. Savaş öncesinde, klasik istihbarat anlayışı içinde toplama gayretlerini casuslar, diplomatlar ve açık kaynaklar domine ederken, savaş ile radarların ve kablosuz iletişimin kullanımının yaygınlaşması ile sinyal istihbaratı yeteneklerinin ağırlığını artırdığı gözlenmektedir. Uçakların yaygınlaşması hava harekâtlarının önemini artırırken, uçakların gözetleme, fotoğraf ve bu görsellere dayalı analiz ile istihbarat alanını da desteklediği görülmektedir.

Toplama vasıtalarının artması, elde edilen verilerin işlenmesi, analizi ve dağıtımını bir problem sahası olarak o tarihlerden itibaren ortaya çıkartmaya başlamıştır. Bu durum istihbarat teşkilatlarını yeni bir alana yönlendirmiştir. Öngörü istihbaratı (Estimative Intelligence) olarak tanımlanan ve elde edilen veriler ışığında yapılan

[144] John Houseman, *Front and Center (1942-1955)* (New York, Simon & Schuster, 1975), 45-46.
[145] Office of Strategic Services, Office of Strategic Services Organization and Functions, (Washington DC: Hyperwar Foundation, 1945. https://www.ibiblio.org/hyperwar/USG/JCS/OSS/OSS-Functions/index.html [Erişim Tarihi: 22.04.2023].

değerlendirmelerle ihtimalleri ortaya koymayı amaçlayan bu alan, karar vericilere strateji ve politika belirlemede taban oluşturabilecek girdiği sağlamaktadır.[146] Bu alan, Merkezi İstihbarat Ajansı'nın (CIA) kuruluşundan beri var olan Analiz Direktörlüğü (Directorate of Analysis) gibi istihbarat teşkilatlarında benimsenmiş ve kurumsallaşmıştır. Diğer departman ise Harekât Direktörlüğüdür (Directorate of Operations) ki ABD dışında istihbarat toplama, sabotaj, yıkıcı faaliyetler, psikolojik harekât gibi diğer faaliyetlerden sorumludur. Ajansın kuruluşunu takip eden yıl, Bilimsel İstihbarat Ofisi'nin, ajans bünyesindeki çeşitli birimlerin birleştirilmesi ile kurulması teknolojinin istihbarat alanındaki giderek artan önemine yönelik ciddi bir öngörüyü işaret etmektedir.[147]

1950'li yıllarda Merkezi İstihbarat Ajansı (CIA) ABD'nin Sovyetler Birliğine karşı yürüttüğü tüm faaliyetlerin merkezinde yer aldığı, istihbarat teşkilatının soğuk savaş döneminde ana enstrüman olarak öne çıktığı gözlenmektedir. Bu dönem; "teknolojik toplama devrimi" olarak da ifade edilmesini sağlayan önemli projelerle dikkat çekmektedir. 1954'te kapsamlı elektronik istihbarat sisteminin, 1956'da U2 casus uçağının, 1960'ta ise Corona casus uydu sisteminin devreye girmesi bu teknoloji istihbarat anlayışının ürünleridir. Teknolojinin toplama yeteneklerini desteklemesi doğal olmakla birlikte belki daha da önemli olan husus, bu zamana kadar alışılmış uygulamaların dışında bu atılımın özel şirketler üzerinden yapılmış olmasıdır. İstihbaratın özelleşmesindeki ilk adımlardan sayılabilecek bu projeler özel sektörün özellikle teknolojinin istihbarat fonksiyonuna entegrasyonu üzerinden dahil olacağının ilk sinyallerini vermiştir. Bu projeleri Merkezi İstihbarat Ajansı (CIA) içinde organizasyonel yapılanmalar takip etmiş, 1948'de Bilimsel İstihbarat ofisi kurulmuş, daha sonra Ajans içindeki teknoloji odaklı çeşitli departmanlarla birleşerek Bilim ve Teknoloji Direktörlüğü olarak teşkil edilmiştir.[148]

Bu teknolojik devrim, istihbarat sisteminin içinde bulunduğu ortamın değişimi içinde yetersiz kalışının ilk işaretlerini iki alanda göstermiştir. İlki; belirsizliği ortadan kaldırmak üzere bilgiye bağımlılığın oluşması ve sistemin sürekli daha fazla veriye

---

[146] Arthur S. Hulnick, "Harold P. Ford, Estimative Intelligence: The Purposes and Problems of National Intelligence Estimating", *Journal of Conflict Studies*, C. 14, S. 1 (1994), 2-3. https://journals.lib.unb.ca/index.php/JCS/article/view/15167 [Erişim Tarihi: 15.08.2023].

[147] Jeffrey T. Richelson, *The Wizards of Langley: Inside the CIA's Directorate of Science and Technology*, (Cambridge: 2002), 24-26.

[148] Herskovitz, a.g.e. 8-9.

ihtiyaç duymasıdır. İkincisi ise; teknolojik gelişmelerle artan toplama yeteneklerinin ABD'nin güç çekişmesinde ihtiyaç duyduğu her bilgi ihtiyacını karşılamaya yetecek olma algısı olarak öne sürülmektedir. Yeni teknolojilerin cazibesi ile karar vericiler ve onlara istihbarat sağlayanlar, stratejik ve jeopolitik sorunların çözümünün yorumlama ve anlamlandırmada yattığını göz ardı ederek, çözümü daha fazla veri toplamada aramışlardır. İnsanlığın pek çok sorununun teknoloji ile çözüleceği algısı, teknolojik determinizmin bir yansıması olarak görülmektedir.[149] Geçen yetmiş yılda yaşanan pek çok stratejik sürprizin nedeninin bilgi yetersizliğinden ziyade bilginin yorumlanarak tedbir alınmamasından kaynaklandığı pek çok akademisyence kabul edilse de hâlâ teknolojinin her sorunun çözümü olduğuna inananların bulunması, bu bilgi bağımlığının ve teknolojik determinizmin etkisinin halen devam ettiğinin göstergesidir.

Sovyet bloğunun çöküşü soğuk savaşı sonlandırmış, ABD; 'Yeni Çağ' olarak nitelendirilen, bilgi çağında istihbaratın işleyişine yönelik küçülmeyle birlikte, sensör teknolojileri, bilgi-işlem ve internet sayesinde bilgiye erişim artan yeni bir anlayış ve yapılanma değişimini hızlandırmıştır. 1996 yılında yayınlanan 'Bilgi Harekâtı' FM 100-6 dokümanı ile 'Bilgi Üstünlüğü (Information Superiority)' olarak adlandırılan anlayış ve istihbarat işleyişini tanımlayan yeni doktrin uygulamaya geçirilmiştir. Sensör tabanlı istihbarat sistemlerini muharebe sistemleri ile bir ağ vasıtası ile entegre eden ABD, o yıllarda 'Ağ Merkezli Savaş' doktrini ile dikkat çekmiş, bu yeni doktrini Körfez Harbinde de uygulamıştır.[150] Sovyet bloğunun çöküşü ile güvenlik algısındaki değişim ve teknoloji destekli istihbarat ile desteklenen kendini Körfez Harbinde kanıtlamış yeni harp doktrini, istihbarat topluluğunun küçülmesi gerektiği yönündeki görüşün kuvvetlenmesine yol açmıştır. ABD İstihbarat Topluluğunu temsil eden Aspin-Brown Komisyonu 1996 tarihli raporunda; soğuk savaş sonrasında kaynakların son derece azalırken, personel giderlerinin artmaya devam ettiğine, bu durumun ise teknolojiye yatırım yapılması ve fonksiyonel esnekliğin yitirilmesine yol açtığını vurgulamıştır.[151] Rapor, bir takım yapısal dönüşümün gerekliliğinin yanında,

[149] Leo Marx, Merritt Roe Smith, *Does Technology Drive History? The Dilemman of Technological Determinizm*, (Cambridge: MIT Press, 1994), 94-95.
[150] Richard M. Bridges, Information Operations: FM 100-6 (Fort Levenworth, US Army, 1996, 11.
[151] ODNI, *Preparing fort he 21st Century: An Appraisal of U.S. Intelligence: Report of the Commission on the Roles and Capabilities of the United States Intelligence Community*, (Washington, DC: Government Printing Office, 1996.

kısıtlanan bütçe nedeniyle teknolojiyi yakalamanın da gerisinde kalındığını vurgulaması adına önemli bir öz eleştiri niteliğindedir.

11 Eylül 2001'deki terör saldırıları ise; istihbarat topluluğu da dahil olmak üzere ABD dış ve savunma politikası ile ulusal güvenlik yapılanmasında önemli yapısal, işlevsel ve anlayışsal değişimi tetiklemiştir. ABD'deki Terör Saldırılarına İlişkin Ulusal Komisyon raporu[152], ABD Başkanının Federal Soruşturma Bürosu (FBI) ve Merkezi İstihbarat Ajansı (CIA) tarafından 'yeterli bilgilendirilmediği' yönünde tespitlerine yer vermiştir.[153] Saldırı sonrasında bir takım yapılanma değişikliklerine giden ABD İstihbarat Topluluğu; Ulusal İstihbarat Direktörlüğü Ofisi'nin (ODNI) tüm istihbarat çabalarını senkronize etme rolü ile kurulması ve ikisi bağımsız (ODNI ve CIA) olmak üzere çeşitli bakanlıklar altında teşekkül edilmiş toplam 18 istihbarat ajansının işleyişini düzenlemesi ile süreç içerisinde günümüzdeki yapıya evrilmiştir. 2002 tarihli Ulusal Güvenlik Strateji Raporu, teknolojik gelişmeleri de işaret ederek, yeni tehdit olarak en ön plana çıkan terörizme karşı reaksiyon süresini kısaltmak adına istihbarat çabaları ile harekâtın entegrasyonun gerekliliğini vurgulamaktadır. Ayrıca terörizmle mücadeleye yönelik olarak kurulan departman ve direktörlüklerin birbirleri ile koordineli çalışmasının önemine dikkat çekilmiş ve işleyişe ilişkin düzenlemelere ışık tutmuştur.[154]

2001 sonrası dönem, tehdit algısının değişinin yanında, daha önce karşılaşılmamış bir şekilde bilgi teknolojilerindeki gelişim ve sosyal ağların yaygınlaşması ile bir bilgi selini beraberinde getirmiştir. Teknolojik bakış açısıyla, özellikle bu dönemin sonlarına doğru, çok çeşitli kaynaklardan elde edilen çok çeşitli bilginin farklı fonksiyon alanlarının bakış açılarıyla derin analizlerine odaklanmış ve 'Çoklu İstihbarat (Multi-Int)' olarak kavramsallaştırılmıştır. Başlarda istihbarat gayretlerini askerî yetenekler ve gereksinimler sürüklerken, 2010 sonrası dönemden itibaren bilgi teknolojileri ve sosyal ağların yaygınlaşması ile artan verinin işlenmesi üstün bilgi-

[152] National Commission on Terrorist Attacks upon The United States, *The 9/11 Report*, (Washington DC: 2002).; National Commission on Terrorist Attacks upon The United States, '9/11 Komisyonu' olarak da anılmaktadır.
[153] John Shovelan, *9/11 Commission Finds 'Deep Institutional Failings*, Australian Broadcasting Corporation, 2006, https://www.abc.net.au/am/content/2004/s1160100.htm [Erişim Tarihi: 06.05.2023].
[154] US Presidency, *The National Security Strategy of the United States 2002*, (Washington DC: The White House, 2002), 29-35. https://web.archive.org/web/20100307072859/http://georgewbush-whitehouse.archives.gov:80/nsc/nss/2002/nss.pdf [Erişim Tarihi: 15 Ağustos 2023].

işlem yeteneklerini ve analiz yöntemlerini beraberinde getirmiştir. İnsanlar; yaratıcı kavramsal ve algısal tekniklerin kullanarak trendleri algılama, paternleri fark etmeleri ve bunlara dayalı çıkarımlarla sınırlıyken; gelişen bilgi-işlem yetenekleri insan kapasitesini aşan veriyi analiz etmede görselleştirmesi, istatistiki çıkarımları ve mekânsallaştırması bakımından üstünlük sağlamaktadır. Veriyi anlamak üzere görselleştirmenin yanında SAS, SPSS, Minitab gibi yazılımlar vasıtasıyla istatistiki çıkarımlarla anlamlandırmak ise analiz yeteneklerine ayrı bir boyut katmıştır. Bu analizlerin coğrafi bilgi sistemleriyle de entegrasyonu, verinin bir mekâna, coğrafyaya oturtulabilmesi ile de daha anlamlı hale gelmesi sağlanmaktadır ki trend ve paternlerin mekân ve zaman bağlamında analizine 'zaman-mekansal analiz (spatiotemporal analysis)' denilmektedir.[155] Günümüzde artan verinin analizi insan yeteneklerinin üzerine çıkmaktadır. Büyük verinin analizinin hızlı ve etkin analizinin bilgi teknolojileri ile yapılması, insanların ise güçlü olduğu hipotezleme ve ilişkilendirme ile analizi tamamlayacak şekilde istihdamı anlam kazanmaktadır.[156]

Biltgen ve Ryan, istihbaratın dönüşümünü anlatılan akış ile uyumlu olarak 4 dönem olarak ele almıştır. Bu sınıflandırmada;

- İkinci Dünya Savaşı sonrasında Komünizmin yükselmesi ile insan istihbaratı ağırlıklı, tek tehdide odaklanmış ve istihbaratın ayrı bir alan olarak kabul edildiği 1911-1962 yılları arası ikinci dönem,
- 1962-2001 yılları arasında soğuk savaş ve ulus devletler arasında tek tehdit odaklı teknik toplama yeteneklerinin ağırlığını artırdığı ikinci dönem,
- 11 Eylül terör saldırıları sonrasında tehdit algısının değişimi ile, terörizm ve bölgesel çatışmalara odaklanan, bilgi teknolojileri, insansız hava vasıtaları, ağ üzerinde işleyen istihbarat ve muharebe komuta sistemlerinin ön plana çıktığı, ABD ana-kıtasının tehdide maruz kaldığı üçüncü dönem,
- 2014 sonrasında terörizm, siber tehdit ve toplu imha silahlarının tehdit algısında yerini aldığı, Çoklu İstihbarat ve Büyük Veri Analitiklerinin ön plana çıktığı, yaygın bir istihbarat paylaşım ve entegrasyonunu tanımlayan

[155] Patrick Biltgen, Stephen Ryan, *Activity-Based Intelligence: Principles and Applications*, (London: Artech House, 2016), 24-25.
[156] Hershkovitz, a.g.e., xii.

bütünleşmiş bir istihbarat anlayışının yerleştiği dördüncü dönem olmak üzere tehdidin değişimi ve bu bağlamda istihbaratın dönüşümü sınıflanmaktadır.

2014 ortasından itibaren ağırlığı gittikçe artan çoklu istihbarat anlayışı, çeşitlenen tehdit, çatışma ortamındaki (çok boyutlu ve çok aktörlü) artan değişim bu dönemi domine etmektedir. Bilgi teknolojilerindeki sıçrama, telekomünikasyon ağı ile insanlığın birbirine bağlanması, konum-bilinçli hizmetler, akıllı telefonlar ve yaygın mobil bilgi işlem yetenekleri de değişimin önünü açan faktörlerdendir. Bu tarihten itibaren teknoloji yoğun çoklu istihbarat anlayışı istihbarat fonksiyonunu domine ederken, karar vericilerin gerçek zamanlı bilgi akışı talepleri istihbaratçılar üzerinde 'ne olabileceğini tahmin etme' konusundaki baskıyı artırmaktadır. Bu baskı, çeşitlenen tehdit ve azalan kaynaklarla daha da artmakta, istihbarat kurumlarını ihtiyacı karşılamak üzere farklı çözüm yolları aramaya zorlamaktadır.[157]

ABD Ulusal İstihbarat Direktörlüğü Ofisince yayımlanan ABD Ulusal Strateji Raporlarını incelediğimizde bu anlayışsal değişimi kolayca gözlemleyebilmekteyiz. 2005 raporu terörizmle mücadele odaklı bir anlayışla bilgi paylaşımına yönelik yeni sistemleri işaret ederken kurumun analitik yeteneklerinin de geliştirilmesine dikkat çekmektedir. 7 kurumsal hedefin ikisi teknoloji odaklıdır. Bunlardan biri; açık kaynak da dahil olmak üzere toplama yeteneklerinin geliştirilmesi ve tüm istihbarat kurumlarında teknolojinin daha iyi kullanımının sağlanması, ikincisi ise; yeni nesil teknolojilerin analiz sürecine entegre edilmesi kapsamında merkezi yönetilebilen fakat âdem-i merkeziyetçi uygulamalara müsaade eden ortak (uniform) bir işleyiş oluşturulmasıdır.[158]

2009 raporunda; radikal şiddet öncelikli, toplu imha silahları ikincil tehdit ve istihbarat topluluğu için hedef olarak belirlenirken, sırasıyla stratejik istihbarat ve erken ikaz, karşı istihbarat, ABD veri altyapısının siber saldırılara karşı güvenliğinin artırılması

[157] Biltgen, Ryan, a.g.e., 1-22.
[158] ODNI, *National Intelligence Strategy Report 2005*, (Washington DC: 2005), 7. https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/NISOctober2005.pdf , [Erişim Tarihi: 17.08.2023].

ve askerî harekâtın desteklenmesi önceliklendirilmiş istihbarat istekleri/hedefleri olarak listelenmektedir.[159]

Önceki yıllardan farklı olarak 2014 ve 2019 yıllarında yayımlanan rapor ise istihbarat topluluğu için sıraladığı 7 hedefte; ABD ulusal güvenliğine yönelik tehditler doğrultusunda stratejik istihbarat, öngörü ve erken ikazı desteklemek üzere istihbarat faaliyetlerine ilk iki sırada yer verirken, harekâtların desteklenmesi, devlet ve devlet dışı aktörlerce oluşturulan siber tehdit, terörizm devlet ve devlet dışı aktörlere uygulanabilecek toplu imha silahı kullanımı riski ve karşı istihbarata daha düşük önceliklendirdiği görülmektedir.[160]

2023 yılı raporunda ABD Ulusal İstihbarat Direktörlüğü Ofisi; istihbarat topluluğunun zamanında ve isabetli değerlendirmelerle lisan, kültürel uzmanlık, açık kaynaktaki büyük veriyi işleme, yapay zekâ ve ileri analitik yöntemler alanlarında yeteneklerini geliştirerek güç mücadelesinde yerini sağlamlaştırmasını öncelikli hedef olarak belirlemiştir. İkinci öncelik olarak, istihbarat topluluğunun başarısının yetişmiş, yetenekli insan kaynağına bağlı olduğuna dikkat çekerek işe alma, istihdam ve terfi sistemlerini geliştirerek personel kalitesini artırmanın önemine dikkat çekmiştir. Bu öncelikleri;

- Kurumlar arası ve uluslararası iş birliği kapsamında birlikte çalışabilirlik ve yenilikçi yöntemlerin hayata geçirilmesi,
- Diğer ülke ve alanda söz sahibi özel şirketler ile iş birliğinin geliştirilmesi, çeşitlendirilmesi ve güçlendirilmesi,
- Teknik yeteneklerin geliştirilmesi,
- Dış tehditlere karşı istihbarata karşı koyma tedbirlerini de kapsayacak şekilde istihbarat topluluğunun direncinin artırılması takip etmektedir.

Rapor, ABD istihbarat topluluğunun etkinliği ve dayanıklılığı için teknolojik gelişmelerin yakalanması, yetişmiş personel ve özel şirketler de dahi olmak üzere iş birliğinin geliştirilmesini kritik görmekte ve 2023 yılı stratejik istihbarat hedefleri

[159] ODNI, *National Intelligence Strategy Report 2009*, (Washington DC: 2009), 5. https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2009_NIS.pdf [Erişim Tarihi: 17.08.2023].
[160] ODNI, *National Intelligence Strategy Report 2019*, (Washington DC: 2019), 7. https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf [Erişim Tarihi: 17.08.2023].

olarak yayımlamıştır.[161] Yıllara sarih bu önceliklendirme değişimi, teknolojik gelişmelerin istihbarat topluluğunun görev ve önceliklerini nasıl etkilediğinin de göstergesi olarak kabul edilmelidir.

Davies ve Steward; batılı istihbarat anlayışının, modern istihbarat örgütlerinin ilk tesis edilmelerinden itibaren en büyük temel değişimi ve dönüşümü yaşadığını ifade ederek bu süreci; (1) Değişen ve dönüşen güvenlik anlayışını kavramış açık bir hükumet anlayışı, (2) gelişen toplama ve analiz yeteneklerindeki olağanüstü gelişim ile birlikte, "bilmesi gereken" prensibinden "paylaşılması gereken" prensibine doğru bir iş birliği anlayışına doğru bir anlayış/algısal değişim, (3) uzayı da kapsayacak şekilde gözetleme ve keşif yeteneklerindeki gelişim, (4) açık olarak erişilebilen verideki artış neticesinde önemi ve etkinliği her geçen gün artan Açık Kaynak İstihbaratı olarak gruplandırmaktadır.[162]

İstihbaratın dönüşümünün evrensel olduğunu öne sürmek bir iddianın ötesine geçmemektedir. Bölgesel dinamikler ile son derece ilişkili olan istihbarattaki değişimin; algılanan iç ve dış tehdide, diğer ülkeler ile ilişkilerin durumuna, silahlı kuvvetlerin seviyesine, ülkenin mevcut ve geleceğe dair hedeflerine göre değişiklik göstermesi mutlak bir gerçektir.[163] Çıtak, istihbarattaki dönüşümün; **istihbarat anlayışındaki dönüşüm**, **yöntemlerde dönüşüm** ve **yapısal dönüşüm** olmak üzere üç ana başlık altına toplanabileceğini öne sürmektedir.[164]

3.1.1. Anlayışsal Dönüşüm

Uluslararası ilişkilerdeki geleneksel güvenlik anlayışı sadece devleti merkezi almakta ve devlete yönelik askerî tehditlere odaklanmaktadır. Fakat 1980'lerden itibaren Kopenhag Barış ve Çatışma Araştırmaları Enstitüsü, uluslararası güvenlik çalışmaları alanında geleneksel anlayışın dışına çıkmıştır. Zira, Soğuk Savaş'ın bitmesinden sonra iki kutuplu dünya düzeni değişmiş; teknolojik olanaklar gelişmiş, iletişim ve ulaşımda büyük dönüşümler yaşanmıştır. Dolayısıyla bu gelişmeler güvenlik kavramının da

---

[161] ODNI, *National Intelligence Strategy Report 2023*, (Washington DC: 2023), 5-15. https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2023.pdf [Erişim Tarihi: 17.08.2023].

[162] Phillip H. J. Davies, Toby Steward. "No War for Old Spies: Putin, the Kremlin and Intelligence" *RUSI*, (2021) https://rusi.org/explore-our-research/publications/commentary/no-war-old-spies-putin-kremlin-and-intelligence [Erişim Tarihi: 19.05.2022].

[163] Michael Herman, "Ethics and Intelligence After September 2001", *Intelligence and National Security*, C. 19, S. 2, (2004), 355.

[164] Emre Çıtak, *Güvenlik ve İstihbarat: Yeni Güvenlik Politikaları ve Türkiye'de İstihbaratın Dönüşümü*, (İstanbul: Yeni Yüzyıl Yayınları, 2017), 185-207.

genişlemesine ve derinleşmesine sebep olmuştur. Diğer bir deyişle bireylerin, devlet dışındaki grupların ve toplumların güvenliği ön plana çıkmış ve güvenlik konusu kabul edilen alanların sayısı artmıştır. Dolayısıyla eskiden askerî alanda taktik, operasyonel ve stratejik istihbarata ihtiyaç duyulurken; güvenliğin genişlemesi ve derinleşmesiyle siyaset, ekonomi, çevre, sosyal yapı, demografi gibi pek çok alanda istihbarat ihtiyacı ortaya çıkmıştır. Bu durum, istihbaratın sivilleşme sürecini başlatan, güvenliği ilk önemli tetikleyici olmuştur.

Güvenliği için kişisel hak ve özgürlüklerinde kısıtlamalara gidilmesini kabullenen toplum, güvenlik-özel hayatın gizliliği ikilemini gündeme getirmekle birlikte, güvenlik için özel hayatın mahremiyetinden bir ölçüde feragat edilmesi **toplumsal anlayış değişikliğine** örnek teşkil etmektedir. Devlet dışı aktörlerin yarattığı tehditler sınır tanımadan küresel güvenliğe meydan okuma yanında, Rusya'nın Kırım'ı ilhakı ile daha çok hissedilmeye başlanan gerginlik, istihbarat alanında da ittifakların öneminin farkındalığına ve istihbarat gibi mahrem sayılan bir alanda devletler arası iş birliğinin öneminin artmasına yol açmıştır. NATO gibi ittifakların yanında, ABD, Birleşik Krallık, Kanada, Avusturalya ve Yeni Zelanda arasında bir istihbarat ortaklığı olan 'Five Eyes'a Japonya'nın ortaklık talebi bu anlayış değişiminin örneklerinden biri olarak gösterilebilir.[165] Bunun yanında; siber uzayın öneminin artması, istihbaratın bir bilim dalı olarak evrilmeye başlaması, istihbarat kavramının askerî mücadelenin dışında fonksiyon alanları ile zenginleşmesi, hesap verebilirliğin öneminin artması gibi bileşenler günümüz tehdit ve güvenlik ortamında istihbaratın algı boyutundaki değişiminin bileşenlerini oluşturmaktadır.[166]

Lowenthal bu anlayış değişimi kapsamında istihbaratın önceliklerinin ülkeler arası çatışmaların yanında, terörizm, silahların yaygınlaşması, ekonomik alanda zorlayıcı tedbirler, narkotik, sağlık ve bilgi sistemlerine yöneltilen saldırılar yönüne de çevrildiğini belirtmektedir.[167] Bilgi teknolojilerinin günümüz çatışma ortamında ağırlığı artan insan faktörünün hayatı ile daha çok iç içe geçmesi, siber alandaki istihbaratın da önemini artırmaktadır. Bununla birlikte, insan istihbaratının önemi tekrar hatırlanırken, teknik istihbarat kapsamında sinyal, ölçüm ve iz istihbaratı,

[165] Jagannath Panda, Ankit Panda, "Japan Is Ready to Become a Formal Member of Five Eyes", *Center for Strategic & International Studies*, C. 3, S. 8, (2020). https://www.csis.org/analysis/resolved-japan-ready-become-formal-member-five-eyes (Erişim Tarihi: 10.04.2022)
[166] Çıtak, a.g.e., 187.
[167] Mark M. Lowenthal, *Intelligence, from Secret to Policy* (Washington DC: CQ Press, 2008), 326-339.

görüntü istihbaratı ile açık istihbaratın birlikte analizi ve diğer müttefiklerle paylaşılarak geliştirilmesine yönelik bir anlayış değişimi yaşanmaktadır. Her bireyin muharip, her şeyin silaha dönüştüğü günümüz çatışmalarında istihbarat örgütlerinin internet sitelerinde halkın kendilerine bilgi sağlayabilmelerine imkân veren bağlantılar paylaşılarak, halk ile entegrasyon ve iletişim kurmaya başlanmıştır.[168]

İstihbarat teşkilatları üzerinden devletlerin bilgi ve istihbaratı dışarıdan da temin etmeye yönelik anlayış değişikliği ile genellikle açık kaynaklardan elde edilen verilerin toplama ve analizi ile istihbarat üreterek müşterileri ile (devlet ve özel şirketler) kâr amaçlı-amaçsız paylaşan Özel İstihbarat Şirketleri ortaya çıkmıştır. Bunların yanında, düşünce kuruluşları da uzmanlaştıkları alanlarda yaptıkları analizler ile dışarıdan temine, yani istihbaratın özelleşmesine katkı sağlamaktadır. Şirketlerin yanında, bilgi teknolojilerindeki gelişim ve veriye erişim imkânlarının artması ile bireysel olarak açık istihbarat üreterek istihbarat örgütleri ve genel kamuoyuna analizler sunan bireysel analistlerin de açık istihbarat kapsamında destek sağladıkları özellikle 2022 Rusya-Ukrayna gerginliğinde gözlemlenmektedir.[169] Kâr amacı gütmeyen bireysel çalışmaların, analiz ve çıkarımların, istihbarat kurumlarının raporlarında kullanıldığı, referans gösterildiği gözlemlenmiştir. Bu tespit, sadece özel istihbarat şirketleri değil, sivillerin bireysel çalışmalarının da günümüzde istihbarat fonksiyon alanına destek sağladığını göstermesi adına önem arz etmektedir.

Bireylerden özel şirketlere ve düşünce kuruluşlarının katkılarını içeren istihbaratın dışarıdan teminini klasik istihbarata dahil eden anlayış, istihbaratın genişlemesinde sağladığı farklı fonksiyon alanlarındaki uzmanlıklara dayalı tespit, değerlendirme, bakış açıları ve yeni yetenekleri ile değişen istihbarat anlayışının önemli bileşenlerinden birini oluştururken, istihbaratın bir disiplin olma yolundaki akademik gelişimini de desteklemektedir.[170]

3.1.2. Yöntemsel Dönüşüm

Anlayıştaki dönüşüm kadar yöntem ve tekniklerdeki yenileşme de çağın gerekliklerini karşılamak üzere istihbaratın dönüşümünde belirleyici rol oynamaktadır. 11 Eylül

[168] Franky Matisek, Ron Granieri. *Podcast-Everything a Weapon, Everyone a Combatant*, (U.S. Army War College, 2022).
[169] Evergreen Intel (@vcdgf555), Konrad Muzyka-Rochan Consulting (@konrad_muzyka), Oryx (@oryxpioenkop), Veli-Pekka Kivimaki (@vpkivimaki) gibi kişiler twitter hesaplarından değerlendirme ve analizlerini yayınlamakta, bu analizlerin bazılarının ise hatırı sayılır istihbarat platformlarında yayımlandığı gözlenmektedir.
[170] Çıtak, a.g.e., 195-196.

saldırıları sonrasında küreselleşen terörizmle mücadele ve devamında hibrit harekât ortamı ile çok bileşenli ve çok tabanlı hale gelen çatışma ortamının ortaya çıkardığı genişleyen ve derinleşen istihbarat ihtiyaçlarını karşılamak üzere yeni yöntemlere ihtiyaç duyulmuştur. Bu doğrultuda en önemli dönüşüm **toplama** alanında gerçekleşmiştir. Teknolojinin gelişimine paralel olarak insansız hava araçları, optik sistemler, lazer ve ölçme sistemlerindeki gelişime ilave olarak bu teknolojilerin kullanıldıkları harekât ortamlarına uzayın da eklenmesi ile özellikle teknik istihbarat alanında önemli bir gelişim sağlanmıştır. Gelişen teknolojinin ilk olarak askerî ve istihbarat alanında kullanıma girmesi özellikle toplama alanında her geçen gün yeni gelişmeleri beraberinde getirmektedir. Bunun yanında, teknik toplamaya önemi her geçen gün artan insan olgusu ve teknoloji ile entegrasyonu sonucunda ortaya çıkan büyük verinin (*Big data*) işlenmesine dayanan açık istihbarat yeteneklerinin eklenmesi ciddi yöntem gelişimlerini beraberinde getirmiştir. Açık istihbarat dezenformasyon ya da manipülasyon ihtimalini ve kısıtlı zamanda veri yığını arasında doğru bilgiyi bulma zorluğunu beraberinde getirse de en çok kullanılan toplama yöntemlerinden biri haline gelmiştir. İnsanın içinde bulunduğu ve kullandığı tüm teknolojilerden bilgi elde edebilmesi, bunun zaman ve mekândan bağımsız şekilde yapılabilmesi, ulaşılmak istenen bilgiye erişimi kısıtlayan unsurların bulunmaması, diğer ifadesiyle bilginin açık olarak erişilebilir olması açık istihbaratı en çok kullanılan toplama yöntemlerinden biri haline getirmiştir.[171]

Yöntemsel dönüşümün bir diğer önemli alanını ise **analiz** yeteneğindeki gelişim oluşturmaktadır. Çoğunlukla tamamlanmamış bilgi ve belirsizlik üzerinden olasılıkçı bir değerlendirme yapan analizciler mümkün olan en doğruyu tahmin etmeye çalışmaktadır.[172] Bu sebeple, üzerinde çalışılan konuya göre ilgili fonksiyon alanlarından **yetişmiş akademisyen veya konunun uzmanı kişilerin** yapılan analize destek sağlamaları ve üzerinde çalışılan konuda farklı disiplin alanı uzmanlarının birlikte katkı sağlamaları son derece önemlidir. Bu durum da belli alanda uzman analizciler istihdam eden özel şirketlere yönelimi desteklemektedir. İstihbarat teşkilatlarının tespit ve toplama yeteneklerinin yanında özellikle son 20 yıl içinde tespitlere müdahale etme yetenekleri sağlayan platformlara da sahip olmaları sadece

[171] Gašper Hribar, Iztok Podbregar, Teodora Ivanuša. "OSINT: A "Grey Zone?", *International Journal of Intelligence and CounterIntelligence*, C. 27, S. 3 (2014), 531.
[172] John Ransom Clark, *Intelligence and National Security: A Reference Handbook,* (London: Praeger Security International, 2007), 64.

toplayıcı değil, aynı zamanda avcı da olmaları yönünde yöntemsel başka bir değişimi beraberinde getirmiştir. İstihbarat teşkilatları paramiliter unsurlar ile nokta operasyonu yapabilen, silahlı insansız hava araçları ile tespit ve teşhis neticesinde yüksek değerli **hedeflere angaje olabilen** kinetik yöntemler kullanabilir hale gelmişlerdir. Bu yetenekler kimi çevrelerce hem iç hem uluslararası hukuk hem de insan hakları hukuku bakımından eleştirilseler de günümüz çatışma ortamının bir gerçeği olarak kabul edilmeye başlanmıştır.[173] Tüm bunların yanında algısal bir değişim olarak bahsettiğimiz istihbarat paylaşımı ve iş birliği, diğer ülkeler ile yapılan iş birliğinin ötesinde düşünce kuruluşları, üniversiteler ve özel istihbarat şirketleri ile ortak yürütülen çalışmalar kapsamında yöntemsel değişim olarak da karşımıza çıkmaktadır.

Özellikle çok tabanlı hâl alan günün harekât ortamı, kapsamlı bir durumsal farkındalığı ve harekâta tesir eden dinamiklere yönelik detaylı analizleri zorunlu kılmaktadır. Günümüz harekât ortamına etki eden tüm faktörler ve aktörlerin tespitinden uygulamaları muhtemel hal tarzlarının tahmin edilmesine yönelik analizler için her bir harekât tabanının kullanılması ayrı ayrı erişim ve avantajları ile kaçınılmaz bir durum almıştır. Güç çekişmesinin sahaya yansıması olan harekâtın dönüşümü ve bu dönüşümün gerektirdiği doktrinel gelişme kapsamında çok boyutlu hale gelmesi ile; harekâtı yönlendiren karar verme sürecini destekleyen en önemli bileşenlerden olan istihbaratın da çok tabanlı bir hâl alarak anlayış, yöntem ve yapısal dönüşüm yaşadığını görmekteyiz.

ABD Kara Kuvvetleri Komutanlığının ortaya attığı çok tabanlı istihbarat kavramını 2028 yılında yerleştirmeyi amaçladığı konseptsel çalışmada 3-7 yıllık dönem içinde; sensör sistemleri (Çok hassas algılama, nesnelerin interneti, gözlemlenemeyen tespit yetenekleri), veri (blok zincir teknolojisi, yapay zeka ve yaygınlaştırılmış öğrenme, sentetik veri, veriye aç analitik metotlar), analiz (tüm analizlerin bilgisayar destekli yapılması, yapay zekâdan azami faydalanma, soruna özel analitik değerlendirmeler) ve destekleyen teknolojiler (5G ağların kullanımı, mobil optik haberleşme sistemleri, ileri teknoloji işlemci yetenekleri) alanlarının istihbarat oluşturma gayretlerini desteklemek üzere hayata geçirilmesi hedeflenmektedir. Ayrıca, tüm teknik toplama gayretlerine ilave olarak, kimlik istihbaratı kapsamında düşmanın ilgi sinyallerini (*Signals of Interest-SOI*) ve faaliyetlerine ilişkin verileri toplamaya yönelik

[173] Milena Sterio, "Lethal Use of Drones When the Executive Is the Judge, Jury, and Execution", *The Independent Review*, C. 23, S. 1 (2018), 37-41.

yeteneklerin de toplama yeteneklerine dahil edilmesi planlanmaktadır. Bu yeni toplama yeteneğine verilen önemden yola çıkarak, insan algı ve ilgisine ilişkin aktivite tabanlı istihbarat (Activity Based Intelligence) anlayışının ve bu çok tabanlı ve teknolojik/sayısal dönüşüm içeren çok yetenekli konseptsel dönüşümün "insan" öğesini merkezi bir yere koyan bir anlayışı benimsediği söylenebilir.[174]

3.1.3. Yapısal Dönüşüm

Anlayış ve yöntemlerdeki değişim, istihbarat teşkilatlarında yapısal değişimleri de beraberinde getirmiştir. Özellikle 11 Eylül saldırılarından sonra istihbarat örgütlerinin daha önce olmadığı kadar çok veriyi içeren, karmaşık ve son derece hızlı değişen küresel ortamda mevcut olan veriyi işleme ve analiz ile sürprizi önleme yeteneğinde geri kaldığı tespit edilmiştir. Bahse konu saldırı ve tehdide karşı, istihbarat teşkilatlarının yetersiz kaldığı değerlendirmeleri neticesinde pek çok ülkede (1) istihbarat teşkilatlarının kaynaklarının ve yasal yetkilerinin artırılması, (2) yurt içi ve yurt dışında istihbarat paylaşımının önünün açılması politikaları uygulamaya alınmıştır.[175] Bunlara ek olarak bu değişen tehdit ortamına adapte olmak üzere ABD istihbarat yapılanmasının ciddi bir reform ile kendini uyarlamaya çalıştığı ve bunun diğer ülkelerin de yapılanmalarını gözden geçirmelerine neden olduğu görülmektedir. Farklı uzmanlık alanlarına yoğunlaşan istihbarat yapılanmaları, teşkilatlar arası paylaşım, birlikte çalışabilirlik, eş güdüm sağlamak üzere birçok ülkede ABD'deki Ulusal İstihbarat Direktörlüğü Ofisi (*Office of Directorate of National Intelligence – ODNI*) gibi **koordinasyon** yapılanmalarının oluşmasını da gerektirmiştir.[176] Günümüzde istihbarat teşkilatlanmalarının, küresel terör ve büyük güç mücadelesi kapsamında ulus ötesi tehditlerle mücadelede devletler, devlet dışı silahlı örgütler, kaçakçılık, doğal veya yapay felaketler, suç örgütleri, aşırı dinci yapılanmalar ve ideolojilere karşı etkin görev almaları beklenmektedir. Soğuk savaş dönemi ile karşılaştırıldığında artan ve çeşitlenen tehditlere karşı, küresel güçler için dünyanın her yerinde, bölgesel güçler için etki ve ilgi sahasında tesir sağlayabilecek, insan istihbaratı, uydu ve insansız hava araçları da dahil olmak üzere teknik istihbarat

[174] US Army, *US Army Multi-Domain Intelligence FY21-22 S&T Focus Areas*, Washington DC: US Army, 2022.
[175] Prem Mahadevan, "Intelligence Agencies: Adapting to New Threats", *CSS Analysis in Security Policy*, S. 82, (2010): 2.
[176] ODNI. *Private Sector Engagement* (Washington DC: Office of the Director of The National Intelligence, 2022), https://www.dni.gov/index.php/who-we-are/organizations/national-security-partnerships/ps-engagement [Erişim Tarihi: 23.05.2022].

kabiliyetleri ve konusunun uzmanı personelce yürütülen açık kaynak istihbaratının birlikte eş güdüm içinde yürütülmesi gerekmektedir. Bilgi teknolojilerindeki gelişimin bir sonucu olarak siber uzayın öneminin daha da artacağı, bu alanın casusluk, takip, bilgi harekâtı, sosyal çatışmalar, algıya yönelik faaliyetler, bilgiye erişim, bilgi hırsızlığı ve kritik altyapılara saldırılar gibi pek çok faaliyet için kullanıldığı ve kullanımının artacağı değerlendirilmektedir. Bu bağlamda özellikle **siber istihbarat** ve bu alandaki faaliyetleri yürütme ve/veya yürüten özel yapılar ile eş güdüm sağlayacak uzmanlaşmış istihbarat teşkilatlarının kurulması gerekliliğine dikkat çekilmektedir.[177]

Kararı destekleyen ve sürprizi önlemek üzere bilinenler, faraziyeler ve emarelerin analizi ile mümkün olan en tutarlı tahmini oluşturmaya çalışan istihbaratın güvenilirliği için en elzem olan veridir. Bu bağlamda genişleyen ve eklenen yeni harekât tabanları ile çok katmanlı hale gelen çatışma/çekişme ortamında istihbaratın; anlayış, yöntem ve yapısal olarak en fazla veri üreten siber (bilgi de dahil olmak üzere) ve uzay harekât tabanlarında daha çok geliştiğini söylemek yanlış olmayacaktır.

Hayatın her alanına giren akıllı teknolojiler ile, iletişim olanaklarının da gelişimi, sanal ortama bırakılan izler ile 'Büyük Veri – Big Data' kavramı oluşmuş, veri yığını içinden anlamlı parçaların ayıklanması ve analizi, yapay zekâ destekli makine öğrenmesinden faydalanan algoritmaları kullanan teknolojiler ile yeni bir sektör olarak belirmiştir. Fakat, yapay zekânın kullanılması ile ilgili olarak üç temel tartışma konusu hakimdir. Bunlardan birincisi kullanılan verilerin kalitesi, ikincisi kişisel verilerin kullanılması ve üçüncüsü ise algoritmik hesap verebilirliğin limitli olmasıdır.[178] Güvenlik alanında pek çok kullanım alanı bulunan bu yeni sektörün, teknolojileri geliştiren üniversiteler öncülüğünde değişime adaptasyonda devlet kurumlarına göre çok daha esnek olan özel şirketlerce domine edildiği görülmektedir.[179] Veriyi işlemenin yanında, sahip olunan verinin güvenliğinin sağlanmasının ehemmiyeti de siber güvenlik kavramını ön plana çıkartmaktadır. Sayısal ortamda toplanan, işlenen ve dağıtılan verinin güvenliğinin de bu alanda sağlanması İstihbarata Karşı Koyma (İKK) kapsamında siber güvenliğin ve

[177] Sanjay Goel, "Cyberwarfare: Connecting the Dots in Cyber Intelligence", *Communications of the ACM*, C. 54, S. 8 (2011), 134-136.
[178] Ana Beduschi, "International Migration Management in the Age of Artificial Intelligence", *Migration Studies*, C. 9, S. 3 (2020), 578.
[179] Sophie-Charlotte Fischer, "NATO and Artifical Intelligence: The Role of Public-Private Sector Collaboration", *NATO Decision-Making in the Age of Big Data and Artificial Intelligence*, der. Sonia Lucarelli, Alessandro Marrone, Francesco Niccolo Moro. Brussels: NATO HQ, (2021), 76.

tam tersi bir yaklaşımla hasma yönelik sayısal ortamda bilgi toplama faaliyetlerini de kapsayacak şekilde bir bütün olarak siber istihbaratın önemi her geçen gün artmakta, istihbarat alanında başat ülkelerce bu alana yönelik anlayış, analitik ve yapısal çözümler getirilmeye çalışılmaktadır. ABD Siber Komutanlığı (*US Cyber Command*); bu harekât tabanındaki tehditlerle küresel olarak mücadele kapsamında hem ABD ulusal çıkarlarını korumak ve geliştirmek hem de kuvvet komutanlıkları bünyesindeki siber-uzay komutanlıklarının planlama ve harekât faaliyetlerini yönetmek, senkronize ve koordine etmek amacıyla müşterek bir komutanlık olarak 2010 yılında kurulmuştur. ABD'nin bu alandaki anlayış, yöntem ve yapısal adımlarını ittifak içindeki diğer ülkeler de takip etmiştir.

Dünya dışı yörüngelere gözetleme ve teknik istihbarat yeteneklerine sahip uyduların yerleştirilmesine Corona Casus Uydu[180] projesi ile başlanmış ve uzayın istihbarat maksatlı kullanımı günümüze kadar artarak devam etmiştir. Yeryüzünde konuşlandırılmış sistemlere nazaran kapsama alanı ve erişim açısından çok daha avantajlı olan uydu sistemleri teknolojinin de gelişimi ile toplama alanına ciddi katkı sağlamıştır. Günümüzde telekomünikasyon, meteoroloji, küresel konumlama ve benzeri pek çok teknoloji için uygun ortam oluşturan uzay ile bir şekilde irtibatı olmayan alan kalmamıştır. Tüm bunların yanında; görüntü, sinyal ve teknik istihbarat alanlarında toplama yetenekleri için ideal ortam oluşturan uzay, günümüz güç mücadelesinde de devletlerin egemen olma çabasında oldukları bir harekât tabanı olarak kabul edilmiştir. Bu alanda da başı çeken ABD; 1985 yılında temelleri atılan çalışmanın gelişimi ile ABD Uzay Komutanlığını 2019 yılında ABD Savunma Bakanlığına bağlı müşterek bir karargâh olarak kurmuştur. Vazifesi; ABD, müttefik ve partnerlerince tesis edilebilecek birleşik müşterek kuvvetlere uzay tabanlı muharebe desteği sağlamak, gerekirse saldırıları bertaraf etmek ve caydırıcılık sağlamak üzere uzayda, uzaydan veya uzaydan geçecek şekilde harekât icra etmek olarak tanımlanmaktadır.[181] Benzer vazife ve vizyon ile Fransız Uzay Komutanlığı[182] ise 2010, Birleşik Krallık Uzay Komutanlığı[183] 2021 yılında kurulmuştur. Görevleri

[180] Kevin C. Ruffner, *CORONA: America's First Satallite Program*, (Washington DC: CIA History Staff Center for the Study of Intelligence, 1995), 2-5.
[181] US Department of Defense, US Space Command, (2022) https://www.spacecom.mil/ [Erişim Tarihi: 15.05.2022].
[182] L'organisation de l'armée de l'Air et de l'Espace, (2022), https://www.defense.gouv.fr/air/organisation-AAE [Erişim Tarihi: 15.05.2022].
[183] Royal Air Force. UK Space Command, (2022). https://www.raf.mod.uk/what-we-do/uk-space-command/. [Erişim Tarihi: 15.05.2022].

ağırlıklı olarak uzay tabanının sağladığı avantajlar ile durumsal farkındalık sağlamaya yönelik istihbarat toplama (sinyal, görüntü, coğrafi ve teknik) üzerine yoğunlaşan ve diğer harekât tabanları ile eşgüdüm içerisinde destek sağlayan bu müşterek komutanlıkların devlete ait ulusal yetenekler ile, benzer yetenekleri sunan özel şirketler ile de iş birliği içinde çalıştıkları belirtilmektedir.[184] Çalışma ABD özelinde konuyu incelemekteyse de istihbaratın gelişimi ve uygulamasında önemli yeri olan ülkelerde ABD uygulamaları ile uyuşan adımlar atılması, yapılan çalışmaların küresel taban bulduğunu göstermektedir.

3.2. Yeni Tehditler

İstihbaratın dönüşümünün bir nedeni de tehdit anlayışındaki değişimdir. Özellikle Sovyet Bloğunun çöküşü ile soğuk savaş döneminin sonlanması istihbarat görevlerinin doğası ve kapsamı üzerinde dramatik bir değişime neden olmuştur. Ulusal güvenlik tehdidi; bir ülkenin halkının güvenliğini, temel refahı, devlet fonksiyonların devamlılığını, bağımsızlığını, stratejik varlıklarını veya milli hedeflerini tehdit eden bir tek ya da devam eden bir olay veya eylem olarak tanımlanmaktadır. Ulusal güvelik tehdidi sadece askerî veya politik risklerin dışında toplum sağlığını tehdit eden salgın hastalıklardan tabii afetlere, olağanüstü iklimsel olaylara, insan etkisi ile gerçekleşen felaketlere (1986 Çernobil felaketi gibi), önemli sosyal ve ekonomik krizlere ve bunların birkaçının bir arada oluşması şeklinde de ortaya çıkabilir. [185]

Tehdidin tek ülke/blok odaklı halden, odaksız ve çok taraflı tehdide (yerel çatışmalar, iklim değişimine bağlı gelişmeler, pandemi, suç ve terör örgütleri ile bunların bağlantılı çalışmaları, insan haklarına yönelik uygulamalar vb.) evrimleştiği görülmektedir. Bunların yanında yeni teknolojilerin de istihbarat kurumları için ayrı bir anlama büründüğü söylenebilir. Bu yeni teknolojilerin hasımlar tarafından da kullanılıyor olması; batılı istihbarat çabalarının tespit edilmesi, bozulması, etkisinin azaltılması ve yanıltılmasını mümkün kılmaktadır.[186]

---

[184] UK Ministry of Defense. *The Orchestration of Military Strategic Effects*, (London: UK Ministry of Defence, 2021, 6.

[185] Kim, R. Holmes, "What is National Security?", *2015 Index of U.S. Military Strength*, (The Heritage Foundation, 2014), 20. https://www.heritage.org/sites/default/files/2019-10/2015_IndexOfUSMilitaryStrength_What%20Is%20National%20Security.pdf [Erişim Tarihi: 20.08.2023].

[186] CSIS Technology and Intelligence Task Force, *Maintaining the Intelligence Edge: Reimagining and Reinventing Intelligence through Innovation*, (Washington DC: Center for Strategic and International

Hershkovitz, yeni teknolojiler odaklı değerlendirmesinde; günümüzün yeni tehditlerini istihbarat örgütünü etkileyen dış ve iç sorun sahaları olarak iki ana sınıfta incelemektedir. Çağımızın çatışma veya çekişme ortamında belirleyici aktör olan insanın oluşturduğu toplumun algısını şekillendirilmesi, teknoloji yarışında geri kalma ve insanlığın güvenliğine yönelen küresel ısınma ve pandemi gibi tehditleri dış kaynaklı; dönüşüme direnci ve yeni teknolojileri ise iç sorun sahaları olarak sınıflandırmaktadır.

Dış kaynaklı sorun sahalarının başında; **toplum algısını şekillendirme** konusunda, 'derin sahtecilik (deep fake)' veya 'sentetik medya' olarak adlandırılan, ses ve görüntülü medya aracılığıyla yapılan manipülasyon istihbarat topluluğunu iki kat yormaktadır. Artan veri okyanusuna eklenen bu sahte bilgi katmanı veriyi işleme yükünü daha da artırırken, istihbarat kurumlarının doğruya yakın analizler üretebilmek üzere doğru ile yanlış bilgiyi ayırmak için ilave çaba harcamasını da zorunlu kılmaktadır. 2016 ABD başkanlık seçimlerine Rusya'nın müdahale iddiaları, benzer şekilde Avrupa ülkelerinde de sosyal medya platformları üzerinden yapılan manipülasyonlar ile seçimlere müdahale çabaları, demokratik rejimin temellerine saldıran en üst seviyede stratejik bir tehdit olarak kabul edilmektedir.

İkinci dış sorun sahası ise **teknolojik üstünlüğü elde etme gayretleri**dir. Günümüzde teknolojik üstünlük ulusal güvenliğin temel bileşenlerinden olarak gösterilmektedir. Siber uzayda üstünlük, yapay zekâ ve kuantum bilgi işleme yetenekleri süper güçler kadar, asimetrik etki oluşturma gayreti içindeki küçük ülkelerin de stratejik hedefleri arasında sayılmaktadır. Mobil iletişim teknolojilerinin yaygınlaşması, güvenlik kamera sistemleri ve benzeri birçok teknoloji ile elde edilen devasa verinin işlenmesinde batılı demokrasilerin önünde kişisel hak ve özgürlükler bağlamında pek çok kısıtlayıcı durum söz konusuyken, totaliter merkeziyetçi yönetimlerin bu tür kısıtları umursamayan uygulamaları ile bu alanda avantaj sahibi oldukları söylenebilir.

Diğer bir dış sorun sahası ise; salgın hastalıklar, insan kaynaklı felaketler, doğal afetler ve iklim değişikliği gibi **halkın huzur ve refahını tehdit eden olaylar** sayılabilir. Devletlerin bu durumlara karşı tedbirleri veya sorumluluğu olan kurumları bulunmakla birlikte, ulusal güvenliği tehdit eden bu durumlara karşı direkt sorumluluğu bulunan

Studies Press, 2021), 5-8. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210113_Intelligence_Edge.pdf [Erişim Tarihi: 20.08.2023].

bir istihbarat kurumunun bulunmaması bir handikap olarak değerlendirilmektedir. Terörist saldırılar, savaş vb. ölümcül ve nispeten kısa dönem olaylarına karşı daha hazırlıklı olan istihbarat topluluğunun, daha uzun soluklu mücadele planı gerektiren bu tip felaketlerle mücadelede karar vericileri desteklemek üzere farklı bir bakış açısı ve paradigma değişimine ihtiyaç olduğu üzerinde durulmaktadır.[187]

İstihbarat topluluğu ve kurumlarını içeriden tehdit eden faktörler incelenmesi gereken bir diğer başlıktır. Ulusal güvenliğin iyi tanımlanmış, ulus devlet tarafından yürütülen gizli faaliyetler ile tehdit edildiği bir dönemde mücadelenin temeli, tehdidi oluşturan devlet ve faaliyetlerine yönelik azami bilgi elde etmekte yatmaktaydı. İstihbarat kurumları; ihtiyaç duyulan bilgiyi tespit etme, toplama vasıtalarını yönlendirme, toplanan verileri işleme, elde edilen istihbaratı yayma anlayışı üzerine kurulu 'istihbarat çarkı' işleyişi ile karar vericilerin ihtiyacını karşılama gayreti içerisindeydi. Bu ihtiyacın daha iyi karşılanması için, daha büyük bütçe, daha fazla sensör ve daha üstün analiz metotlarına ihtiyaç duyulacağı varsayımı Soğuk Savaş dönemi için kabul görmekteydi. Sovyetler Birliğinin çöküşü ile Soğuk Savaş döneminin sona ermesinden ve 2001 terör saldırıları sonrasında tehdit algısındaki değişimle birlikte ulusal güvenliğe yönelen tehditlerin çeşitlenmesi döneminde de istihbarat çarkı metodolojisinin ihtiyacı karşıladığı kabul edilmektedir. Ancak Biltgen ve Ryan'ın 'istihbaratın 4'üncü dönemi' olarak tanımladığı 2014 sonrası çoklu istihbarat anlayışı ve büyük veri analitiklerinin öne çıktığı süreçte ulusal güvenlik ortamı radikal bir şekilde değişmiştir.[188] Yeni teknolojilerin sağladıkları 'istihbarat çarkı' metodolojisinin çok önüne geçmiş ve istihbarat topluluğunun saygınlık ve güvenilirliğini korumak adına (1) Görev, (2) Organizasyon Yapısı ve (3) İşleyiş alanlarında bir reforma ihtiyaç olduğuna yönelik çalışmalar yapılmış ve bu ihtiyaç ABD istihbarat topluluğunun ileri gelenlerince de ifade edilmeye başlanmıştır.

ABD istihbarat sisteminde dönüşümün gerekliliği konusunda genel bir fikir birliği olmakla birlikte, bu dönüşümün hangi kapsam ve çapta olması gerektiği yönünde farklı görüşler bu konu odaklı yapılan pek çok çalıştay, seminer veya akademik çalışmada tartışılmıştır. 2005 yılında yayımlanan 'ABD İstihbaratının Dönüşümü' başlıklı çeşitli makalelerden oluşan çalışmada uzmanlar; mevcut politikalar ve uygulamayı

[187] Hershkovitz, a.g.e., 21-22.
[188] Biltgen ve Ryan, a.g.e., 22-24.

eleştirerek ABD'nin gelecekte karşılaşacağı tehditlerle mücadele konusunda yetersiz kalmasına sebep olacağı öne sürmektedir. Buna rağmen çalışmanın sonundaki tavsiyeler yüzeysel ve kısıtlı bir dönüşüm ile sınırlı kalmıştır.[189]

İstihbaratın geleceğine ilişkin RAND tarafından yapılan belki de ilk kapsamlı çalışmada; büyük veri ve yapay zekâ teknolojileri ele alınsa da 2006 tarihli çalıştayda bu teknolojiler henüz yeterince gelişmemiş olmaları ve özellikle yönetici seviyesindeki katılımcıların yaş grubu itibariyle teknolojiye mesafeleri nedeniyle beklenen ilgiyi çekememiştir.[190] Buna rağmen çalışma; gelişen yeni teknolojilere dikkat çekerken, istihbarat topluluğunun yeninden yapılanma ve işleyişi konusunda geleceğe adaptasyon adına önemli bir dönüşüme ihtiyaç duyulduğunu ortaya koyması adına önem arz etmektedir.[191]

2010 Arap Baharı olayları, istihbarat teşkilatlarını sürprize uğrattığı gibi, sıradan insanların iletişim teknolojilerinin sağladığı imkânlar ile ne kadar etkili olabildiğini göstermesi adına bir dönüm noktası olarak kabul edilmektedir. İstihbarat teşkilatlarının metotlarının yeni teknolojilerin kullanımıyla katalize olan yeni meydan okumalara hazır olmadığını göstermiştir. Bunun üzerine, veri toplama, analiz, tahmin ve öngörü oluşturmaya yönelik yeni metodolojiler önerilmiştir. Bir kısım reformu tehdit ortamının değişmesine bağlarken, bir kısmı ise teknolojik gelişmeler ışığında yeni analitik tekniklerin bir kısım organizasyonel yapı değişiklikleri ile adaptasyonunu önermektedir. Bu alandaki pek çok çalışmanın yanında William Lahneman'ın RAND bünyesinde yapılan çalışmalar üzerine yazdığı eseri köklü değişim önermeleri ile diğerlerinin önüne geçmektedir. Tek tehditten çoklu ve dağınık tehdit olgusunun bir algı değişimini gerektirdiğini, buna adaptasyonda gecikilmesinin karar vericiler ile istihbarat topluluğu arasında gerilime neden olduğunu, bu nedenle sorun alanlarına yönelik değerlendirmelerde bir eşgüdüm, ortak bir anlayış sağlanamadığını vurgulamaktadır. Lahneman, ajanslar arasında daha fazla iş birliği ve paylaşımın gerekliliğine dikkat çekerken, istihbarat topluluğu dışında üniversiteler ve özel sektör ile de bu iş birliği ve bilgi paylaşımının gerekliliğine dikkat çekmektedir. Farklı bakış açısı ve uzmanlıklardan azami faydalanılması için daha geniş bir mesleki yelpazeden

[189] Burton L. Gerber ve Jennifer E Sims. *Transforming U.S. Intelligence* (Washington DC: Georgetown University Press, 2005), 288-293.
[190] Hershkovitz, a.g.e., 28.
[191] Gregory F. Treverton, Seth G. Jones, Steven Boraz, Phillip Lipscy, *Toward a Theory of Intelligence: Workshop Report*, (Santa Monica California: RAND, 2006), 30-32.

istihdamın gerekli olduğunu ve bu personelin sektör içindeki paradigma değişimine uygun, değişen görevler, değerler, yapısal değişimler ve metodolojiye uygun şekilde güncellenmiş bir eğitime tabi tutulması ihtiyacına işaret etmektedir. Tüm bunların yanında bilgi teknolojilerindeki gelişmelerin metodolojiye adaptasyonuna yeterince değinmemesiyle de eleştirilmekle birlikte, özel sektör ile iş birliğinin önemini vurgulamasının altındaki temel gerekçenin özel sektörün teknolojiye adaptasyonu sağlama ve teknolojiyi sürükleme konusunda kamu istihbaratının önüne geçmiş olması gösterilmektedir.[192]

Değişim konusundaki bir diğer önemli çalışma da David Moore'a aittir. Lahneman gibi istihbaratta bir paradigma değişimine işaret eden Moore, daha ileri giderek 'istihbarat çarkı'nın günümüz şartları için yetersiz kaldığını öne sürmektedir. İstihbarat topluluğunun çözmekte zorlandığı problemlerin, değişen tehdit ortamı ve değişen istihbarat ihtiyaçlarından kaynaklandığı, ajansların bu sorunu sadece toplama yeteneklerini geliştirerek çözemeyeceklerini ileri sürmektedir. Ancak o da akademisyenlerce; siber uzayın yeni harekât ortamı olduğu, bu alanın sosyal, ekonomik ve kültürel alanlara etkilerini gözden kaçırmakla eleştirilmektedir.[193]

İstihbarat topluluğu ve işleyişindeki dönüşüm gereksinimine ilişkin çeşitli makalelerden oluşan 'İstihbaratın Geleceği (The Future of Intelligence)' adlı eser içinde barındırdığı birkaç makalede[194] pesimist de olsa, ABD istihbarat topluluğunun öğrenen ve uyum sağlayabilen bir organizasyon olduğu vurgusu ile radikal transformasyon önerilmektedir. Laqueur'un tespitleri[195] ile uyumlu şekilde; istihbaratın politika veya stratejinin alternatifi değil, destekleyen bir unsur olduğu, bu desteğin sağlıklı ve güvenilir şekilde sağlanmaya devam edilebilmesi için güncelin gerekliliklerini yerine getirecek dönüşümün önemine dikkat çekilmektedir.[196] Birçok

[192] William J. *Lahneman, Keeping U.S. Intelligence Effective: The Need for a Revolution in Intelligence Affairs*, (Plymouth: Scarecrow Press, 2011)

[193] David Moore, *Sensemaking: A Structure for an Intelligence Revolution* (Washington DC: NDIC Press, 2011), Sf.149-156.

[194] David Omand, "The future of Intelligence: What are the threats, the challenges and the opportunities?", *The Future of Intelligence:Challenges in the 21st Century*, ed. Isabelle Duyvesteyn, Ben de Jong, Joop van Reijn. New York: Routledge, 2014, 14-25.; Arthur S. Hulnick, "The future of the intelligence process: the end of the intelligence cycle?", *The Future of Intelligence:Challenges in the 21st Century*, ed. Isabelle Duyvesteyn, Ben de Jong, Joop van Reijn. New York: Routledge, 2014, 47-57.; Trerverton, 2014, 27-38.

[195] Walter Laqueur, *The Future of Intelligence*, (Society Publishing, 1985), 3–11.

[196] George Dimitriu, Isabelle Duyvesteyn, "Conclusions: It may be 10 September 2001 Today", *The Future of Intelligence:Challenges in the 21st Century*, ed. Isabelle Duyvesteyn, Ben de Jong, Joop van Reijn. New York: Routledge, 2014., 158-159.

alanda oldukça köklü değişimler önerse de eser, istihbarat topluluğu ve işleyişi ile ilgili kapsamlı bir yapı ortaya koyamamıştır.

Değişim ve dönüşüme yönelik gereklilik akademisyenler başta olmak üzere, istihbarat topluluğunca da gerekli görülürken, bu bağlamda özellikle teknolojiye uyum sağlamanın önemine dikkat çeken yazında ve söylemlerde da artış görülmeye başlamıştır. Önerilen yeni konseptler, tanımlar ve istihbarat topluluğu için yeni görev tanımları önerilmeye başlanmıştır. 2019 sonrası ABD İstihbarat topluluğu yöneticilerinin bu konuya yönelik söylemleri incelendiğinde;

- ABD İstihbarat ve Araştırma Bürosu (INR) başkan yardımcısı Ellen McCarty 2019 yılındaki konuşmasında istihbarat topluluğunun iki önemli alanda geri kaldığına işaret ederken bunları; teknolojik gelişmelerin sisteme dahil edilmesindeki gecikme ve açık kaynak istihbaratının hızlı, etkin şekilde sürece entegre edilmesindeki güçlükler olarak sıralamıştır. Ayrıca bu iki alanda özel sektör istihbaratının bu iki sorun sahasında devlet kurumlarının önünde olduğuna da dikkat çekmiştir.[197]

- ABD'nin gözetleme uydularını geliştiren ve tedarik eden Ulusal Keşif Ofisi'nin (National Reconnaissence Office-NRO) direktörü Christopher Scolese ABD Senatosu Silahlı Kuvvetler Komitesine verdiği ifadede; kurumunun önündeki en büyük güçlüğün, yeni teknolojileri devreye alarak mevcut faaliyetleri sekteye uğratmadan ve toplanan veriyi işleme hızını düşürmeden, bütünlüğünü ve güvenilirliğini bozmadan işlemeye devam ederek rakiplerin önünde kalmak' olduğunu ifade ederek teknoloji yarışında geri kalmamak gerektiğine dikkat çekmiştir.[198]

- ABD İstihbarat Topluluğunun baş bilgi sorumlusu olan John Sherman; 'Rakiplerimiz siber harekât tabanında (domain), yapay zekâ, makine öğrenmesi (machine learning), bilgi ve asimetrik harekât ve bahsetmeye gerek olmayan konvansiyonel harp teknolojileri ve uzay gibi diğer yeteneklerde oldukça hızlı

[197] Michael Morell ve Ellen McCarthy, "Head of State Department's Intelligence Arms on Assessing Foreign Leaders: Intelligence Matters", *Intelligence Matters Podcast*, 2019. https://podcasts.apple.com/ee/podcast/head-state-departments-intelligence-arm-on-assessing/id1286906615?i=1000444085895 [Erişim Tarihi: 02.08.2023].

[198] Kelsey Reichmann, "3 Space Challenges fort he Intelligence Community", *C4ISRNET*, 4 Ağustos 2023, https://www.c4isrnet.com/battlefield-tech/space/2019/06/05/3-space-challenges-for-the-intelligence-community/ [Erişim Tarihi: 10.08.2023].

gelişiyorlar. Mücadele, güç çekişmesi arenası gittikçe teknoloji, veri ve güvenlikle tanımlanmaya başladı, bu alanda rekabete devam edebilmek için daha büyük yenilenmenin yanında özel istihbarat endüstrisi, akademi ve müttefiklerle iş birliği gereklidir.' şeklinde teknoloji ile anlayış ve işleyişi de kapsayacak bir reformun gerekliliğine dikkat çekmiştir.[199]

- ABD Ulusal İstihbarat eski Direktörü Dan Coats diğerlerinden çok önce 2018'de; ABD İstihbarat Topluluğunun çok daha yenilikçi ve esnek olması gerektiğini söylemiştir. Yeni teknolojileri destekleyen bir istihbarat devrimi, bilgi ve yapı yönetiminde iyileştirmeler ve özel sektör ile daha geniş ve derin bir iş birliği için çağrıda bulunmuştur.[200]

- Merkezi İstihbarat Ajansı (CIA) eski Direktörü Mike Pompeo da 2019'da daha çevik ve sürekli değişime daha iyi uyum sağlayan bir istihbarat topluluğu olma gerekliliğini vurgulamıştır.[201]

- ABD Ulusal Güvenlik Ajansı (NSA) genel danışmanı Glenn Gerstell; dönüşümün gerekliliğini teknolojinin toplum ve hükumetlerin uyum sağlayabileceğinden daha hızlı gelişmesi ile savunmuş, büyük veri analitiklerinin özel hayatın gizliliği normlarını tehdit ettiğini, siber savaşın devlet dışı aktörler tarafından dahi uygulanabilir hale geldiğini ve ABD'nin düşmanlarının interneti demokrasiyi ortadan kaldıracak şekilde kullandıklarını ifade etmiştir. Gerstell, istihbarat topluluğunun hızlı bir şekilde teknolojiye adaptasyonunu sağlayabilmesi için hükumetin istihbarat fonksiyon alanına ağır bir yatırım yapması ve personelden en etkin şekilde verim almak üzere bu alandaki yeteneklerin cezbedilmesi gerekliliğini dile getirmiştir. Ayrıca istihbarat kurumlarının özel sektör ile daha da fazla iş birliği içinde olması yönünde tavsiyede bulunmuştur.[202]

---

[199] Jack Corrigan, "Cyber Threats Are Emerging Faster Than DHS Can Identify and Comfront Them", *Defense One*, 2023. https://www.defenseone.com/threats/2019/03/cyber-threats-are-emerging-faster-dhs-can-address-them-secretary-says/155719/ [Erişim Tarihi: 10.08.2023].

[200] Dan Coats, "Confronting 21st Century Challenges", *ISP Intelligence Studies*, Etter-Harbin Alumni Centre, 2018 https://video.ibm.com/recorded/114060119 , [Erişim Tarihi: 10.08.2023].

[201] Marc A. Thiessen "Intelligence Beyond 2018: A Conversation with CIA Director Mike Pompeo", *AEI Events Podcast*, American Enterprise Institute, 2019 https://www.aei.org/events/intelligence-beyond-2018-a-conversation-with-cia-director-mike-pompeo-livestreamed-event/ [Erişim Tarihi: 23.08.2023].

[202] Glenn S Gerstell, "I Work For N.S.A. We Cannot Afford to Lose the Digital Revolution", *New York Times*, 10 Eylül 2019, https://www.nytimes.com/2019/09/10/opinion/nsa-privacy.html , [Erişim Tarihi: 23.08.2022].

- ABD Merkezi İstihbarat Ajansı eski direktörleri Michael Morell ve akademisyen Amy Zegart da 2019 tarihli makalelerinde benzer konuların önemine değinmiş, teknolojik gelişmelere adaptasyon ve özel istihbarat sektörü ile daha derin, kapsamlı bir iş birliğinin gerekliliğine dikkat çekmiştir.[203]

3.3. Yeni Teknolojiler ve Yeni İhtiyaçları

Akademisyenler ve istihbarat topluluğu yöneticilerinin de pek sıklıkla dile getirdiği, günümüz istihbarat anlayışına tesir eden teknolojilere de değinmekte fayda vardır. Özellikle mobil teknolojilerin kullanımının yaygınlaşması toplanabilir ve işlenerek anlamlandırılabilir veri miktarında olağan üstü bir artış getirmiştir. Bilgi üstünlüğü kapsamında; sadece ABD değil, dünyada da istihbarat örgütleri işleyebilecekleri veriden çok daha fazlasını toplamaktadırlar ki bu 1960'lardan beri süregelen bir durumdur.[204] Bu sorunsalın çözümü için süreç içerisinde çeşitli metodolojiler geliştirilmişse de çözüm hep teknolojide aranmış, istihbarat ve teknoloji hep kol kola olmuştur. Teknoloji istihbaratı değiştirmiş, istihbarat teşkilatları yeni teknolojiler geliştirmiş veya geliştirilmesi için motive edici olmuştur. Ancak günümüz, daha önce yaşananlardan çok daha hızlı gelişen ve çok farklı uygulama alanları ile istihbarat kurumlarını tarafından alışılagelmiş metodoloji ve yaklaşımların dışında bir yaklaşımla değerlendirmeye iten teknolojilerle karşı karşıya bulunmaktadır. İstihbaratı, anlayış, organizasyon yapısı ve metodolojide değişim ve dönüşüme iten bu yeni teknolojileri inceleyerek kullanım alanları ile sağladıkları/sağlayabilecekleri katkıları incelemekte fayda vardır. **Nesnelerin interneti (IoT) ve bulut veri depolama ve 5G teknolojileri:** Normal nesnelere yerleştirilen sensörler ile, elde edilen sayısal verilere, ölçümlere, ses, görüntü kaydına imkân veren, bu verileri internet üzerinden aktaran veya uzaktan erişilebilen (bulut veri depolama) sunuculara gönderebilen teknolojiyi ifade etmektedir. Araştırma şirketi olan IDC; 2025 yılında nesnelerin internetine 75 ila 100 milyar cihazın bağlanacağını ve bu cihazlardan elde edilecek verinin büyüklüğünün 80 zettabayta ulaşacağını ön görmektedir.[205] Bu

[203] Amy Zegart ve Michael Morell, "Spies, Lies and Algorithms: Why U.S. Intelligence Agencies Must Adapt or Fail", *Foreign Affairs*, 2019, https://foreignaffairs.com/articles/2019-04-16/spies-lies-and-algorithms , [Erişim Tarihi: 23.08.2023].
[204] Hershkovitz, a.g.e., 47.
[205] Larry Dignan, "IoT Devices to Generate79.4 ZB of sata in 2025, says IDC:Video Surveillance Will Generate a Lot of Data and Enterprise, Industrial and Individual Data Will Also Surge", *ZDNe*t, 18 Haziran 2019. https://www.zdnet.com/article/iot-devices-to-generate-79-4zb-of-data-in-2025-says-idc/ [Erişim Tarihi 23.08.2023].

verinin büyüklüğü 250 milyar DVD veya 36 milyon yıllık yüksek çözünürlüklü video ile eşdeğer olduğunu düşünmek, büyüklüğü hakkında fikir verebilir. Bu büyüklükte verilerden bahsederken, bu veriyi depolama alanına yükleme veya indirme için de yüksek veri transfer hızına sahip beşinci jenerasyon (5G) mobil ağlar neredeyse anında erişim sağlayacak hız, güvenli, iletişim için elzemdir. Verinin 5G teknolojisi ile bütünleşik mobil erişim sağlanan sunucular ve veri depolama alanlarında saklanması ise kurumlar ve iş birliği içinde çalışılan şirketlerce ortak erişim sağlamasının yanında, güvenlik ve kurum içinde bu sürücüler için yer ayrılmasına ve işletilme çaba ve maliyetinin üstlenilmesine gerek kalmaması açısından avantaj sağlamaktadır.[206]

- **Büyük Veri Analitikleri:** İnsanlığın kullandığı her bir mobil iletişim vasıtası, e-posta, sensörlerce kaydedilen onca veri, kameralar ve dahası tarafından üretilen veri düşünüldüğünde bu verinin insan kapasitesiyle işlenmesinin mümkün olmayacağını söylemek zor olmayacaktır. Bu verinin işlenmesinde paternleri öğrenebilecek akıllı makinelere, ki yapay zekâ başlığı altında incelenecektir, ihtiyaç duyulmuştur. İstihbarat kurumları için büyük veri konusundaki ana sorun; dev veri havuzu içinden ilgilenilen konu ile ilişkili, çıkarım yapılarak bir değerlendirmeye ulaşmakta kullanılabilecek verinin çıkartılmasıdır. Diğer bir sorun alanı ise; bilginin göreceli doğasıdır. Kendisinden bilgi elde edilebilen verinin konuya ilişkin veri olması ve bu ilişkinin bilginin kıymetli olduğu, ihtiyaç duyulduğu zaman çerçevesinde erişilebilir olmasıdır. Bir diğer sorunsal ise ihtiyaç duyulan veriye daha hızlı erişim için, depolanan verinin cinsine (yazılı metin, coğrafi bilgi, grafik bilgi, vb.) göre sınıflandırılmasıdır. Diğer bir sorun alanıysa; doğru bilgi (gerçek) ile düzmece/yanlış/yanlı (misinformation) bilginin ayrıştırılmasıdır.[207]

  Bu büyük veriyi işleme ve depolama ihtiyacı hızla artmaktadır. Ayrı bir uzmanlık alanı ve teknoloji olarak kendine yer edinmiş bu yetenek, devlet kurumları kadar özel sektörden de talep görmektedir. Bir araştırma firması olan Global Industry Analysts'in firma değeri 2019 itibariyle 130 milyar dolar iken, bu değerin, sunduğu

[206] Timothy Buennemeyer, "A Strategical Approach to Network Defense: Framing the Cloud", *Paremeters*, C. 41, S.3, (2011), 43-45.
[207] Hershkovitz, a.g.e., 42.

hizmetlere olan talep değerlendirildiğinde, 2027 yılında 230 milyar doları aşacağı tahmin edilmektedir.[208]

Büyük miktardaki verinin işlenmesinde makine teknolojilerinin kullanılması, insan faktörünü tamamen ortadan kaldırmamıştır. İnsanların anlamlandırma, yargı çıkartma, bilgiyi tercüme etme yani yorumlama ve bu yorumlardan çıkarım yapma yetenekleri ile halen analizin önemli bir bileşeni olmaya devam etmekle birlikte, makinelerin yorumlama yeteneklerini geliştirmeye yönelik çalışmalar da devam etmektedir. Davranışsal paternleri yazılımla yorumlamaya yönelik çalışmaların davranış bilimciler ve bilgi işlem teknolojileri uzmanlarınca birlikte yürütülen çalışmaların devam ettiği, bu çalışmaların makinelerin insan odaklı analiz safhalarının bir kısmının da makinelerce üstlenilebileceğinin ilk işaretlerini vermektedir.[209]

- **Yapay zekâ ve robotik teknolojiler:** Yapay zekâ; makinelerin bulundukları ortamı algılamaları ve bu algıları doğrultusunda kendilerine atanan görevleri yerine getirme şansını maksimize edecek şekilde davranış geliştirmeleri veya insanların çalışma/öğrenme ve problem çözme gibi algısal yeteneklerini taklit etmesi olarak tanımlanmaktadır.[210] Makineler yapay zekâyı; (1) insan bilgisini basit şart/kurallara tercüme etmek, (2) makinenin çeşitli eylemleri planlama ve icrasına izin verme (birkaç seçenekten birini seçme veya iki nokta arasındaki optimum rotayı oluşturmak gibi), (3) dinamik bir veri tabanında tekrar eden sorgulamalara dayanarak makine öğrenmesi ile yeni bilgi oluşturmak olmak üzere üç seviyede uygulamaktadır.

  Görülmektedir ki veri, yapay zekâ ve makine öğrenmesi için elzemdir. Yapay zekâ ve büyük verinin birlikte kullanımının analiz yeteneklerinde yeni bir çağ açacağı, zamanla makinelerin daha sağlıklı ilişkiler kurabileceği, durumlardan daha istikrarlı çıkarımlar yapabileceği değerlendirilmektedir.[211] Bu yeteneklerin fiziki

[208] StrategyR. "Big Data World Market Report", https://strategyr.com/market-report-big-data-forecasts-global-industry-analysts-inc.asp [Erişim Tarihi: 16.07.2023].
[209] Doug Irving, "Big Data, Big Questions", *RAND Review*, Washington DC: RAND, 2017. https://www.rand.org/blog/rand-review/2017/10/big-data-big-questions.html [Erişim Tarihi: 20.08.2022].
[210] Stuart Russell, Peter Norvig. *Artificial Intelligence: A Modern Approach*. New Jersey: Pearson, 2010, 1-4.
[211] Hershkovitz, a.g.e., 44.

aktiviteye dönüştürülmesi, yani robot teknolojisi ile insan ordularının yerini robot orduların alabileceği öngörülmektedir. Örneğin; Rus askerî Endüstri Komitesi 2030 yılında ordunun muharip gücünün %30'unu robotik sistemlerin oluşturmasını ön gören bir planı onaylamıştır.[212]

Bu teknolojinin yaygınlaşması ve ucuzlamasıyla, analizleri yanlış yönlendirmek üzere 'güvenilir bilgi gibi görünen' yanlış bilgi üretiminin de mümkün olacağı değerlendirilmektedir. Bu durum, hasım tarafından toplum algısını yönlendirmek üzere uygulanan bilgi harekâtı ve psikolojik harekâtta etkinliği artıracağı düşünüldüğünde, bununla mücadelede istihbarat teşkilatlarına verinin doğruluğunu teyit gibi ilave bir yükümlülük de getireceği değerlendirilmektedir.[213]

- **Blok zincir teknolojisi:** Çevrim içi aktivitelerin güvenliğini sağlayan ve merkezi bir kontrol olmadan taraflar arası veri transferlerinin doğrulamasını sağlayan bir teknolojidir. Yönetici rolü; kişiler arası (peer to peer – P2P) ağ tabanlı bağlantı tarafından sağlanan bağımsız bir veri bloğu transferinde her bir blok gönderici ve alıcı adres bilgileri ile gönderilen veriyi barındırır. Bu sayede merkeziyetçi olmayan güvenli ve değiştirilemez bir veri transferi sağlanmış olur. Bu transferlerin kayıtları, sistemi işleten nodüllerde tutulur. Bu teknoloji, veri gönderme ve paylaşımında veriyi oluşturanın kimliğini teyit eden ve transfer esnasında verinin değiştirilmediğini garanti eden bir teknoloji olarak güvenli transfer sağlaması adına istihbarat alanında kullanım bulan/bulma potansiyeli olan bir teknolojidir.[214] Bu teknoloji; nesnelerin interneti, büyük veri analitiği, yapay zekâ arasındaki veri transferinin güvenli bir şekilde yapılmasında da kullanım alanı bulmaktadır. Birbirine veri gönderen ve aralarında güven ile ilgili şüphe oluşan durumlarda blok zincir teknolojisi, gönderilen/alınan verinin kaynağını ve transfer esnasında

[212] Karla Lant, "China, Russia and the US Are in Artificial Intelligence Arms Race", *Futurism*, 12 Eylül 2017, https://futurism.com/china-russia-and-the-us-are-in-an-artificial-intelligence-arms-race [Erişim Tarihi: 20.08.2022].
[213] Stephan De Spiegeleire, Matthijs Maas, Tim Sweijs. *Artificial Intelligence and the Future of Defense: Strategic Implications for Small and Medium-sized Force Providers*. Nederlands: Hague Centre for Strategic Studies, 2017, 100-102.
[214] Antony Lewis, *The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them* (New York: Mango Media, 2021), 12-13.

değiştirilmediğini garantilemesi açısından önemli bir teknolojik gelişme olarak kabul edilmektedir.[215]

- **Kuantum bilgi işleme teknolojisi:** Konvansiyonel bilgisayarlarda kullanılan, 1 veya 0 değerleri ile işlem yapan mikroçiplerin aksine aynı zamanda hem 1 hem 0 değeri alabilen çipleriyle kuantum bilgi işleme teknolojisi, normal bilgisayarlardan çok daha fazla veriyi işleyebilmektedir. Bu yüksek teknolojinin halen ısı hassasiyeti, nem hassasiyeti ve güvenilirlikle ilgili sorunları bulunsa da bu sorunların çözülmesi durumunda normal bilgisayarlardan kat ve kat fazla işlemci gücüne sahip olmayı vaat etmektedir. Quantum Artificial Intelligence Lab isimli araştırma kuruluşunun yaptığı Sycamore adlı prototip kuantum bilgisayar, süper bilgisayarların binlerce yılda çözebileceği birtakım problemleri birkaç dakikada çözerek bu teknolojinin ne kadar güçlü bir bilgi işlem gücü sağlayacağını göstermiştir. Bu teknoloji ile; kırılamaz kodları üretilebilir, kırılamaz denen kodlar kırılabilir. Telekomünikasyon, siber güvenlik, gelişmiş imalat, finans, tıp ve birçok endüstride köklü değişim gerçekleşmesi beklenmektedir.[216]

ABD İstihbarat topluluğunun, İstihbaratın 4'üncü dönemi olarak tanımlanan günümüzün ihtiyaçlarını karşılamak adına akademisyenlerin çalışmaları ve topluluğun önde gelen isimlerinin söylemleri doğrultusunda;

- Bahsi geçen yeni teknolojilerin toplama ve analiz fonksiyonlarını destekleyecek şekilde istihbarat topluluğunun işleyişlerine dahil edilmesi,
- Çevik ve sürekli değişime uyum sağlayan bir organizasyon kültürünün oluşturulması,
- Gerekli teknolojik altyapının oluşturulması gerekli yatırımların yapılması,
- Siber ve uzay da dahil olmak üzere her harekât tabanında etkinlik sağlayacak şekilde toplama ve analiz yeteneklerinin geliştirilmesi,
- Derin sahtecilik veya sentetik medya ve dezenformasyonla mücadele etmek üzere verinin gerçekliğini test edecek teknoloji ve metotlar ile analizlerin güvenilirliğine

[215] Jed Presgrove, "Blockchain in Government Will Boil Down to Policy, Practice", *GovTech*, 25 Eylül 2019. https://www.govtech.com/products/blockchain-in-government-will-boil-down-to-policy-practice.html [Erişim Tarihi: 19.08.2022].
[216] CBInsight, "What is Quantum Computing?", *CBInsight Research Report*, 7 Ocak 2021, https://www.cbinsights.com/research/report/quantum-computing/ [Erişim Tarihi: 19.08.2023].

tesir edecek yanlış bilginin ve toplum algısının manipüle edebilecek dezenformasyonu tespit yeteneklerinin geliştirilmesi,

- Toplanan veriyi bütünlüğünü ve güvenilirliğini bozmadan gerçek zamanlıya yakın süratte işlenmesi,
- ABD İstihbarat Topluluğu'nu oluşturan 18 kurumun Merkezi yönetilebilen fakat âdem-i merkeziyetçi uygulamalara müsaade eden ortak (uniform) bir işleyiş, bilgi paylaşımı ve koordinasyonunu geliştirilmesi,
- Personelin etkinliğini maksimize etmek üzere bu alanlarında yetenekli gençler ile tecrübe sahibi nitelikli personelin cezbedilerek istihdamının sağlanması,
- Farklı bakış açıları ve uzmanlıklardan faydalanmak adına geniş bir mesleki yelpazeden yetenekli personelin istihdamının,
- İstihbarat topluluğu ile pek çok alanda bu topluluğa destek sağlayan özel sektör ile daha geniş ve derin iş birliğinin gerektiği çıkarımını yapmak mümkündür.

Gerek akademik çevrelerin özellikle 2014 sonrası istihbarat topluluğunun geleceğine yönelik çalışmaları ve istihbarat topluluğunun yönetim kademesinin de yaptığı öz eleştiriler, anlayış, organizasyonel yapı ve analiz yöntemlerinde bir dönüşümün gerekliliğini vurgulamaktadır. Özel sektör, toplum, akademi ve karar vericiler ile istihbarat topluluğu arasında iş birliğine dayalı bir yaklaşım (Collaborative Approach), yoğun olarak yeni teknolojilerden azami istifade etmek üzere teknolojinin entegrasyonu ve geleneksel analiz yöntemlerinin günümüz şartlarına göre tekrar gözden geçirilerek güncellenmesi istihbaratın dönüşümü kapsamında tavsiye edilen konseptler olarak öne çıkmaktadır. Özellikle anlayış değişimi kapsamında, doğası gereği muhafazakâr olan istihbarat fonksiyon alanının özel sektör ile iş birliğinin genişletilmesi ve derinleştirilmesine yönelik görüşler çokça tartışılsa da avantaj ve dezavantajlarıyla ABD istihbarat topluluğuna 20'nci yüzyılın ortalarından beri çeşitli alanlarda destek sağlamalarının, bu iş birliğinin kuvvetlendirilmesinde kolaylaştırıcı rol oynadığı ön görülebilir. ABD istihbarat topluluğu özelinde, çağın gereksinimlerine uyum sağlama kapsamında bir çözüm yolu olarak önerilen özel istihbarat şirketleri ile iş birliği ve istihbarat ihtiyaçlarının dışarıdan teminin detaylı incelenmesinde fayda vardır.

4. BİR ÇÖZÜM YOLU OLARAK ÖZELLEŞME

Singer, uzmanların özel askerî sektörün ortaya çıkışı ve devletlerce kabul görmesi hususunda üç ana neden üzerinde uzlaştıklarından bahsetmektedir. Bunların ilkini, Soğuk Savaş dönemi sonrasındaki serbest pazar ekonomisinin özelleşme dalgasını beraberinde getirmesi; ikincisini, orduların küçülmesi ile sürdürülmesi gereken hizmetlerin dışarıdan tedarik edilme ihtiyacının doğması ve üçüncüsünü de süper güçlerin gelişen dünyaya müdahale etme isteği ve bunun için dolaylı yol olarak özel şirketleri kullanma arzusu olarak sıralamaktadır.[217] Ayrıca politik kaygılarla yüksek riskli bölgelerde askerî zayiat miktarını düşük göstermek üzere, muharip unsurlar da dahil olmak üzere kimi hizmetlerde dışarıdan teminin tercih edilebildiği gözlemlenmektedir. Harekâtta dahi pek çok alanda dışarıdan hizmet temini günümüz çatışma ortamının bir gerçeği haline dönüşmüşken, gelişen teknolojiyle yetenekleri kamu kurumlarının ötesine geçen özel şirketlerden istihbarat fonksiyon alanını desteklemek üzere faydalanılmasını göz ardı etmek mantıksız karşılanmaya başlamıştır.

İstihbarat elde etmek üzere iletişimin dinlenmesi 1840'lara, telgraf hatlarının dinlenmesine dayansa da telekomünikasyon hizmetinin sağlanmasında 1940'lardan itibaren özel şirketlerin sektörde ağırlığının artması devletlerin resmî kurumlarını özel sektör ile bu alanda iş birliğine yöneltmiştir. 1940'ların sonlarından itibaren telekomünikasyon şirketlerinden telefon/telgraf dinlemelerinin paylaşılması bağlamında destek almaları istihbarat elde etmede özel sektörden destek alınmasının ilk örnekleri olarak kabul edilmektedir. Devlet kurumlarının elinde olmayan teknik yeteneklerde özel sektörden destek alınması genel kabul görmüş bir uygulama olmakla birlikte, özellikle 11 Eylül 2001 terör saldırılarından sonra özel sektörün istihbarat alanında tarihte hiç olmadığı kadar büyük oranda katkı sağladığı ve ABD istihbarat topluluğu içinde hatırı sayılır bir ağırlığa sahip hâle geldiği görülmektedir.

[217] Peter W. Singer, "The Private Military Industry and Iraq : What Have We Learned and Where to Next?", *Geneva Centre for the Democratic Control of Armed Forces (DCAF) Policy Paper*, Kasım 2004. https://www.files.ethz.ch/isn/14132/PP4_Singer.pdf [Erişim Tarihi: 02.04.2022].

Günümüzde değişen ve genişleyen güç mücadelesinde karar vericilere en önemli desteği sağlayan istihbarat alanında özelleşmenin, güvenlik odaklı istihbarat bakış açısı ile güç kullanımının icrasının esaslarını belirleyen doktrinel değişimden ve istihbarat alanındaki dönüşümden ayrı tutularak incelenmesi sağlıklı sonuçlara ulaştırmayacaktır. Sağladığı avantajlar kadar pek çok mahsurları da doğasında barındıran özel sektör istihbaratı, bir meslek dalı olarak da zanaattan bilimselleşmeye doğru gelişimini sürdürmektedir.

Faydaları ve mahsurları ile çokça tartışılan ve istihbaratın dışarıdan temini olarak da ifade bulan, istihbaratın özelleşmesi, bu alandaki gelişmelere öncülük eden ve kendi istihbarat topluluğu ile en kapsamlı iş birliği içinde bulunan ABD örneği üzerinden açıklanmaya çalışılmıştır.

Bu bölümde; dönüşen güç mücadelesi ve bu mücadelenin icrasındaki doktrinel dönüşüm içinde değişen istihbarat ihtiyaçları, bunları karşılamada bir çözüm seçeneği olan dışarıdan temini, dışarıdan teminin tarihsel gelişim sürecini, bu süreçteki evrimleşmenin fayda ve mahsurlarını irdeleyerek, istihbarat gibi doğasında mahremiyet barındıran bir alanın özel sektör istihbaratı ile en uygun entegrasyonunun nasıl olması gerektiğinin ortaya çıkartılması amaçlanmıştır.

4.1. Özel Sektör İstihbaratı

Özel sektör istihbaratı; bir şirketin kaynak veya işleyişine veya istihbarat hizmeti alan devlete direkt fiziki veya saygınlığına tehdit oluşturabilecek muhtemel hasım aktörler, zararlı küresel faaliyetleri engelleme veya bu konuda oluşabilecek risk konusunda durumsal farkındalık yaratmak üzere stratejik ve/veya taktik bilgiyi, açık kaynak istihbaratı, sosyal medya istihbaratı ve insan istihbaratı vasıtaları ile toplama, analiz etme ve yayımlama olarak tanımlanabilir.[218] Hatta toplama metotlarına sinyal ve teknik istihbarat yeteneklerini de dahil etmek yanlış olmayacaktır. Özel sektör istihbaratının maksadı, yöneticiler, karar vericiler, paydaş ve çalışanlara karşı karşıya kalınması muhtemel riskler ve tehditler konusunda erken ikaz ile bahse konu iş kolu

[218] Maria Robson-Morrow, "Private Sector Intelligence: on the Long Path of Professionalization", *Intelligence and National Security Journal*, C. 37, S. 3 (2022), 402-403. https://www.belfercenter.org/publication/private-sector-intelligence-long-path-professionalization [Erişim Tarihi: 02.08.2022].

veya güvenliğin tesisine yönelik çabaların emniyetle devamını sağlamaktır. İç ve dış tehditlere yönelik analizler, risk değerlendirmeleri ve bilgi paylaşımı kapsamında devletin istihbarat kurum veya kurumlarının (topluluğunun)[219] ile irtibat ve iş birliğinin sağlanması ilave sorumluluklar olarak öne çıkmaktadır.[220] Morrow ise, çeşitli kaynaklardan derlediği tanımında özel istihbarat faaliyetlerini; kanuni ve açık bir şekilde stratejik karar mekanizmasını desteklemek, jeopolitik ve güvenlik kökenli riskleri asgariye indirmek üzere devlet dışı organizasyonlar tarafından istihbarat tekniklerinin uygulanarak analizlere dayalı istihbarat oluşturulması olarak tanımlamaktadır.[221]

Açık Kaynak İstihbaratı uzmanları uzun zamandır gizliliği bulunmayan verinin toplama ve analizinde özel şirketlerin rolünün artırılmasını savunmaktadır. Bu iddiaları da özel şirketlerin çok miktardaki belli formata göre düzenlenmemiş veriyi toplama, işleme ve yorumlamada son teknolojinin nimetlerinden daha fazla faydalanabiliyor olmalarına dayanmaktadır. Mercado; açık kaynaktan elde edilecek istihbarattan azami fayda elde etmek için, istihbarat kurum veya kurumlarının (topluluğunun) kendi açık kaynak İstihbaratı teknik imkânlarını, gelişmiş makine-destekli ses/video yorumlama yazılımları, daha akıllı arama motorları ve daha gelişmiş araçlara sahip özel sektörün toplama, analiz, üretim ve yayım imkânlarına bağlaması gerektiğini söylemektedir.[222]

İstihbaratta özelleşmeyi savunan pek çok akademisyen ve istihbaratçı, özel sektörün yeni tehdit paradigması karşısında devletin hantal yapısı ve işleyişine nazaran kendini daha iyi teçhiz ettiğinden bahsetmektedir. Geleneksel askerî istihbarat metodolojisinin odağını muharebe düzenlerini ortaya çıkarmaya yönelik analizler, emareler ve ikazlar ile, tehdit odaklı teknik ölçümlerin oluşturduğu düşünülürse; günün değişen, genişleyen ve derinleşen harekât ortamında ortaya çıkan uluslararası terörizm ve diğer konvansiyonel olmayan tehditlere karşı devlet imkânlarının yetersiz kalabileceği çıkarımında bulunmak yanlış olmayacaktır. Günümüz muharebe sahasının aktörleri arasında artık kalıcı bir yer edinmiş olan terörist örgütler ile çeşitli ülkelerin birlikte

[219] Bir ülkedeki istihbarat ile görevli kurumların tamamını tanımlamak için kullanılmıştır.
[220] Torres-Baches, Efren R. "Welcoming the New Age of Intelligence", *Journal of European and American Intelligence Studies*, C. 1, S. 2 (2018): 22.
[221] Morrow, a.g.e., 2.
[222] Stephen C. Mercado, "Sailing the Sea of OSINT in the Information Age a Venerable Source in a New Era Sailing the Sea of OSINT in the Information Age" *Studies in Intelligence; Journal of the American Intelligence Professional*, C. 48, S. 3 (2004): 9.

çalıştığı devlet dışı silahlı/silahsız oluşumların faaliyetlerinin takibi için gerekli faydalı bilginin çoğunlukla finansal transferler, genel ağ (internet) üzerinden yapılan haberleşmeler ve büyük miktardaki belli formata sahip olmayan yazı ve verinin analizine dayandığı bir gerçektir.[223] Bahse konu analizler incelendiğinde, birçok özel sektör şirketince normal mesainin bir parçası olarak yapıldığı görülmektedir. Özellikle finansal analizler, nakit akışı ve varlık transferlerinin takibi finans danışmanlık şirketlerince; kritik ve çift kullanım alanına sahip malzemelerin küresel bazda yer değiştirmesinin takibi uluslararası lojistik şirketlerince; siber alandaki iletişim ve sosyal medya analizleri siber güvenlik firmalarınca; büyük veri analizleri ise düşünce kuruluşları ve istatistik/veri analiz şirketlerince normal iş tanımları içinde her günkü olağan iş olarak işlenmekte ve kıymetlendirilmektedir. Bu bağlamda, istihbaratı desteklemek üzere terörist örgütler ile mücadele ve devlet dışı oluşumlar ile mücadelede de bu yeteneklere sahip şirketlerin imkânlarından destek almak kadar normal ne olabilir?

Daha önce de belirtildiği gibi devletler yüksek teknolojiye haiz, gizli istihbarat yeteneklerini bu bağlamda geliştirirken, bu sistemlerden elde edilecek istihbaratı açık kaynak verileriyle destekleyerek güvenilirliğinin artırılması ve/veya emarelerin değerlendirilmesi ile olası tehditlere toplama vasıtalarının vakitlice yönlendirilmeleri sürprizin önüne geçilebilmesi için elzemdir. Dolayısıyla, gizliliğe sahip sistemler ile açık kaynaklardan elde edilen istihbaratın entegrasyonu çağın bir gereksinimi; açık ve gizli kaynaktan elde edilecek istihbaratın teminine yönelik gayretlerden tasarruf etmek ve hali hazırda mevcut olan sivil kaynaklı yeteneklerden istihbarat alanında da faydalanma, soruna ilişkin mantıklı bir çözüm olarak belirmektedir.

4.2. Neden Özelleşme?

Küresel güvenlik ortamının, güç mücadelesinin dönüşümü ile her geçen gün eklenen yeni aktörler ve yetenekler ile karmaşık bir hal alması karar vericilerin sağlıklı değerlendirmelere ihtiyaç duymalarına, bu da daha fazla istihbarat ihtiyacının ortaya çıkmasına sebep olmuştur. Her seviyede karar verici, karşı karşıya kaldığı risklere rağmen doğru karar vermek ve yerinde uygulamalar için; zamanında, güvenilir, mantıklı ve icraata geçirilebilir değerlendirmelere ihtiyaç duyar. Hızla değişen,

[223] Glenn James Voelz, *Managing the Private Spies: the Use of Commercial Augmentation for Intelligence Operations* (Washington DC: Joint Military Intelligence Collage Press, 2006), 20-21.

dönüşen ve erişilebilir verinin tarihte hiç rastlanmadığı kadar arttığı günün güvenlik ortamında nitelikli verinin toplanması, analizi ve anlamlı değerlendirmelerle karar vericilerin desteğine sunulmasına olan ihtiyaç hiç olmadığı kadar önem kazanmıştır. Bu durum, konusunun uzmanı, güvenilir, mesleki eğitim, bilgi ve tecrübeye sahip analizcilerin istihdamını gerekli kılmaktadır.[224]

Özellikle Soğuk Savaş sonrasında her anlamda küçülen istihbarat kurumları, 11 Eylül saldırıları ile alışık olmadıkları coğrafya ve düşman tipine karşı yürütülecek mücadelede kendilerinden talep edilen acil ve güvenilir istihbaratı karşılamada yetersiz kalmıştır. Elbette sahadaki elemanlara bölgesel dilleri öğretmek veya görev yapmakta oldukları coğrafyadan bir anda ihtiyaç duyulan mekâna kaydırmak mümkün olmamıştır. Tarihin belki de en büyük terör saldırısı ve ardından ilan edilen "terörle küresel savaş", ortaya çıkan acil istihbarat ihtiyacının karşılanmasında istihbarat desteğinin büyük oranda dışarıdan temin edilmeye çalışılmasının en önemli nedeni olarak görülmektedir.[225] Bush yönetimi ve ABD Kongresi, müteakip terör olaylarını önlemek adına istihbarat bütçesi için ciddi bir artış yapmış, terörle mücadele için Ulusal Terörle Mücadele Merkezi (*National Counterterrorism Center*) gibi yeni kurumların hayata geçirilmesinin yanında Merkezi Haber Alma Ajansı (CIA) ve diğer istihbarat ajanslarına binlerce analist ve insan istihbaratı (İNİS) uzmanının istihdamı konusunda yetki vermiştir. Ancak 1990'ların büyük kesinti ve küçülmeleri neticesinde güvenlik yetkisi-kleransı sahibi yetişmiş istihbarat personelinin bünye dışına çıkartılması neticesinde artık özel sektörde çalışıyor olmaları, ortaya çıkan bu acil gereksinimin hizmet alımı şeklinde özel sektörden karşılanması yoluna gidilmesi ile sonuçlanmıştır.[226]

Bu kısa vadeli hızlı çözüm, daha sonra uzun vadeli bir bağımlılığa dönüşecektir. Ulusal İstihbarat Ofisi Direktörlüğünün (*ODNI*)[227] 14 Mayıs 2007'de bir endüstri konferansında verdiği brifingde istihbarat üretmek üzere özel sektöre ayrılan bütçenin 42 milyar dolar - genel istihbarat bütçesinin %70'i - oluşturduğunu tarihte ilk defa

[224] Justin Crump, *Corporate Security Intelligence and Strategic Decision Making* (Boca Raton: CRC Press Taylor & Francis Group, 2015), 20-22.
[225] Mark Galeotti, *The Weaponisation of Everything: A Field Guide to The New Way of War* (Cornwall: Yale University Press, 2022), 61.
[226] Tim Shorrock, "The Corporate Takeover of U.S. Intelligence", *Salon*, 2007. https://www.salon.com/2007/06/01/intel_contractors/ [Erişim Tarihi: 14.05.2022].
[227] Ulusal İstihbarat Ofisi Direktörlüğü (Office of the Director of National Intelligence-ODNI) 2004 yılında ABD'nin 16 istihbarat ajansının faaliyetlerini koordine etmek üzere kurulmuştur.

açıklanacaktır.[228] Aynı brifingde bir slaytta yer alan "Satın almazsak istihbarat da yapamayız" (*"We can't spy … If we can't buy!"*) ifadesi ise bu bağımlılığın ABD'de istihbaratın dışarından temininin tüm ABD istihbarat gayretlerinde ne kadar büyük bir pay sahibi haline geldiğini istihbarat tarihine yazdırmıştır.[229]

Kinetik güç kullanımını ve espiyonaj faaliyetlerini içermeyen - kanuni ve açık olarak - daha çok açık kaynaklardan elde edilen coğrafi, jeopolitik, fiziki güvenlik ve siber güvenlik gibi alanlarda hizmet sunan özel sektör istihbaratı, taktikten stratejik seviyeye kadar karar mekanizmasını desteklemektedir. Önceleri çoğunlukla teknik konularda destek sağlanırken sonrasında bilgi işlem güvenliğinden telekomünikasyon verilerini toplamaya kadar teknik alanların yanında, analiz yetenekleri ile özel istihbarat şirketleri nitelikli istihbarat ürünleri ve istihbarat taleplerinin karşılanmasında sorumluluğun paylaşılması boyutuyla resmî istihbarat kurumlarını destekleyen cazip bir çözüm olarak kabul görmüştür.

4.3. İstihbaratta Özelleşmenin Tarihsel Gelişimi – ABD İstihbarat Modeli

ABD istihbarat topluluğunun özel sektör ile iş birliğinin çok eskilere dayandığı ifade edilmekle birlikte, özel sektörden talep edilmiş kayda geçen ilk desteğin; 1940'lı yılların sonlarına doğru Ulusal Güvenlik Ajansı (NSA)'nın iletişim şirketleri olan *Western Union* ve *AT&T* başta olmak üzere diğer birkaç telekomünikasyon şirketi ile yurt dışı telefon görüşmelerinin dinlenmesi ve telgrafların okunmasına ilişkin mutabakatları gösterilmektedir. Aynı dönem içinde AT&T'nin aynı şekilde Merkezi İstihbarat Ajansı (CIA) ile de iş birliği içinde olduğu bilinmektedir. 1950'lerin başında bilişim teknolojilerinin gelişmesi ile *IBM, Bell Laboratories* ve *Cray* gibi firmaların NSA için diplomatik ve askerî mesajların kriptolarını kırmak, büyük miktardaki sinyal istihbaratının uygulanabilir istihbarat geçirilmek üzere analiz edilmesine yardımcı olacak ilk süper bilgisayarlar ile kripto çözme teçhizatını ürettiği bilinmektedir. Bu dönemde özellikle bilgi sistemleri ve telekomünikasyon şirketlerinin küresel çapta CIA ve NSA'e teknik danışmanlık ve servis sağlama kapsamında destek oldukları görülmektedir. Günümüzde özel sektörün istihbarat alanında en büyük şirketleri, faaliyetlerine resmî istihbarat ajanslarına teknik destek sağlayarak başlamıştır.[230]

[228] Shorrock, 2008, 50 (e-kitap).
[229] Galeotti, 2022, 61.
[230] Shorrock, 2008, 96 (e-kitap).

ABD'nin istihbaratta özelleşme alanında imzaladığı ilk projelerin Sovyet Sosyalist Cumhuriyetler Birliği'nin Soğuk Savaş dönemi nükleer kabiliyetlerini tespit ve izleme ihtiyacı, uzay yarışı ve Kruşçev'in 1958 Berlin Ültimatomu ile II. Dünya Savaşı'nın eşiğine gelinmesinin etkili olduğu söylenebilir.[231] 1958'de başlayan, 1960'da imzalanan ve Sovyetler Birliği ve Çin Halk Cumhuriyeti'nin en mahrem bölgelerinde nükleer yeteneklerinin gözetlenmesini amaçlayan iki önemli proje, istihbaratın özelleşmesi alanında mihenk taşı kabul edilmektedir. İlk proje *Lockheed Corporation* firmasına verilen U2 casus uçak projesi; ikincisi ise *TRW, General Electric, Eastman Kodak, Itek Corporation* ve *Poloroid* firmalarına kontrat edilen CORONA casusu uydu projesidir.[232] Bu projelerin hayata geçirilmesi ile çok gizli Sovyet askerî tesis ve yeteneklerinin çok yüksek irtifa ve atmosfer dışı uzaydan o ana kadar görülmemiş çözünürlükte ve detayda fotoğraflanması mümkün olmuştur. Her iki proje de havadan/uzaydan gözetleme konularında öncü olarak alanlarındaki diğer çalışmalara ilham kaynağı olmuştur.

1980'lerde Reagan yönetimi, 2000'li yılların başlarına kadar gizliliğini sürdüren, olası bir nükleer saldırıda ABD yönetiminin ortadan kalkması durumunda ülkeyi yönetmeye devam edecek gölge bir hükümet oluşturan büyük bir projeyi hayata geçirmiştir. "Hükumetin Devamı" (*Continuity of Government – COG*) olarak kısaltılan ve "*Armageddon* Projesi" olarak da bilinen bu gizli devlet projesi daha önce devlet kurumlarında önemli makamlarda çalışmış sivillerin, olası bir nükleer felakette gizli bir lokasyonda toplanarak ABD'yi yönetmeye devam etmesini esas aldığı, bu gölge hükümetin, Batı Virjinya eyaletinde *Greenbrier* Tatil Tesisinde inşa edilen devasa sığınakta[233] ve Pensilvanya'da bir özel çiftlikte yılın belli dönemlerinde gizli toplantılarda bir araya geldikleri gazeteci James Mann tarafından 2002 yılında ortaya çıkartılmıştır.[234] Projenin önemli isimlerinden Donald Rumsfeld, Dick Cheney gibi birçok ismin güvenlik/istihbarat sektöründe özel şirketlerin yönetim kurullarında görev yapmaya devam ederken bu gölge hükümette görev almaları, müteakiben projeyi desteklemeye devam eden Bush yönetiminde de bakan/direktör seviyesinde

[231] Şükrü. S. Gürel, "Berlin Sorunu (1944-1972)", *Ankara Üniversitesi SBF Dergisi*, C. 32, S. 1 (1977), 217-218.
[232] Shorrock, 2008, 138-139 (e-kitap).
[233] NPR, "The Secret Bunker Congress Never Used", *NPR*, 2011. https://www.npr.org/2011/03/26/134379296/the-secret-bunker-congress-never-used [Erişim Tarihi: 20.05.2022].
[234] James Mann, *Rise of the Vulcans: The History of Bush's War Cabinet* (New York: Penguin Group, 2004), 16-18.

görev almalarının, *Armageddon* Projesinin istihbaratın özelleşmesi ve özel istihbarat sektörünün büyümesinde katalizör rolü oynadığı ifade edilmektedir. Clinton yönetimi bu projeye sıcak bakmadığından sürdürmemiş olsa da özel istihbarat sektörü yöneticilerinin kritik devlet kadrolarında görev almaları ve görevlerinin bitiminde tekrar özel savunma sanayii/istihbarat şirketlerinde yönetici olarak görev almaları sektörün gelişiminde önemli rol oynamıştır.

Clinton yönetimi döneminde Sovyetler Birliğinin dağılması ve Soğuk Savaşın sona ermesi, Çin'in kapitalizmi benimseyen politikaları neticesinde savunma hükümet politikasında önceliğini kaybederken, savunma ve istihbarat bütçelerinde ve istihdamda önemli kesintilere gidilmiştir. Bu politikalar neticesinde; savunma sanayii ve istihbarat alanında küçülme ve özellikle 1997 yılından itibaren bu ihtiyaçların dışarıdan teminine ağırlık verilmiştir.

11 Eylül 2001 terör saldırısının ABD üzerinde yarattığı etki ve neticesinde faturanın istihbarat topluluğunun yetersizliği ile koordinesizliğine kesilmesi, acil ihtiyaç duyulan istihbaratın dışarıdan temininin kısa vadede cazip bir çözüm olarak tercih edilmesine neden olmuştur. Acil ihtiyaçlar hem istihbarat bütçesinin artmasına hem de bu bütçenin ihtiyaçları karşılayabilecek özel şirketlere kontratlar olarak aktarılmasına neden olmuştur. İstihbarat şirketlerine 2002 yılında ABD istihbarat bütçesinden ayrılan 32 milyar $, 2005 – 2007 döneminde ise yıllık 43,5 milyar $ seviyelerine yükselmiştir.[235] 2007 yılında toplam kontrat değeri 400 milyar $ seviyesine yükselmiştir ki bu gelir seviyesine yükselen şirketler, ABD Hükumeti üzerindeki nüfuzları nedeniyle 'Gölge Hükumet' olarak anılmaya başlanmıştır. İlginçtir ki istihbarat kontratlarını çevrim içi kontrol eden Federal Satın alma Veri Tabanı dahi özel istihbarat şirketi tarafından kontratla işletilmektedir.[236] Bir özel istihbarat şirketi olan SAIC'in 2007 yılındaki başkanı olan Kenneth C. Dahlberg bir konferansta 'hükumet hayatta kalabilmek için dışarıdan temine devam etmek zorundadır' ifadesiyle ABD istihbarat topluluğu ve dolayısıyla ABD yönetiminin ulusal güvenliğin sağlanmasında özel istihbarat şirketlerine ne kadar bağımlı hale geldiğini göstermiştir.[237]

[235] Shorrock, 2008, 97-100 (e-kitap).
[236] Shane Nixon, Ron Nixon"In Washington, Contractors Take on Biggest Role Ever". *New York Times*. 7 Şubat 2007 https://www.nytimes.com/2007/02/04/washington/04contract.html [Erişim tarihi 02.08.2022].
[237] Shorrock, 2008, 68 (e-kitap).

Özetlemek gerekirse; ABD'de istihbaratta özelleşmenin bir sektör olarak gelişimini dört ana gelişme çerçevesinde anlatmak mümkündür. Bu dönemleri, (1) Reagan döneminde bir anlayış değişimi ile birlikte özellikle teknik konularda özel şirketlerin sektöre dahil olmaları; (2) Clinton döneminde izlenen politikalar gereği personel ve bütçe kısıtlamaları neticesinde 1990'ların sonlarına doğru ihtiyacın dışarıdan teminine yönelik eğilimlerin artması; (3) istihbarat topluluğu kapasitesindeki daralmanın çözümü olarak CIA Direktörü George Tenet'in özel sektör istihbaratını destekleyen uygulamaları; (4) 11 Eylül saldırılarının yarattığı acil istihbarat ihtiyaçlarının derhal karşılanması için kısa vadeli çözüm olarak dışarıdan temininin bir kurtarıcı olarak görülmesi ve özel sektörün imzalanan dev bütçeli ve uzun vadeli kontratlarla ABD istihbarat topluluğunda yerini belki de dönülmez bir şekilde sağlamlaştırması olarak ifade edilebilir.[238]

İstihbarat teşkilatlarının özel sektör ile iş birliğinin temelinde; teknolojiye hızlı ulaşım ve bu alanlardaki uzmanlığa erişimde rekabet etmekten ziyade ilgili alanın uzmanlarından ihtiyaç duyulan istihbaratın oluşturulmasında iş birliği içinde istenenlerin sağlanması olduğu görülmektedir. Resmî istihbarat kurumları ihtiyaç duyulan alanlarda hizmet satın alarak sektörel gelişimin motivasyonunu sağlarken, özel şirketlerin teknolojiye hakimiyet, ilgi sahasına göre istihdam esnekliği, değişen coğrafya ve tehditlere kolay adaptasyonu avantajlarından faydalandığı görülmektedir. Bu da çeşitli olumsuzluklarına rağmen istihbaratın dışarından temininin tercih sebeplerinin başında gelmektedir

4.4. Özel İstihbarat Şirketlerinin Üstlendikleri Fonksiyonlar

Genel olarak istihbarat şirketlerinin faaliyetleri incelendiğinde; operasyonel destek (uydu aracılığı ile hedef takibi, yabancı ülkelerde insan kaynağı temini, sorgulama gibi hizmetler, aranan teröristlerin isim, adres, iletişimde olduğu gruplar hakkında bilgi temini ve bu teröristlerin karışmış olabilecekleri potansiyel şiddet eylemleri hakkında bilgi vb.), teknik destek (İstihbarat teşkilatlarının teknik konularda ihtiyaç duydukları yazılım ve donanımsal çözümler) ve analitik destek (veri analizi, internet servis sağlayıcıları veya telefon operatörleri vb. şirketlerin müşteri verileri üzerinden

[238] Shorrock, 2008, 134-205 (e-kitap).

yaptıkları analizler gibi) olarak üç ana fonksiyonda rol aldıkları görülmektedir.[239] Bahse konu her bir destek fonksiyonu zaman zaman farklı istihbarat veya özel askerî şirketlerce, bazen de her üç fonksiyon alanında da destek sağlayan büyük istihbarat şirketlerince (Booz Allen Hamilton, CACI, General Dynamics, vb.) karşılanmaktadır.[240]

Ana görevler bağlamında açık kaynaklardan ve özel şirketler üzerinden nasıl desteklenebileceği incelendiğinde;

- Stratejik sürprizi engellemeye yönelik erken haber alma ve ikaz kapsamında: Hasım devletlere ve devlet dışı silahlı örgütlere ait kuvvetlerinin hareketliliği, harekât hazırlıkları görüntü, sinyal ve ölçme/imza istihbaratı ile gözetlenmeye ve olası değişiklikler karar mercilerine harekât icra edilebileceğinin bir emaresi olarak aktarılmasında rol oynayabilir. Bu tespitlerden çok daha önce hasım unsurların silahlanma faaliyetleri, savunma bütçesindeki artış, bu bütçeden belli askerî yeteneklere yapılan harcamalar, imzalanan yetenek artırıcı projeler, politik söylemler, belli bölgeye yönelik ilginin artması gibi emareler açık kaynaklardan tespit edilerek çok erken ikaz sağlayabilir. Açık kaynaktan elde edilen emarelerin değerlendirilmesi, gizli istihbarat sistemlerinin doğru tehdide yönlendirilmesini ve tehdidin bu sayede daha önceden tespitine imkân verebilir.

- Bir bölgeye yönelik istihbarat hazırlığı kapsamında: Bir harekât planının hazırlanmasına ışık tutmak üzere hazırlanan istihbarat hazırlığında askerî istihbarat yetenekleri ile muharebe sahasına ilişkin analizler yapabilir. Bu bağlamda;

  - Coğrafi bilgi sistemleri temelli çalışan özel sektörün[241] kullandığı uydu görüntüsü analiz yazılımları ile arazi etüdü,

  - Harekât alanındaki sivil halkı tanımaya yönelik sosyo-kültürel analizler,

  - Halkın gelişmeler hakkında görüşlerini tespit etmek üzere icra edilen sosyal medya analizleri,

[239] Frederic Lemieux, "The Rise of the Private Intelligence Sector". *Intelligence and State Surveillance in Modern Societies* (Bingley: Emerald Publishing Limited, 2018),193.
[240] Tim Shorrock, age. Sf.235-273 (e-kitap).
[241] Petro-kimya şirketleri, madencilik sektörü gibi yer kabuğunu inceleme üzerine çalışan şirketler.

- Konvansiyonel olmayan unsurlarca düzenlenebilecek saldırılarda kullanılmak üzere temin edilmeye çalışılan kritik patlayıcıların küresel hareketleri uluslararası ticaret ve lojistik şirketlerinin takip kabiliyetleri,

- Örgütlerin eylem, silahlanma, eleman temini vb. faaliyetlerini tespit etmek için önemli bir emare olan finans akışını takip etmeye yönelik finansal analiz yetenekleri,

- Son dönemde bankacılık sistemini aradan çıkartarak örgütler arası gizli para transferine imkân sağlayan blok zincir (*Blockchain*) teknolojisini, özellikle transferlerde sağladığı gizlilik nedeni ile tercih edilen Monero Kripto Paranın[242] izlerini takip ve algoritmasının çözümü için bu alanda faaliyet gösteren bilişim firmalarının uzmanlığı ve yetenekleri[243] ile destek sağlayabilirler.[244]

- Cari durumun takibi ve güncellemesi kapsamında: Harekât bölgesindeki durumun güncellenmesi ve takibi maksadıyla sivil gözetleme sistemleri, bölgede faaliyet gösteren insani yardım kuruluşları ve sivil şirketlerin irtibatları vasıtaları ile operasyonel destek verebilirler.

- Hedef tespiti, teşhisi ve ateş destek vasıtalarına bildirilmesi kapsamında: Hedef istihbaratını desteklemek üzere, teknik istihbarat, uydu ve hava gözetlemesi, ölçme ve ölçüm ve iz istihbaratı (MASINT)[245] konusunda devletlerin kendi yeteneklerine ilave yetenekler sunabilirler.

- Kuvvet koruma istihbaratı (Beka, harekât güvenliği, birlik güvenliği): güvenlik ve bilişim teknolojisi üzerine uzmanlaşmış şirketler aracılığı ile harekât bölgesindeki telekomünikasyon ve internet üzerinden icra edilen haberleşmenin süzülerek tehdit emaresi veren haberleşmenin dinlenmesinin yanında yine gözetleme (Hava ve uydu) imkânları sunabilirler.

---

[242] Marissa Bruder, Caroline Hilty ve Michelle Kaplun. "The Crypto Current: An Analysis of Monero Report", *The Counterterrorism Group - Illicit Finance Team*, (2021), 1-3.

[243] ABD İç Güvenlik Bakanlığı, Monero transferlerinin takibi ve algoritmasının çözümü için Cypher Trace şirketinden teknik destek almaya başlamıştır. Ayrıca ABD İç Gelir Servisi Monero'nun gizlilik özelliğinin kırılması için 625,000 ABD Doları ödül koyduğunu duyurmuştur (Mapperson, 2020).

[244] Sebastian Sinclair "CipherTrace Says Homeland Security Work Gave Rise to Monero-Tracking Patent Filings", *Coindesk*, 2020. https://www.nasdaq.com/articles/ciphertrace-says-homeland-security-work-gave-rise-to-monero-tracking-patent-filings-2020 [Erişim Tarihi: 10.05.2022].

[245] Boeing firması Uydu sistemi ile https://www.boeing.com/space/boeing-satellite-family/ , Airbus firması Earth Observation Constallation sistemi ile https://www.airbus.com/space/earth-observation.html gözetleme, ölçme ve imza istihbaratı faaliyetlerini ABD İstihbarat Topluluğu ve talep eden diğer ülkeler için ticari olarak yürütmektedir.

- Harekât alanı hasar kıymetlendirmesi: Özel sektöre ait uydu ve hava gözetleme vasıtaları ve benzeri yetenekler, açık kaynak veri ve yetenekleri kullanılarak devlete ait kurumlar ve/veya özel sektör tarafından elde edilebilecek verilerin analiz ile askerî istihbarata destek sağlanabilir.[246]

4.5. İstihbaratın Özelleşmesinin Olumlu Yönleri

Jones ve Newburn'a göre devletleri dışarıdan istihbarat temin etmeye yönelten nedenlerin başında finansal kısıtlamalar gelmektedir. Devlet harcamaları üzerindeki kısıtlamalar, arzu edilen alanlarda yetenek geliştirme ve personel istihdam etme maliyetleri yerine, bahse konu hizmetlerin dışarıdan hizmet alımı şeklinde karşılanmasını maliyet etkin hale getirmektedir.

Bir diğer faktör ise yeni istihbarat gereksinimleri için gerekli organizasyonel değişikliklerin kaynak (yetenek, altyapı, personel) maliyetinin yanında aynı zamanda ve belki daha da önemli olarak zaman kısıtı, aciliyetidir. Karakteristik olarak istihbaratın zaman zaman gri ve karanlık alanları kullanması gerekliliği de dikkate alındığında, bazı konularda özelleşmenin bir nedeni de devlet kontrolünden kaçmak olduğu söylenebilir. İstihbarat kurumları talep edildiğinde meclis komisyonları önünde açıklama yapma zorunluluğu içindeyken sivil şirketlerin bu gibi bir sorumluluğu yoktur.[247]

Özel sektörün istihbarat alanındaki uzman personele sağladığı imkânların devlet kurumlarınca sağlananın hayli üzerinde[248] olduğu dikkate alındığında, kalifiye personelin devlet kurumlarında yetiştikten sonra özel şirketlere geçmeleri de özel şirketlerden alınacak hizmetin kalitesini yükselten ve bu nedenle tercih edilmelerini destekleyen bir etken olarak öne çıkmaktadır.

Ülkelerin istihbarat teşkilatları veya silahlı kuvvetlerinin erişiminin kısıtlı veya mümkün olmadığı bölgelere sızma ve o bölgelerde faaliyet gösterme imkânlarının olması özel şirketlerce sağlanabilen fonksiyonlar arasında sayılabilir. Kolombiya iç savaşında ABD silahlı kuvvetleri adına özel askerî şirketlerin danışmanlıktan istihbarata pek çok alanda etkin rol aldıkları, ülkede o dönemde görev yapan ABD

[246] Lemieux, a.g.e., 160-165.
[247] Chesterman ve Angelina, a.g.e., s186.
[248] Özel şirketlerin kalifiye personele devlet kurumlarına nazaran ortalama %35 daha fazla gelir sağladığı bilinmektedir.

askerlerinin ise görev alanının uyuşturucu ticareti ile mücadele ile kısıtlı tutulduğu bilinmektedir.[249]

İstihbarat teşkilatlarının icra ettiği gizli istihbarat faaliyetleri ile özel sektörün icra ettikleri soruşturmalar arasındaki sınırlar da bulanıklaşmaya başlamıştır. Hamas üyesi olan Mahmoud al-Madhoudûn 2010 yılında Dubai'de öldürülmesinin arkasında MOSSAD'ın olduğun bir gazetecinin ısrarlı soruşturmasıyla tespit edildiği Dubai Polis Şefi Dhali Khalfan Tamim tarafından bir basın toplantısında açıklanmıştır. [250]

Hershkovitz; Ar-Ge, siber de dâhil olmak üzere istihbarat operasyonları, bilgi toplama ve işleme vb. birçok fonksiyon günümüzde özel şirketlerce yapılmakta olduğunu ve bunda asıl gayenin etkinlik ve maliyet azaltmak olduğunu belirtmektedir.[251]

Hasımlara karşı teknolojik üstünlüğün sürdürülmesi ABD istihbarat topluluğunun kendine koyduğu hedeflerden bir tanesi olarak ODNI'nin yıllık Ulusal İstihbarat Stratejisi Raporlarında gösterilmiştir. Maliyet etkin olması baş etken olmak üzere istihbarat teşkilatları yüksek teknolojiye sahip yetenekleri kendi bünyelerinde kurmaktansa, bu yeteneklere sahip özel şirketlerden bu hizmetleri satın alma yoluna gitmektedirler. Özellikle açık kaynak vasıtasıyla veriye erişmede üstünlüğü ele geçiren özel sektör, bu veriyi yüksek teknolojileri kullanarak istihbarata dönüştürerek kamu kurumlarına servis etmektedir.

İlişkilendirilmesi durumunda uluslararası krize neden olabilecek, hasma yönelik gizli birtakım faaliyetlerin (siber casusluk, siber saldırı vb.) özel şirketlere yaptırıldığı da bilinmektedir. Bu tip görevlerin özel şirketlere yönlendirilmesi inkâr edilebilirliğin yanında, yapılan faaliyetin hedef ülke tarafından tespit edilmesini de zorlaştırmakta ve saldıranın tarafı tespit edilemeyeceğinden karşı saldırı ihtimali de düşmektedir. [252]

Bunların yanında Puyvelde özel sektörün varlığına farklı bir perspektiften bakarak, özel sektör tarafından sağlanan desteğin tamamının resmî kurumlarca karşılanabilmesinin ekonomiye getireceği yükün yanında, demokratik değerleri kısıtlayan bir Polis Devlete dönüştüreceği yorumu yapmaktadır. Özel istihbarat şirketleri kamu istihbaratına çeşitli yetenekler sunarken, bu kurumların mutlak kontrol

[249] Singer, a.g.e., 10-12.
[250] Frank James, 'Dubai Police Chief '99%' Sure Israil's Mossad Killed Hamas Militant', National Public Radio, 18 Şubat 2010, https://www.npr.org/sections/thetwo-way/2010/02/dubai_police_chief_99_sure_mos.html , (erişim tarihi 20 Ağustos 2022).
[251] Hershkovitz, a.g.e., 75.
[252] Hershkovitz, a.g.e., 77.

ve otoritesinin de paylaşılması ile bir nevi demokratik kontrol mekanizması oluşturduğu görüşünü savunmaktadır. [253]

4.6. İstihbaratın Özelleşmesinin Beraberinde Getirdiği Riskler

Pek çok avantajının yanında özel şirketlerden istihbarat desteği alınmasının da çeşitli sakıncaları bulunmaktadır. Eleştiri konuları, çalışmanın asıl konusu olmaması nedeniyle kısaca sıralanacak olursa;

- Hesap sorulamama (*Lack of Accountability*)[254],
- Şirketlerin aldıkları kontrattaki yükümlülükleri yerine getirirken sivil hak ve özgürlükleri göz ardı edebilmeleri (*Threat to Civil Liberties*)[255],
- Resmî olarak görev yapılamayan ülkelerde istihbarat faaliyetlerinin sivil şirketler üzerinden yürütülmesi (*Loss of Stateness*)[256],
- Özel istihbarat şirketlerinin görevlerini yaparken kanunlara uyup uymadıklarının kontrol mekanizmalarınca tespitinin zor olması,
- Devlet adına görev yapan sivil istihbarat ve askerî şirket personelinin görev yaptıkları bölgelerde toplum güvenliğini önemsemeyen uygulamaları (*Threat to Public Safety*)[257],
- Devlet saygınlığını tehdit etmesi (*Reputational Concerns*)[258],

[253] Damien Van Puyvelde, *The US intelligence community and the private sector: How rational are privatization rationales?* (El Paso: National Security Studies Institute The University of Texas, 2014), 13. http://web.isanet.org/Web/Conferences/ISSS%20Austin%202014/Archive/6698f449-30ac-4dda-9486-fa5951f48754.pdf [Erişim Tarihi: 19.08.2023].

[254] Irak'ta Ebu-Grahib, Küba'da Guantanamo çok tartışılan sonuçları ile gündeme gelen geliştirilmiş sorgulama tekniklerini uygulayan şirket çalışanları hakkında işlem yapılamamıştır.

[255] Özellikle telekomünikasyon alanında faaliyet gösteren şirketlerin özel bilgiler ve görüşmeler ile ilgili detayları hukuksuz olarak işledikleri ve paylaştıkları iddia edilmektedir.

[256] ABD'nin Pakistan'da istihbari faaliyet göstermesi ile ilgili kısıtların sivil şirketler üzerinden aşılması vb.

[257] Özel Askerî Şirketlerce gerçekleştirilen ve sivil ölümleri ile gündeme gelen olaylar gibi.

[258] Booz Allen Hamilton çalışanı Edward Snowden'ın kritik bilgileri sızdırması neticesinde ABD'nin güç durumda kalması bu konuya örnek verilebilir.

- Özel sektörün ücret politikası, çalışma şartları ve yüksek teknolojisi devlet kurumlarında yetişmiş nitelikli personeli cezbetmesi ve personelin kurumda tutulamaması (*Threat to Public Analyst Jobs*)[259] olarak listelenebilir.[260]

- Özel şirketler, görev yaparken kişisel hak ve özgürlüklere devlet kurumları kadar dikkat etmeyebildiği de devlet yetkililerince dahi kabul edilmiş bir handikaptır. ABD eski Başkanı Obama; %100 özel hayatın gizliliği sağlanırken, %100 güvende olamayız' diyerek bu konuda ulusal güvenliğin sağlanması için bir miktar feragatın zorunlu olduğunu vurgulamıştır. [261]

Ayrıca; 2016 yılı itibariyle özel istihbarat sektöründe çalışan 45,000 personelin %80'i beş büyük firmada istihdam edilmektedir.[262] Bu durum bahse konu şirketlerin ekonomik ve dolaylı olarak politik gücünü artırmaktadır.

Tüm bu mahsurlar incelendiğinde; istihbaratta özelleşme konusunda başı çeken ABD'de istihbaratın sivil şirketlerden teminine ya da sivil entitelerin istihbarat temini için görevlendirilmesine yönelik genel bir hukuki altyapı eksikliği önemli bir açık olarak karşımıza çıkmaktadır. Devletler ve istihbarat kurumları bu konuyu hizmet alımı gibi yöntemlerle aşsalar da icra edilen görevlerin çerçevesini çizme, yetki ve sorumlulukların belirlenmesine yönelik ciddi bir hukuki altyapı eksikliği bulunduğu da göz ardı edilmemelidir. Özellikle son dönemde özel istihbarat şirketlerinin sorumlusu olduğu sansasyonel fiyaskoların[263] arkasında yatan temel sorun olarak, bu alandaki yetki ve sorumluklar ile olası sorunlarda uygulanacak yaptırımların kodifiye edilmemiş, hukuki bir tabana oturtulmamış olması gösterilmektedir.

Bunların yanında, ülkelerin örtülü faaliyetler ile iç içe geçmiş istihbarat uygulamaları için de özel şirketler, özel askerî şirketler veya suç örgütleri ile de çalıştıklarına

---

[259] Özel şirketlerin sağlayabildiği maddi imkânlar, devlet kurumlarındaki yetişkin personelin elde tutulmasını güçleştirmekte, nitelikli personelin kaybı ise nitelikli analiz için bu tip personeli istihdam eden şirketlere bağımlılığı artırmaktadır.

[260] Lemieux, a.g.e., 202-204.

[261] Jacob Sugarman, "You Can't Have 100 Percent Security and Also Have 100 Percent Privacy', Key Quotes from the President's Defense of His Government's Secret Surveillence Program", *Salon,* 7 Haziran 2013, https://www.salon.com/2013/06/07/you_cant_have_100_percent_security_and_also_have_100_percent_privacy/ [Erişim Tarihi: 03.08.2022].

[262] Tim Shorrock, "5 Corporations Now Dominate Our Privatized Intelligence". *The Nation*, 8 Eylül 2016. https://www.thenation.com/article/archive/five-corporations-now-dominate-our-privatized-intelligence-industry/ [Erişim Tarihi: 05.Mayıs 2022].

[263] NSA eski analisti Edward Snowden'in Wiki-leaks gizlilik dereceli verilerin sızdırılması olayı, Guantanamo ve Ebu Garib hapishanelerinde özel istihbarat şirketlerince uygulan "gelişmiş sorgulama metodları" uygulamaları vb.

rastlanmaktadır. Rusya'nın eski istihbarat teşkilatı mensupları vasıtasıyla Avrupa'da örtülü faaliyetlerde (suikastlar, tedhiş, sabotaj vb.) kullandığı yönünde değerlendirmeler daha sık karşımıza çıksa da bu gibi uygulamaların sadece Rusya ile sınırlı kalmadığını söylemek yanlış olmayacaktır. Bu durum, devletlerin kirli faaliyetleri için de özel (askerî) şirketler ya da suç ağları, hacker grupları vb. oluşumlardan faydalanabileceğinin bir örneğini teşkil etmektedir.[264] Günümüzün karmaşık mücadele ortamında komuta kontrol, otorite ve sorumluluk kavramlarının bulanıklaşmasına neden olan bu çok aktörlü ve inkâr edilebilir karakterdeki uygulamalar, istihbarat gibi hassas ve mahremiyeti olan bir konuda dışarıdan teminin tartışılan sakıncalı yönlerinden biri olarak karşımıza çıkmaktadır. Avantajlarının yanında pek çok dezavantajı da bünyesinde barındıran özel istihbarat sektörü ile iş birliği, daralan bütçeler, gelişen teknolojiler ve artan analiz yükü döneminde üst düzey yöneticilerin bürokratik zorluklardan kaçınmak için sığındıkları bir liman olarak görülmemesi gerekmektedir.[265]

Özellikle ABD modeli üzerinden yaptığımız incelendiğinde, dışarıdan teminin istihbarat fonksiyonu içinde olması gerekenin çok ötesinde istihbarat temin ve analiz sürecine dahil olduğu yönünde hâkim bir görüş tespit edilmiştir. İstihbarat topluluğuna özel sektörce sağlanan bu katkının bir kısmının kapsam ve derinlik olarak kamu istihbarat kurumlarına devredilmesi, özel sektörün mümkün oldukça gizli faaliyetlerden açık kaynak istihbaratına yöneltilmesinin özellikle şeffaflık ve hesap verebilirlik bazında özelleşmenin mahsurlarını asgariye indirmeye yardımcı olacağı değerlendirilmektedir.[266]

ABD istihbarat topluluğunun günümüz ihtiyaçlarının karşılanmasında özel istihbarat sektörünün desteğine güvenmesinin ciddi bir bağımlılık yarattığı, özel sektör olmadan işleyemeyeceği yönündeki görüş genel kabul görmektedir. Roper, 'İstihbaratın özelleşmesine karşı çıkan ve tüm fonksiyonların devlet kurumlar tekelinde olması gerektiğini savunanlar, hantal devlet bürokrasisinin gerekli çeviklik, yenilikçilik, esneklik ve mesleki becerinin sadece istihbarat kurumlarınca sağlanamayacağını

[264] Galeotti, 2022, 62.
[265] Puyvelde, a.g.e., 13.
[266] Armin Krishnan, "The Future of U.S. Intelligence Outsourcing", *The Brown Journal of World Affairs*, C. 18, S. 1 (2011): 195.

görmezden gelmektedir' diyerek ABD istihbarat sisteminin özel sektöre istihbarat fonksiyonlarını işletmekte ne kadar bağımlı olduğunu vurgulamaktadır.[267]

4.7. Özel Sektör İstihbaratında İstihdam ve Diğer Ülkelerde Uygulamalar

Robson Morrow; özel istihbarat şirketlerinin istihdam konusunda tercihlerini, sadece bunlarla sınırlı kalmamakla birlikte, ağırlıklı olarak resmî istihbarat kurumu, silahlı kuvvetler veya kolluk kuvvetleri geçmişi olan personelden yana kullandıklarını tespit etmiştir. Bu tercihin arkasındaki neden olarak da özel sektörde uygulanan istihbarat çalışmalarına hali hazırda yatkınlık, mesleki anlayışın ve temel eğitimin oturmuş olması ve resmî istihbarat kurumları ile irtibatlarda kişisel bağlantıların önemi gösterilmektedir. Bununla birlikte Robson-Morrow, sektör içinde yaptığı mülakatlara dayanarak; resmî kurum geçmişinin tercih nedeni olmasının her geçen gün azaldığı ve işverenlerin çalışılan alanda eğitim almış, konuya farklı bakış açıları ile yaklaşabilecek farklı mesleki geçmişe sahip personelin istihdamı yönünde bir anlayış değişikliğine gittiğinin gözlemlendiğini öne sürmektedir. Bu bağlamda düşünce kuruluşları, üniversiteler veya çalışılan bölgeye ve konuya özgü sektörlerden personel istihdamının arttığı kanaatine varmıştır. Gizliliğe haiz konularda güvenlik kleransı ihtiyacı dikkate alındığında, eski devlet çalışanlarının bu bağlamda da avantajlı olmaları, sektörde kişisel bağlantıların önemi, mesleki yatkınlık ve prosedürlere hakimiyet nedeniyle eski devlet çalışanları bir nebze avantajlı olsalar da spesifik alanlarda konusunun uzmanı personelin sağladığı avantajlar, farklı bakış açısına sahip personelin sağlayacağı katkı, gelişen teknolojiye adaptasyon ve bu alanda ihtiyaç duyulan meleke ve eğitim diğer sektörlerden gelen personele yönelik talebin de artmasına neden olan etkenler olarak ön plana çıkmaktadır.[268]

İstihbaratın özelleşmesine öncülük eden ABD örneği üzerinden açıklamaya çalışılan, gelişen ve dönüşen güç mücadelesi ortamında karar vericilerin ihtiyaç duydukları istihbaratın resmî istihbarat kurumlarının gayretlerini desteklemek üzere dışarıdan temini, diğer ülkelerde muhalif görüşler olsa da uygulamaya geçmiş ve gelişmekte olan bir çözüm olarak genel olarak kabul görmüştür. Özellikle belirtilmelidir ki, istihbarat alanında çalışan özel şirketlerin büyük çoğunluğu hizmetlerini ulus-aşan bir

[267] James E. Roper, "Using Private Corporations to conduct Intelligence Activities for National Security Purposes: An Ethical Appraisal" *International Journal of Intelligence Ethics*. C. 1, S. 2 (2010), 72-73.
[268] Robson-Morrow, a.g.m., 5.

anlayışla pazara sunmakta, istihbarat ihtiyaçlarını dışarıdan temin etme gayreti içerisinde en sağlıklı, güvenilir ürüne ulaşma niyeti ile ulusal şirketlerin dışında kuruluşlarla çalışmayı tercih edebilmektedir. Bu durumum Anglosakson ülkeler arasında azami olmakla birlikte, batılı anlayışa sahip ülkelerde daha yaygın, daha muhafazakâr bir anlayışa sahip doğu bloğu veya oryantalist ülkelerinde daha ulusalcı bir yaklaşımın hâkim olduğu görülmektedir. Suudi Arabistan, Togo, Venezüella ve hatta İspanya'nın İsrail menşeili teknik istihbarat şirketi *NSO Group* (https://www.nsogroup.com/) ve İtalyan *Hacking Team* (https://www.hackingteam.it/) siber istihbarat şirketlerinden terör ağlarının dinlenmesi ve mesajlaşmalarının sekteye uğratılması maksadıyla destek aldığı bilinmektedir. Hatta Rusya'nın kendi istihbarat teşkilatı FSB'ye güvenmeyerek Sovyetler Birliğinin dağılması sürecinde kaybolan mali karşılığı olan kaynakları bulmak üzere ABD merkezli veri analizi ve risk yönetimi odaklı çalışan *Kroll Associates* (https://www.kroll.com/en) şirketinde destek alması özel istihbarat şirketlerinden hizmet alımında en büyük soru işaretlerinden bir olan "güven" konusuna ilginç bir örnek teşkil etmektedir.[269]

Farklı bir bakış açısı ile; istihbarat ihtiyaçlarını karşılamaya genel olarak batılı toplumlar daha açık ve yapıcı yaklaşımlar izlemekle beraber, bu konuyu ayrıntılı bir şekilde irdeleyen Fransa, özel sektörün istihdam ve teknolojiye adaptasyon konusunda sahip olduğu esneklik nedeniyle ihtiyaçların dışarıdan temininin resmî istihbarat teşkilatlarında uzman personel sıkıntısına, devlet kurumlarının teknolojinin gerisinde kalmasına neden olacağı çıkarımında bulunmaktadır. Devlet-özel sektör istihbaratı karşılaştırıldığında bunu özel sektörün esnekliğinden dolayı haksız bir rekabet olarak görmekte ve uzun vadede ABD benzeri bir bağımlılığa dönüşeceği çıkarımı ile istihbarat alanında özelleşmenin olumsuz etkilerinin daha fazla olacağı sonucuna varmaktadırlar. İstihbarat konusunda diğer batılı toplumlara nazaran daha muhafazakâr bir tutumla genel olarak istihbarat ihtiyaçlarının zorunlu ve elde bulunmayan kabiliyetler dışında, ihtiyaç duyulan yeteneklerin ulusal olarak edinilerek devletçe edinilerek resmî olarak karşılanmasının daha mantıklı bir yaklaşım olduğu yönünde bir istihbarat politikası benimsemektedir.[270]

---

[269] Galeotti, 2022. 62.

[270] Damien Van Puyvelde, "Quelles leçons tirer de la privatisation du Renseignement aux États-Unis / ABD'de İstihbaratın Özelleştirilmesinden Çıkarılması Gereken Dersler", *IRIS Editions, Revue Internationale et Stratégique*, S. 87 (2012), 50–52. https://www.researchgate.net/publication/272806351_Quelles_lecons_tirer_de_la_privatisation_du_renseignement_aux_Etats-Unis [Erişim Tarihi: 12.08.2022].

5. SONUÇ

Günümüz savaşı; çatışmanın belli bir bölgeden küresel bir niteliğe kavuşmasına, güç kullanmada ağırlığın devlet tekelinden devlet dışı aktörlerin üzerine kaymasına, askerî uygulamalardan sivilleşmeye, uluslararası hukukun boşluklarını suiistimal ile hukuk dışılığa, farklı harekât ortamlarında eşgüdüm içerisinde ve tüm aktörlerin birlikte kullanımına, risk analizli senkronize icrası ile karmaşık, melez, hibrit bir güç mücadelesine dönüşmüştür. Hibrit savaş terimi ile kavramsallaştırılmaya çalışılan çatışma tipinde aktörler, kullanılan araçlar ve tarafların politikaları doğrultusunda uyguladıkları stratejiler, son derece durumsal odaklı hale gelmiş ve netlikten oldukça uzaklaşmıştır.

Bileşenlerine bakıldığında politik-stratejik seviyede bir mücadele olduğu aşikâr olan hibrit savaşta yöntem ve kullanılan araçlar yerine hasmın amaçlarına odaklanmak, düşmanın niyetini, hedeflerini tespit ederek, kullandığı araçlar ile ilişkisini ortaya koyabilmek ana stratejiyi oluşturmaktadır.[271] Bu alandaki savaşın sisini[272] stratejik istihbarat kaldırmaya çalışırken, çatışma alanında yürütülen mücadeleyi anlamaya yönelik olarak da operatif ve taktik seviyede, eşgüdüm içerisinde istihbarat faaliyetleri yürütülmektedir.

Sebepleri politik ve stratejik olan hibrit savaşta mücadele, sosyal ve beşerî şartların analizi sonucunda oluşturulacak politikalar ile şekillenir. Ancak sıklıkla çözüm arayışlarının güç kullanımını zorunlu kıldığı durumlarla karşılaşılmaktadır. Bu durum, düzensiz unsurlarla bileşik harekât kabiliyetine sahip düzenli birliklerce uygulanabilecek yeni nesil bir teşkilatlanma, zihniyet ve müşterek harekât doktrini gerekli kılmaktadır.

Tarihsel süreç içerisinde değişen ve gelişen savaş, tarafların mücadeleyi icra ediliş şekillerini belirleyen doktrinleri de tehdit türü ile uyguladığı taktik ve teknikler doğrultusunda birçok değişime tabi tutmuştur. Gelecekte çok aktörlü ve çok tabanlı

[271] Johnson, a.g.e., 1.
[272] Clausewitz, a.g.e. 101.

yeni muharebe ortamı ile karşılaşılacak olması, konvansiyonel muharebeler için tasarlanmış ordular, komuta kontrol ve karar destek sistemleri (istihbarat da dahil olmak üzere karar verme sürecini destekleyen tüm sistemeler) başta olmak üzere tüm fonksiyon alanlarının her seviyede (taktik, operatif ve stratejik) yeni doğan harekât ihtiyaçlarını karşılamada yeterli kalamayacağını düşündürmektedir.[273]

Halihazırda son derece dinamik harekât alanında; organizasyonel ataletini yenmiş, yüksek uyum kabiliyetine sahip, değişen harekât ortamı içinde değişen askerî (ve sivil) ihtiyaçlara yenilikçi çözümler üretebilen silahlı kuvvetler ve harekâta destek sağlayan kurum/kuruluşlarının başarı sağlayabileceği öngörülmektedir.[274] Tarihî süreci içinde teknolojik gelişimin öncülüğünde siyasal konjonktür çerçevesinde uygulanan savaş ile döneme uygun strateji ve doktrinde de değişikler görülmektedir. Birçok kaynakta 1991 tarihli Körfez Savaşı son konvansiyonel savaş olarak gösterilmektedir. Bu savaşta hayata geçirilen 'Etki Odaklı Harekât' ve birbirleri ile ağ üzerinden haberleşen kuvvetlerin müşterek harekât doktrinini tanımlayan 'Ağ Merkezli Harekât' öne çıkmıştır. Savaşın değişimi çerçevesinde devlet dışı tehditlerin çatışma ortamına damga vurması ile 'Düzensiz Savaş', diğer devlet kurumlarının da desteğini içeren 'Tüm Devlet Yaklaşımı' ve çok katmanlı hale gelen günümüz harekât alanının tüm boyutlarında mücadeleyi esas alan 'Çok Tabanlı Harekât' yaklaşımları, icranın metodolojisini tanımlayan doktrinel bir süreç içinde gelişmiştir. Günümüz ve yakın geleceğin harekât ihtiyaçlarını karşılamak üzere 'Çok Tabanlı Harekât Doktrini' geliştirme çabalarının ise artarak devam ettiği gözlenmektedir.

Bu doğrultuda günümüz güç mücadelesinin yürütüldüğü ortamların, harekât tabanlarının (*Operational Domains*) tanımlanmasının ve sınıflandırılmasının ihtiyacı zaruri olarak ortaya çıkmıştır. İstihbaratı destekleyen gözetleme sistemleri atmosferin dışına taşmış ve uzay; güç ve nüfuz mücadelesi içinde olan büyük devletler için harekâtlarını destekleyecekleri yetenekleri konuşlandırabilecekleri bir diğer harekât ortamı olarak belirmiştir. 2019 yılı Haziran ayında icra edilen NATO Savunma Bakanları toplantısında NATO Uzay Siyasası bir harekât tabanı olarak kabul edilmiştir.[275] İnsanın artan önemi ve etkisi neticesinde bilgi ve teknolojilerinin karar destek sistemleri ile iletişim üzerindeki ağırlığı doğrultusunda siber, iletişim ve

[273] Uşaklı ve Alper, a.g.e., 43.
[274] a.g.e., 39.
[275] NATO, NATO's Approach to Space, 3.

istihbarat toplama yeteneklerinde, elektromanyetik harekâta katkı sağlayan alanlar olarak doktrine dahil edilmiştir.

Bu doktrinel değişim sürecinin teknolojik gelişmeler ışığında gelişmeye devam edeceği açıkça görülmektedir. Yenilikçi bakış açısı ile sürekli bir değişim içinde olan günümüz mücadele ortamının gereksinimlerini karşılayabilecek bir dinamizm içinde olunması hedefi, hayati ilke olarak belirmektedir.[276] Bu bağlamda karar vericilerin durumsal farkındalığını sağlama, sürprizleri önleme, hasmın savaşma azim ve iradesini kıracak hareket tarzlarının üretilmesinde önemli bir role sahip olan istihbarat alanının da incelediğimiz günümüz harekât alanının ihtiyaçlarını karşılayacak şekilde dönüşüm içinde olması beklenmelidir.

Günümüzde karar vericiler; çatışma ortamının, yer altı da dahil olmak üzere çok tabanlı bir hal alması, mobilitenin yanında bilgi teknolojileri ve karar destek sistemlerinin etkinliğinin artması ile dinamikleşen muharebenin daha hızlı karar vermeyi zorunlu kılması ve belki de en önemli faktör olan muharebe sahasındaki insan faktörünün tarihte hiç olmadığı kadar önemli hale gelmesi neticesinde soğuk savaş dönemi tek devlet odaklı tehdit anlayışı ile sınırlı tehdide yöneltilmiş klasik istihbarat anlayışının ötesinde, tüm bu faktörleri karşılayacak bir istihbarata ihtiyaç duymaktadırlar. Bu ihtiyacın karşılanması için yeni bir anlayışın yanında, daha gelişmiş sensörler, bilgi sistemleri, çok tabanlı gözetleme sistemleri, sosyal ağ analizleri başta olmak üzere beşerî değerlendirmeler için büyük veri analizlerine ihtiyaç duyulmaktadır. İşte bu bağlamda, çevik yapıları, yüksek teknolojik donanım ile yetişmiş personel istihdam edebilen, değişime kolay uyum sağlayabilen ve teknolojiye yaptıkları yatırımlar ile ihtiyaçlara cevap vermede kamu istihbarat teşkilatlarından hızlı hareket edebilen özel istihbarat şirketleri değişen istihbarat isteklerini karşılamada bir çözüm seçeneği olarak öne çıkmaktadır.

Çalışma, başlangıcı 1940'lar olarak kabul edilen istihbaratta özelleşme konusunun, fayda ve mahsurları ile ve karşılaştırmalı olarak değerlendirilmesi gerektiğini bir kez daha ortaya çıkarmıştır. Özellikle soğuk savaş sonrası istihbarat topluluğundaki küçülmenin ardından karşılaşılan yeni nesil tehditler istihbarat teşkilatlarını, veri toplama ve analiz yetenekleri yetersiz bırakmıştır. İnceleme, yeterli insan gücünden yoksun kalan istihbarat teşkilatlarının, çözümü özel sektör desteği almakta

[276] Uşaklı ve Alper, a.g.e., 49.

bulduklarını göstermiştir. Bu bağlamda ihtiyaç duyulan personelin istihdamı ya da yeni yeteneklerin organik olarak edinilmesinin yerine çok daha uygun/ucuz olacak şekilde dışarıdan temininin ve sorumluluğun paylaşılmasının çok daha cazip geldiği fikri ile hareket edildiği görülmüştür. Bu noktada nitelikli personel yetiştirmenin yüksek maliyeti ve sürecinin uzunluğu gibi faktörlerin de ihtiyacın özel sektörden teminine gidilen süreci etkilediğini ortaya koymuştur. İstihbaratın dışardan temini sürecinin, istihbarat alanında bir özel sektör oluşmasına neden olduğu, çalışmanın tespitleri arasında yer almıştır.

ABD istihbarat topluluğunun kurumsallaşması olarak kabul edilebilecek Merkezi İstihbarat Ajansı'nın (CIA) 1947'de kurulmasının genel olarak özel sektöre istihbarat fonksiyonunu destekleyen büyük projeler verilmesi ile aynı döneme denk geldiği görülmektedir. Bu tespitten yola çıkarak, ABD istihbarat topluluğunun özel sektör ile iş birliği içinde kurulduğu ve tarihsel süreç içerisinde ABD istihbaratının özel sektöre bağlı/bağımlı olarak istihbarat ürettiği söylenebilir.

İlk örneklerinin Soğuk Savaş döneminde görülmeye başlandığı ve 11 Eylül 2001 saldırısı sonrasında istihbarat alanında devrim niteliğinde alınan tedbirler ile ciddi bir artış göstermeye başlamış olan istihbaratta özelleşmenin, bir istihbarat endüstrisi yarattığı ve adeta bir "gölge istihbarat topluluğu" oluşturduğu çalışmanın başlıca tespitleri arasındadır.

Kurumsallaştığı ilk dönemden itibaren özel sektör ile içi içe olan ABD istihbarat topluluğunun özel sektör olmadan işlemesinin mümkün olmayacağı genel bir kanı olarak kabul görmektedir. İstihbarat gibi doğası gereği muhafazakâr olan bir fonksiyonun devlet tekelinde olması gerektiğini savunanlar olsa da devlet bürokrasisinin, özellikle günümüzün hızla gelişen sosyo-kültürel ağlar ve teknolojisi karşısında gerekli yenilik, esneklik ve kritik yetenekleri karşılayamayacağını görmezden gelmektedirler. Özel sektörün alandaki yetenekleri ve uzmanlığı onu ABD istihbarat topluluğu için elzem olarak değerlendirilmesinin en büyük nedeni olarak gösterilirken, paylaşılan yükün büyüklüğüne de dikkat çekilmektedir. Bu yükün sadece kamu tarafından üstlenilmesinin sistemi hantallaştırırken, demokratik yapıyı da olumsuz etkileyeceği yorumunda bulunulabilir.

İstihbarat fonksiyon alanının toplama, analiz ve örtülü faaliyetler alt fonksiyonlarında ABD İstihbarat topluluğuna destek sağlayan özel istihbarat şirketleri, özellikle

günümüzün değişen istihbarat ihtiyaçlarını karşılamada kamu istihbarat kurumlarına önemi destek sağlamaktadır. Kamu yeteneklerinin ötesine geçen bu destek; gelişen toplama ve analiz teknolojileri ile büyük veri analizi, bilgi güvenliği ve İKK, güvenli ve yüksek kapasiteli veri depolama ve paylaşımı ile devlet kurumları için riskli veya politik olarak kısıtlı bölgelerde örtülü faaliyetler icra etme fonksiyonlarını kapsamaktadır.

Sağladıkları avantajların yanında, yetki ve sorumlulukları çoğunlukla göz ardı edilen bu şirketlerin, sorumsuz uygulamaları pek çok kez sansasyonel olayların vuku bulmasına, hizmet alımı yapılmış olsa da bu şirketlerin hatalarının ülkenin itibarını zedelediği ve kimi zaman uluslararası kamuoyunda zor durumda bıraktığına şahit olunmuştur. Gerek sakıncalı durumların tekerrürünün önüne geçilmesi gerekse özel sektör istihbaratının nimetlerinden azami fayda sağlanabilmesi için; kamu istihbaratını desteklemek üzere sözleşme yapılan şirketlerin etik ilkeler, hukuki çerçeve ve mesleki teamüllere göre belirlenmiş yetki ve yükümlülüklerini tanımlayan çalışma esaslarının kanunla düzenlenmesi gerekliliği aşikârdır.

KAYNAKÇA

Avant, Deborah Denise. *The Market for Force The Consequences of Privatizing Security*, New York: Cambridge University Press, 2005.

Bartkowski, Maciej. "Nonviolent Civilian Defense to Counter Russian Hybrid Warfare", Johns Hopkins University Krieger School of Arts and Sciences, 2015. https://www.nonviolent-conflict.org/wp-content/uploads/2018/12/GOV1501_WhitePaper_Bartkowski.pdf [Erişim Tarihi: 30.05.2022].

Bartles, Charles K., "Getting Gerasimov Right", *Military Review*, (Ocak-Şubat 2016): 30–38. https://www.researchgate.net/publication/329933852_Getting_Gerasimov_Right [Erişim Tarihi: 30.05.2022].

Batscheley, Allen. *Effects-Based Operations: A New Operational Model?*, US Army War Collage: US Army Publication, 2002. https://web.archive.org/web/20070927213243/http://www.iwar.org.uk/military/resources/effect-based-ops/ebo.pdf [Erişim Tarihi: 16.01.2023].

Beduschi, Ana. "International Migration Management in the Age of Artificial Intelligence" *Migration Studies*, C. 9, S. 3 (2020), 576–596.

Bērziņš, Jānis. "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy," (2014): 1–14. https://sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf [Erişim Tarihi: 16.08.2023].

Bıçakcı, Salih. "Hibrit Savaş", *Uluslararası İlişkiler Konseyi Güvenlik Yazıları Serisi*, C. 33, S. 8 (2019). https://doi.org/10.13140/RG.2.2.32236.10883 [Erişim Tarihi: 16.01.2023].

Biltgen, Patrick, Stephen Ryan. *Activity-Based Intelligence: Principles and Applications*, London: Artech House, 2016.

Bridges, Richard M., *Information Operations: FM 100-6*, Fort Levenworth: US Army Publication, 1996.

Bruder, Marissa, Caroline Hilty, Michelle Kaplun. "The Crypto Current: An Analysis of Monero Report", *The Counterterrorism Group - Illicit Finance Team*, 2021.

Buennemeyer, Timothy. "A Strategical Approach to Network Defense: Framing the Cloud", *Paremeters*, C. 41, S.3, 2011.

Büyükakıncı, Erhan. "Yeni Savaşlardan Savaşın Dönüşümüne: Uluslararası Sistem ve Aktörlerde Değişimin Sürekliliği", *Savaşın Dönüşümü; Yeni Dinamikler, Aktörler ve Araçlar*, der. Erhan Büyükakıncı. Ankara: Adres Yayınları, 2021.

Casey, George W. "America's Army In an Era Of Persistent Conflict.", Army Journal , C. 58, S. 1 (2008): 19–28.

https://www.ausa.org/sites/default/files/Casey_1008.pdf [Erişim Tarihi: 16.01.2023]

Caşın, Mesut Hakkı. "Modern Harbin Doğasında Değişim Modeli Olarak Hibrit Savaş", *Savaşın Dönüşümü: Yeni Dinamikler, Aktörler ve Araçlar*. der. Erhan Büyükakıncı, Ankara: Adres Yayınları, 2021, 204-243.

CBInsight, "What is Quantum Computing?", *CBInsight Research Report*, 7 Ocak 2021, https://www.cbinsights.com/research/report/quantum-computing/ [Erişim Tarihi: 19.08.2023].

Chekov, Alexander D., Anna V. Makarycheva, Anastasia M. Solomentseva, Maxim A. Suchkov ve Andrey A. Sushentsov. "War of the Future: A View from Russia." *Survival*, C. 61, S. 6 (2019): 25–48. https://doi.org/10.1080/00396338.2019.1688563 [Erişim Tarihi: 16.01.2023]

Chersterman, Simon. *The Privatization of Intelligence*: EJIL: Talk Blog of the European Journal of International Law, 2009. https://www.ejiltalk.org/privatization_of_intel/ [Erişim Tarihi: 20.08.2022].

Chesterman, Simon, Angelina Fisher, "Introduction", *Private Security, Public Order The Outsourcing of Public Services and Its Limits*, der. Simon Chesterman, London: Oxford University Press, 2009.

Clark, John Ransom. *Intelligence and National Security: A Reference Handbook*, London: Praeger Security International, (2007).

Clausewitz, Carl von. *On War*. Londra: Oxford University Press, 2007.

Cluzel, François du. "Cognitive Warfare", *Innovation Hub*, 2020. https://www.innovationhub-act.org/content/cognitive-warfare#:~:text=Cognitive [Erişim Tarihi: 16.01.2023].

Crump, Justin. *Corporate Security Intelligence and Strategic Decision Making*, Boca Raton: CRC Press Taylor & Francis Group, 2015.

Coats, Dan. "Confronting 21st Century Challenges", *ISP Intelligence Studies*, Etter-Harbin Alumni Centre, 2018 https://video.ibm.com/recorded/114060119 , [Erişim Tarihi: 10.08.2023].

Comelly, Owen, *Blundering to Glory: Napoleon's Military Campagins*, (Lanham MD: Rowman & Littlefield, 2006).

Cormac, Rory, Richard J Aldrich. "Grey Is the New Black: Covert Action and Implausible Deniability", *International Affairs* C. 3 (2018): 477–494. https://doi.org/10.1093/ia/iiy067 [Erişim Tarihi: 16.01.2023].

Corrigan, Jack. "Cyber Threats Are Emerging Faster Than DHS Can Identify and Comfront Them", *Defense One*, 2023. https://www.defenseone.com/threats/2019/03/cyber-threats-are-emerging-faster-dhs-can-address-them-secretary-says/155719/ [Erişim Tarihi: 10.08.2023].

Creveld, Martin Van, *Transformation of War*. New York: The Free Press, 1991.

Cropsey, Seth. "Wither Hybrid War", *Real Clear Defence*, 2022.

Cullen, Patrick J., Erik Reichborn-Kjennerud, *Understanding Hybrid Warfare*. Oslo: Norwegian Institute of International Affairs, 2017. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf [Erişim Tarihi: 16.01.2023].

Çalışkan, Murat. "Hybrid Warfare through the Lens of Strategic Theory", *Defense and Security Analysis*, C. 35, S. 1 (2019): 40–58, https://doi.org/10.1080/14751798.2019.1565364 [Erişim Tarihi: 16.01.2023].

Çıtak, Emre. *Güvenlik ve İstihbarat: Yeni Güvenlik Politikaları ve Türkiye'de İstihbaratın Dönüşümü*. İstanbul: Yeniyüzyıl Yayınları, 2017.

CSIS Technology and Intelligence Task Force, *Maintaining the Intelligence Edge: Reimagining and Reinventing Intelligence through Innovation*. Washington DC: Center for Strategic and International Studies Press, 2021. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210113_Intelligence_Edge.pdf [Erişim Tarihi: 20.08.2023].

Darczewska, Jolanta. "The Anatomy of Russian Information Warfare", *Point of View*, der. Anna Łabuszewska, C. May 2014. Warsaw: Centre for Eastern Studies, 2014. http://www.osw.waw.pl/en/publikacje/point-view/2014-05-22/anatomy-russian-information-warfare-crimean-operation-a-case-study [Erişim Tarihi: 16.01.2023].

Davies, Phillip H. J., Toby Steward. "No War for Old Spies: Putin, the Kremlin and Intelligence", *RUSI*, 2021. https://rusi.org/explore-our-research/publications/commentary/no-war-old-spies-putin-kremlin-and-intelligence [Erişim Tarihi: 19.05.2022].

Development Concepts and Doctrine Centre, "UK Multi-Domain Integration - Joint Concept Note 1/20", (London: UK Ministry of Defence, 2020). https://www.gov.uk/government/publications/multi-domain-integration-jcn-120 [Erişim Tarihi: 16.01.2023].

DiCicco, Jonathan M. ve Tudor A. Onea, *Great Power Competition*, Londra: International Studies and Oxford University Press, 2023. https://oxfordre.com/internationalstudies/display/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-756 [Erişim Tarihi 23.08.2023].

Dignan, Larry. "IoT Devices to Generate79.4 ZB of sata in 2025, says IDC:Video Surveillance Will Generate a Lot of Data and Enterprise, Industrial and Individual Data Will Also Surge", *ZDNet*, 18 Haziran 2019. https://www.zdnet.com/article/iot-devices-to-generate-79-4zb-of-data-in-2025-says-idc/ [Erişim Tarihi 23.08.2023].

Dimitriu, George, Isabelle Duyvesteyn, "Conclusions: It may be 10 September 2001 Today", *The Future of Intelligence:Challenges in the 21st Century,* ed. Isabelle Duyvesteyn, Ben de Jong, Joop van Reijn. New York: Routledge, 2014.

Echevarria II, Antulio J.. *Operating in the Gray Zone An Alternative Paradigm for U.S. Military Strategy*, Carlisle: Strategic Studies Institute and U.S. Army War College Press, 2016. https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1424&context=monographs [Erişim Tarihi: 16.01.2023].

Fabian, Sandor. "The Russian Hybrid Warfare Strategy–Neither Russian nor Strategy", *Defense and Security Analysis*, C. 35, S. 3 (2019): 308–325. https://doi.org/10.1080/14751798.2019.1640424 [Erişim Tarihi: 16.01.2023].

Feickert, Andrew. "Defense Primer : Army Multi-Domain Operations (MDO)", *Focus*, 2021. https://sgp.fas.org/crs/natsec/IF11409.pdf [Erişim Tarihi: 15.05.2022].

Fischer, Sophie-Charlotte. "NATO and Artifical Intelligence: The Role of Public-Private Sector Collaboration", *NATO Decision-Making in the Age of Big Data and Artificial Intelligence*, der. Sonia Lucarelli, Alessandro Marrone, Francesco Niccolo Moro. Brussels: NATO HQ, (2021), 74-83.

Fridman, Ofer. *Russian Hybrid Warfare: Resurgence and Politicization*. Londra: Oxford University Press, 2018.

Galeotti, Mark. "The 'Gerasimov Doctrine' and Russian Non-Linear War", *In Moskow's Shadows*, 2014. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/ [Erişim Tarihi: 16.12.2022].

_____. "Hybrid, Ambiguous, and Non-Linear? How New Is Russia's 'New Way of War'?", *Small Wars and Insurgencies* C. 27, S. 2 (2016): 296-297. https://doi.org/10.1080/09592318.2015.1129170 [Erişim Tarihi: 15.05.2022].

_____. "I'm Sorry for Creating the 'Gerasimov Doctrine.'" *Foreign Policy*, 2018. https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/ [Erişim Tarihi: 16.01.2023].

_____. *The Weaponisation of Everything: A Field Guide to The New Way of War*. Cornwall: Yale University Press, 2022.

Gerasimov, Valery. "The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations", *Military Review*, Washington DC, (2016). https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf [Erişim Tarihi: 15.05.2022].

Gerber, Burton L., Jennifer E. Sims. *Transforming U.S. Intelligence*, Washington DC: Georgetown University Press, 2005.

Gerstell, Glenn S.. "I Work For N.S.A. We Cannot Afford to Lose the Digital Revolution", *New York Times*, 10 Eylül 2019, https://www.nytimes.com/2019/09/10/opinion/nsa-privacy.html , [Erişim Tarihi: 23.08.2022].

Goel, Sanjay. "Cyberwarfare: Connecting the Dots in Cyber Intelligence", *Communications of the ACM*, C. 54, S. 8 (2011), 132–140.

Goltz, Colmar von der, *The Nation in Arms*. Londra: W.H.Allen & Co., 1887.

Guha, Manabrata, "Multi-Domain Warfare: Waging Unrestricted Warfare", 2019, https://www.researchgate.net/publication/331771727_Multi-Domain_Warfare_Waging_Unrestricted_Warfare [Erişim Tarihi: 15.05.2022].

Gutmann, Myron P. "The Origins of the Thirty Years' War". *The Journal of Interdisciplinary History*, C. 18. S. 4 (1988): 749–770. http://www.jstor.org/stable/204823 [Erişim Tarihi: 15.05.2022].

Güçyetmez, Ferdi "The Changing Concept of War and America's Defence Policy.". *Lectio Socialis*, C. 5, S. 2 (2021): 75–88. https://doi.org/10.47478/lectio.837638 [Erişim Tarihi: 15.05.2022].

Gürel, Şükrü. S.. "Berlin Sorunu (1944-1972)", *Ankara Üniversitesi SBF Dergisi*, C. 32, S. 1 (1977), 207–229.

Heidelberg Institute for International Conflict Research, *Conflict Barometer Reports*. Heiderberg, 2020.

Herman, Michael. "Ethics and Intelligence After September 2001", *Intelligence and National Security*, Cilt 19, Sayı 2, (2004), 342–358.

Hershkovitz, Shay. *The Future of National Intelligence: How Emerging Technologies Reshaped Intelligence Communitie.* Londra: Rowman & Littlefield, 2022.

Hoffman, Frank G. *Conflict in the 21st Century: Rise of Hybrid Wars*. *Arlington*: Virginia, 2007. https://doi.org/10.20542/0131-2227-2019-63-12-56-66 [Erişim Tarihi: 15.05.2022]

_____. "Hybrid Warfare and Challenges." *Joint Forces Quarterly*, S. 52 (2009): 274–283. https://doi.org/10.2307/j.ctv7cjw3j.32 [Erişim Tarihi: 15.05.2022].

_____. "Hybrid Threats': Neither Omnipotent nor Unbeatable." *Orbis*, C. 54, S. 3 (2010): 441–455. https://doi.org/10.1016/j.orbis.2010.04.009 [Erişim Tarihi: 15.05.2022].

_____. "On Not So New Warfare: Political Warfare Vs Hybrid Threats", *War on the Rocks*, (2014). https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/ [Erişim Tarihi: 15.05.2022].

Holmes, Kim, R. "What is National Security?", *2015 Index of U.S. Military Strength*, The Heritage Foundation, (2014), https://www.heritage.org/sites/default/files/2019-

10/2015_IndexOfUSMilitaryStrength_What%20Is%20National%20Security.pdf [Erişim Tarihi: 20.08.2023].

Houseman, John. *Front and Center (1942-1955)*. New York: Simon & Schuster, 1975.

Hribar, Gašper, Iztok Podbregar, Teodora Ivanuša. "OSINT: A "Grey Zone"?", *International Journal of Intelligence and CounterIntelligence*, C. 27, S. 3 (2014), 529–549.

Hulnick, Arthur S.. "Harold P. Ford, Estimative Intelligence: The Purposes and Problems of National Intelligence Estimating", *Journal of Conflict Studies*, C. 14, S. 1 (1994), https://journals.lib.unb.ca/index.php/JCS/article/view/15167 [Erişim Tarihi: 15.08.2023].

Hulnick, Arthur S.. "The future of the intelligence process: the end of the intelligence cycle?", *The Future of Intelligence:Challenges in the 21st Century*, ed. Isabelle Duyvesteyn, Ben de Jong, Joop van Reijn. New York: Routledge, 2014, 47-57.

International Court of Justice, "Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)", *Merits, Judgment. I.C.J. Reports 1986*, 1986. https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf [Erişim Tarihi: 15.05.2022].

Irving, Doug. "Big Data, Big Questions", *RAND Review*, Washington DC: RAND, 2017. https://www.rand.org/blog/rand-review/2017/10/big-data-big-questions.html [Erişim Tarihi: 20.08.2022].

Johnson, Robert. "Hibrit Tehdidin Tarihsel Evrimi", *Hibrit Savaş; Savaşın Değişen Modeli*, İstanbul: Milli Savunma Üniversitesi Basımevi, 2018.

Judson, Jen. "Multidomain Operations Concept Will Become Doctrine This Summer". *Defense News*, 2022. https://www.defensenews.com/land/2022/03/23/multidomain-operations-concept-will-become-doctrine-this-summer/ [Erişim Tarihi: 15.05.2022].

Kaldor, Mary. "Wanted: Global Politics", *The Nation*, C. November 2001, (2001).

_____. *New and Old Wars: Organized Violence in a Global Era*. Stanford: Stanford University Press, 2006.

Kapusta, Philip. "The Gray Zone*"*, *Special Warfare*. (2015). https://www.soc.mil/SWCS/SWmag/archive/SW2804/GrayZone.pdf [Erişim Tarihi: 15.05.2022].

Karabulut, Ali Nedim. "Eski Savaş, Yeni Strateji: Rusya'nın Yirmibirinci Yüzyıldaki Hibrit Savaş Doktrini ve Ukrayna Krizi'ndeki Uygulaması", *Uluslararası İlişkiler Dergisi*, C. 13, S. 49 (2016): 25–42.

Karaosmanoğlu, Ali L.. "Yirmibirinci Yüzyılda Savaşı Tartışmak: Clausewitz Yeniden" *Uluslararası İlişkiler Dergisi*, C. 8, S. 29 (2011): 5-25.

http://www.uidergisi.com/wp-content/uploads/2013/02/21st-yuzyilda-savasi-tartisma.pdf [Erişim Tarihi: 15.05.2022].

Kissinger, Henry. *World Order*. New York: Penguin Books, 2015.

Krishnan, Armin. "The Future of U.S. Intelligence Outsourcing", *The Brown Journal of World Affairs*, C. 18, S. 1 (2011), 195–211.

Lahneman, William J.. *Keeping U.S. Intelligence Effective: The Need for a Revolution in Intelligence Affairs'*, Plymouth: Scarecrow Press, 2011.

Lake, Eli. "U.S. Eyes Russian Spies Infiltrating Ukraine", Daily Beast. 2014. https://www.thedailybeast.com/us-eyes-russian-spies-infiltrating-ukraine [Erişim Tarihi: 15.05.2022].

Lanoszka, Alexander. "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe", *International Affairs*, C. 92, S. 1 (2016): 175–195. https://doi.org/10.1111/1468-2346.12509 [Erişim Tarihi: 15.05.2022].

Lant, Karla. "China, Russia and the US Are in Artificial Intelligence Arms Race", *Futurism*, 12 Eylül 2017, https://futurism.com/china-russia-and-the-us-are-in-an-artificial-intelligence-arms-race [Erişim Tarihi: 20.08.2022].

Laqueur, Walter. *The Future of Intelligence*, Society Publishing, 1985.

Lemieux, Frederic. "The Rise of the Private Intelligence Sector". *Intelligence and State Surveillance in Modern Societies*. Bingley: Emerald Publishing Limited, 2018, 191–206,

Lewis, Antony. *The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them*. New York: Mango Media, 2021.

Lind, William S.. *On War: The Collected Columns of 2003-2009*, London: Castalia House, 2009.

_____. "Understanding Fourth Generation War." *Military Review*, 2014, https://www.hsdl.org/?view&did=482203 [Erişim Tarihi: 15.05.2022].

Lowenthal, Mark M.. *Intelligence, from Secret to Policy*, Washington DC: CQ Press, (2008).

Luttwak, Edward N. "A Brief Note on 'Fourth-Generation Warfare". *Contemporary Security Policy*, C. 26. S. 2 (2005) 227–280 https://doi.org/10.1080/13523260500211009 [Erişim Tarihi: 15.05.2022].

Luttwak, Edward N.. *Strategy: The Logic of War and Peace*, Londra: The Belknap Press of Harva, 2001.

Mahadevan, Prem. "Intelligence Agencies: Adapting to New Threats", *CSS Analysis in Security Policy*, S. 82, (2010): 1–3.

Mann, James. *Rise of the Vulcans: The History of Bush's War Cabinet*. New York: Penguin Group, 2004.

Marx, Leo, Merritt Roe Smith, *Does Technology Drive History? The Dilemman of Technological Determinizm*, Cambridge: MIT Press, 1994.

Matisek, Franky, Ron Granieri. *Podcast-Everything a Weapon, Everyone a Combatant*, U.S. Army War College, (2022). https://warroom.armywarcollege.edu/podcasts/everything-everyone/ (Erişim Tarihi: 19.04.2022).

Mazarr, Michael J. "Mastering the Gray Zone", *Understanding a Changing Era of Conflict*, Carlisle, PA: U.S. Army War Collage US Army Publication, 2015. https://publications.armywarcollege.edu/pubs/2372.pdf [Erişim Tarihi: 19.04.2022].

McCulloh, Timothy B.. *The Inadequacy of Definition and the Utility of a Theory of Hybrid Conflict: Is the 'Hybrid Threat' New?* Fort Leavenworth/KA: 2012. https://www.hsdl.org/?view&did=758318 [Erişim Tarihi: 19.04.2022]

McCulloh, Timothy, Richard Johnson. *Hybrid Warfare-JSOU Report 13-4*. McDill AFB: Joint Special Operations University, 2013. https://jsou.libguides.com/ld.php?content_id=2876897 [Erişim Tarihi: 19.04.2022].

McFarland, David. *Understanding Hybrid Warfare: Navigating the Smoke and Mirrors of International Security*. Las Vegas: David McFarland, 2021.

Mercado, Stephen C.. "Sailing the Sea of OSINT in the Information Age a Venerable Source in a New Era Sailing the Sea of OSINT in the Information Age" *Studies in Intelligence; Journal of the American Intelligence Professional*, C. 48, S. 3 (2004): 1–14.

Ministere Des Armees, L'organisation de l'armée de l'Air et de l'Espace, (2022), https://www.defense.gouv.fr/air/organisation-AAE [Erişim Tarihi: 15.05.2022].

Minow, Martha. "Outsourcing Power: Privatizing Military Efforts and the Risks to Accountability, Professionalism, and Democracy." In *Government by Contract: Outsourcing and American Democracy*, ed. Jody Freeman, Martha Minow. Cambridge, MA: Harvard University Press, 2009, 110–127. https://doi.org/10.2307/j.ctv22jnrsb.9. [Erişim Tarihi: 15.05.2022].

Mitchell, Paul T. "Network Centric Warfare and Coalition Operations: The New Military Operating System", *Routledge*, (2009), https://doi.org/10.4324/9780203881163 [Erişim Tarihi: 19.04.2022].

Moore, David. *Sensemaking: A Structure for an Intelligence Revolution*, Washington DC: NDIC Press, 2011.

Morell, Michael, Ellen McCarthy, "Head of State Department's Intelligence Arms on Assessing Foreign Leaders: Intelligence Matters", *Intelligence Matters*

Podcast, 2019. https://podcasts.apple.com/ee/podcast/head-state-departments-intelligence-arm-on-assessing/id1286906615?i=1000444085895 [Erişim Tarihi: 02.08.2023].

Münkler, Herfried. *The New Wars*. Oxford: Polity Press, 2005.

_____. *İmparatorluklar: Eski Roma'dan ABD'ye Dünya Egemenliğinin Mantığı*. İstanbul: İletişim Yayınları, 2009.

National Commission on Terrorist Attacks upon The United States, *The 9/11 Report*, Washington DC: 2002.

National Security Council, *National Security Council Directive on Office of Special Projects (1948)*, (1948). https://history.state.gov/historicaldocuments/frus1945-50Intel/d292 [Erişim Tarihi: 19.04.2022].

NATO, "Allied Joint Doctrine for the Conduct of Operations (AJP-3)", Brussels: NATO Standardization Office, North Atlantic Treaty Organization, 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/797323/doctrine_nato_conduct_of_ops_ajp_3.pdf [Erişim Tarihi:17.05.2022].

NATO, "NATO's Approach to Space.", North Atlantic Treaty Organization 2021. https://www.nato.int/cps/en/natohq/topics_175419.htm#:~:text=In2019%2C [Erişim Tarihi: 16.01.2023].

Newman, Edward. "The 'New Wars' Debate: A Historical Perspective Is Needed", *Security Dialogue*, C. 35, S. 2 (2004): 173–89, https://doi.org/10.1177/0967010604044975 [Erişim Tarihi: 19.04.2022].

Nixon, Shane, Ron Nixon. "In Washington, Contractors Take on Biggest Role Ever". *New York Times*. 7 Şubat 2007 https://www.nytimes.com/2007/02/04/washington/04contract.html [Erişim tarihi 02.08.2022].

North Atlantic Council. *Wales Summit Declaration*. Cardiff, 2014.

NPR. "The Secret Bunker Congress Never Used", *NPR*, 2011. https://www.npr.org/2011/03/26/134379296/the-secret-bunker-congress-never-used [Erişim Tarihi: 20.05.2022].

Nye, Joseph S.. *Cyber Power*. London: Belfer Center for Science and International Affairs of Harvard Kennedy School, 2010. https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf [Erişim Tarihi: 20.05.2022].

ODNI, *Preparing fort the 21st Century: An Appraisal of U.S. Intelligence: Report of the Commission on the Roles and Capabilities of the United States Intelligence Community*, Washington, DC: Government Printing Office, 1996.

ODNI, *National Intelligence Strategy Report 2005*, Washington DC: 2005. https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/NISOctober2005.pdf [Erişim Tarihi: 17.08.2023].

ODNI, *National Intelligence Strategy Report 2009*, Washington DC: 2009. https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2009_NIS.pdf [Erişim Tarihi: 17.08.2023].

ODNI, *National Intelligence Strategy Report 2019*, Washington DC: 2019, https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf [Erişim Tarihi: 17.08.2023].

ODNI. *Private Sector Engagement*, Washington DC: Office of the Director of The National Intelligence, 2022, https://www.dni.gov/index.php/who-we-are/organizations/national-security-partnerships/ps-engagement [Erişim Tarihi: 23.05.2022].

ODNI, *National Intelligence Strategy Report 2023*, Washington DC: 2023, https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2023.pdf [Erişim Tarihi: 17.08.2023].

Office of Strategic Services, *Office of Strategic Services Organization and Functions*, Washington DC: Hyperwar Foundation, 1945. https://www.ibiblio.org/hyperwar/USG/JCS/OSS/OSS-Functions/index.html [Erişim Tarihi: 22.04.2023].

Omand, David "The future of Intelligence: What are the threats, the challenges and the opportunities?", *The Future of Intelligence:Challenges in the 21st Century*, ed. Isabelle Duyvesteyn, Ben de Jong, Joop van Reijn. New York: Routledge, 2014, 14-26.

Palmer, Diego A. Ruiz. Back to the Future? Russia's Hybrid Warfare, Revolutions in Military Affairs, and Cold War Comparisons. (Research Paper - NATO Defense College, Sayı: 120, 2015). https://www.files.ethz.ch/isn/194718/rp_120.pdf [Erişim Tarihi: 23.05.2022].

Panda, Jagannath, Ankit Panda, "Japan Is Ready to Become a Formal Member of Five Eyes", *Center for Strategic & International Studies*, C. 3, S. 8, (2020) https://www.csis.org/analysis/resolved-japan-ready-become-formal-member-five-eyes [Erişim Tarihi: 10.04.2022].

Prelipcean, Alina, Andrei Albert, "Landmarks of Russia's Use of Information Warfare." *Strategies XXI- Security and Defense Faculty*, C. 17, S. 1 (2021): 140–144. https://doi.org/10.53477/2668-2001-21-16 [Erişim Tarihi: 10.04.2022].

Presgrove, Jed. "Blockchain in Government Will Boil Down to Policy, Practice", *GovTech*, 25 Eylül 2019, https://www.govtech.com/products/blockchain-in-government-will-boil-down-to-policy-practice.html [Erişim Tarihi: 19.08.2022].

Pukhov, Piotr. “Миф о ‘гибридной войне’. Независимое военное обозрение”, 29 Mayıs 2015.

Puyvelde, Damien Van. “Quelles leçons tirer de la privatisation du Renseignement aux États-Unis / ABD’de İstihbaratın Özelleştirilmesinden Çıkarılması Gereken Dersler”, *IRIS Editions, Revue Internationale et Stratégique*, S. 87 (2012), 42–52. https://www.researchgate.net/publication/272806351_Quelles_lecons_tirer_de_la_privatisation_du_renseignement_aux_Etats-Unis [Erişim Tarihi: 12.08.2022].

Puyvelde, Damien Van. *The US intelligence community and the private sector: How rational are privatization rationales?*. El Paso: National Security Studies Institute The University of Texas, 2014. http://web.isanet.org/Web/Conferences/ISSS%20Austin%202014/Archive/6698f449-30ac-4dda-9486-fa5951f48754.pdf [Erişim Tarihi: 19.08.2023].

Qiao, Liang , Xiangsui Wang, *Unrestricted Warfare*, New Delhi: Natraj Publishers, 2007.

Reichmann, Kelsey. “3 Space Challenges fort he Intelligence Community”, *C4ISRNET*, 4 Ağustos 2023, https://www.c4isrnet.com/battlefield-tech/space/2019/06/05/3-space-challenges-for-the-intelligence-community/ [Erişim Tarihi: 10.08.2023].

Renz, Bettina. “Russia and ‘Hybrid Warfare”, *Contemporary Politics*, C. 22, S. 3 (2016): 283–300. https://doi.org/10.1080/13569775.2016.1201316 [Erişim Tarihi: 15.05.2022].

Richelson, Jeffrey T., *The Wizards of Langley: Inside the CIA’s Directorate of Science and Technology*, Cambridge: 2002.

Robson-Morrow, Maria A.. “Private Sector Intelligence: on the Long Path of Professionalization”, *Intelligence and National Security Journal*, C. 37, S. 3 (2022), 402-420. https://www.belfercenter.org/publication/private-sector-intelligence-long-path-professionalization [Erişim Tarihi: 02.08.2022].

Romdhani, Oussama. “Tunisia, the West, and the ‘Arab Spring’ ”, *The Atlantic Council*, (2017). https://www.atlanticcouncil.org/blogs/menasource/tunisia-the-west-and-the-arab-spring/ [Erişim Tarihi: 10.04.2022].

Roper, James E.. “Using Private Corporations to conduct Intelligence Activities for National Security Purposes: An Ethical Appraisal” *International Journal of Intelligence Ethics*. C. 1, S. 2 (2010), 46-73.

Royal Air Force, UK Space Command, (2022), https://www.raf.mod.uk/what-we-do/uk-space-command/ [Erişim Tarihi: 15.05.2022].

Ruffner, Kevin C.. *CORONA: America’s First Satallite Program*, Washington DC: CIA History Staff Center for the Study of Intelligence (1995).

Rumer, Eugene. “The Primakov (Not Gerasimov) Doctrine in Action.” *Carnegie Endowment for International Peac*e, C. June 2019, (2019): 1–10.

Rumsfelt, Donald. *The National Defense Strategy of the United States of America*. Washington DC: 2005.

Russell, Stuart, Peter Norvig. *Artificial Intelligence: A Modern Approach*. New Jersey: Pearson, 2010.

Shorrock, Tim. *Spies for Hire_ The Secret World of Intelligence Outsourcing* New York: Simon & Schuster, 2008.

_____. “The Corporate Takeover of U.S. Intelligence”, *Salon*, 2007. https://www.salon.com/2007/06/01/intel_contractors/ [Erişim Tarihi: 14.05.2022].

_____. “5 Corporations Now Dominate Our Privatized Intelligence”. *The Nation*, 8 Eylül 2016. https://www.thenation.com/article/archive/five-corporations-now-dominate-our-privatized-intelligence-industry/ [Erişim Tarihi: 05.Mayıs 2022].

Shovelan, John. *9/11 Commission Finds ‘Deep Institutional Failings,* Australian Broadcasting Corporation, 2006, https://www.abc.net.au/am/content/2004/s1160100.htm [Erişim Tarihi: 06.05.2023].

Sinclair, Sebastian. “CipherTrace Says Homeland Security Work Gave Rise to Monero-Tracking Patent Filings”, *Coindesk*, 2020. https://www.nasdaq.com/articles/ciphertrace-says-homeland-security-work-gave-rise-to-monero-tracking-patent-filings-2020 [Erişim Tarihi: 10.05.2022].

Singer, Peter W.. “The Private Military Industry and Iraq : What Have We Learned and Where to Next?”, *Geneva Centre for the Democratic Control of Armed Forces (DCAF) Policy Paper*, Kasım 2004. https://www.files.ethz.ch/isn/14132/PP4_Singer.pdf [Erişim Tarihi: 02.04.2022].

Smith, Edward. *Effect Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War*, Washington DC: CCRP- Cforty Onesr Cooperative Research Publication, 2002.

Spiegeleire, Stephan De, Matthijs Maas, Tim Sweijs. *Artificial Intelligence and the Future of Defense: Strategic Implications for Small and Medium-sized Force Providers*. Nederlands: Hague Centre for Strategic Studies, 2017.

Sterio, Milena. “Lethal Use of Drones When the Executive Is the Judge, Jury, and Execution”, *The Independent Review*, C. 23, S. 1 (2018), 35–50.

StrategyR. “Big Data World Market Report”, https://strategyr.com/market-report-big-data-forecasts-global-industry-analysts-inc.asp [Erişim Tarihi: 16.07.2023].

Sugarman, Jacob. “You Can’t Have 100 Percent Security and Also Have 100 Percent Privacy’, Key Quotes from the President’s Defense of His Government’s Secret Surveillence Program”, *Salon*, 7 Haziran 2013, https://www.salon.com/2013/06/07/you_cant_have_100_percent_security_and_also_have_100_percent_privacy/ [Erişim Tarihi: 03.08.2022].

Thiessen, Marc A.. “Intelligence Beyond 2018: A Conversation with CIA Director Mike Pompeo”, *AEI Events Podcast*, American Enterprise Institute, 2019 https://www.aei.org/events/intelligence-beyond-2018-a-conversation-with-cia-director-mike-pompeo-livestreamed-event/ [Erişim Tarihi: 23.08.2023].

Tokmakoğlu, Gürsel. “Hibrit Savaş”, *Politik Merkez*, 2021. https://politikmerkez.com/konular/guvenlik/hibrit-savas/ [Erişim Tarihi: 06.05.2023].

Torres-Baches, Efren R. "Welcoming the New Age of Intelligence", *Journal of European and American Intelligence Studies*, C. 1, S. 2, (2018), 17–30.

TRADOC, “The U.S. Army in Multi-Domain Operations 2028 - TRADOC Pamphlet 525-3-1”, Washington DC, U.S. Army Training and Doctrine Command, 2018. https://api.army.mil/e2/c/downloads/2021/02/26/b45372c1/20181206-tp525-3-1-the-us-army-in-mdo-2028-final.pdf [Erişim Tarihi: 06.05.2023].

Treverton, Gregory F., Seth G. Jones, Steven Boraz, Phillip Lipscy, *Toward a Theory of Intelligence: Workshop Report*, (Santa Monica California: RAND, 2006)

Treverton, Gregory F.. “The Future of Intelligence: Changing Threats, Evolving Methods”. *The Future of Intelligence Challenges in the 21st Century*. ed. Isabelle Duyvesteyn, Ben de Jong and Joop van Reijn. New York: Routledge, 2014, 27-38.

Tucker, Patrick. “‘Underground’ May Be the U.S. Military’s Next Warfighting Domain”, *Defense One*, 2018. https://www.defenseone.com/technology/2018/06/underground-may-be-us-militarys-next-warfighting-domain/149296/ [Erişim Tarihi: 06.08.2023].

UK Ministry of Defence, “UK Terminology Supplement to NATOTerm (2019 Edition)”, London: Joint Doctrine Publication 0-01.1, (2019). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1138055/20230220-JDP_0_01_1_2023_Edition_A.pdf [Erişim Tarihi: 06.05.2023].

UK Ministry of Defense. *The Orchestration of Military Strategic Effects*, London: UK Ministry of Defence, 2021.

UNGA, *The United Nations General Assembly Resolution 2625, The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States*, New York: Resolution 2625, (1970), https://www.un.org/ruleoflaw/files/3dda1f104.pdf [Erişim Tarihi: 06.05.2023].

US Army, *US Army Multi-Domain Intelligence FY21-22 S&T Focus Areas*, Washington DC: US Army, 2022.

US Department of Defense, "Quadrennial Defense Review Report", *Quadrennial Defense Review: Assessing U.S. Defense and Security*, (Washington DC: 2006) https://www.airforcemag.com/PDF/DocumentFile/Documents/2006/QDR2006_020606.pdf [Erişim Tarihi: 06.05.2023].

US Department of Defence, *JP 3-13 Information Operations*, Washington DC: Joint Publication Series, 1(1), 2014.

US Department of Defense, US Space Command, (2022) https://www.spacecom.mil/ [Erişim Tarihi: 15.05.2022].

US Presidency, *The National Security Strategy of the United States 2002*, Washington DC: The White House, 2002, https://web.archive.org/web/20100307072859/http://georgewbush-whitehouse.archives.gov:80/nsc/nss/2002/nss.pdf [Erişim Tarihi: 15 Ağustos 2023].

Uşaklı, Ali Bülent, İrfan Hasan Alper. "Teknolojik Gelişmelerin Savaşları Dönüştürmesi ve Gelecekteki Savaşlara Hazır Olmak.", *Savaş: Farklı Disiplinlerde Yeni Yaklaşımlar*, der. Haldun Yalçınkaya, (Ankara: Siyasal Kitap Yayın-Dağıtım, 2010).

Voelz, Glenn James. *Managing the Private Spies: the Use of Commercial Augmentation for Intelligence Operations*, Washington DC: Joint Military Intelligence Collage Press, 2006.

Yalçınkaya, Haldun. "Savaşın Değişimi ve Savaş Çalışmalarında Farklı Disiplinler", *Savaş: Farklı Disiplinlerde Yeni Yaklaşımlar*, der. Haldun Yalçınkaya (Ankara: Siyasal Yayın-Dağıtım, 2010).

Yalçınkaya, Haldun, Kadir Tamer Türkeş. "Yirmi Birinci Yüzyılda Çatışma Alanlarında Görülen Yeni Unsurlar". *Güvenlik Stratejileri Dergisi*, C. 4, S. 7 (2008): 55–90, https://dergipark.org.tr/en/pub/guvenlikstrtj/issue/7536/99214 [Erişim Tarihi: 06.05.2023].

Yıldız, Gültekin. "Hibrit Savaş Ne Kadar Post-Moderndir? Avrasya Askerî Tarihine Yeniden Bakış", *Hibrit Savaş; Savaşın Değişen Modeli*, İstanbul: Milli Savunma Üniversitesi Basımevi, 2018.

Zegart, Amy, Michael Morell. "Spies, Lies and Algorithms: Why U.S. Intelligence Agencies Must Adapt or Fail", *Foreign Affairs*, 2019, https://foreignaffairs.com/articles/2019-04-16/spies-lies-and-algorithms , [Erişim Tarihi: 23.08.2023].