ANALİZ

TÜRK DÜNYASINDA İSTİHBARAT PAYLAŞIMI: ORTAK GÜVENLİKTE STRATEJİK FIRSATLAR

Doç. Dr. Muhammet Koçak

EKİM 2025

Milli İstihbarat Akademisi

TÜRK DÜNYASINDA İSTİHBARAT PAYLAŞIMI: ORTAK GÜVENLİKTE STRATEJİK FIRSATLAR

Doç. Dr. Muhammet Koçak

ANALİZ / EKİM 2025

Milli İstihbarat Akademisi

Milli İstihbarat Akademisi

Telif

Yayın Tarihi: Ekim 2025

Millî İstihbarat Akademisi
E-Posta: bilgi@mia.edu.tr

"Bandrol Uygulamasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 5'inci maddesinin 2'nci fıkrası çerçevesinde bandrol taşıması zorunlu değildir."

ANALİZ / Ekim 2025

TÜRK DÜNYASINDA İSTİHBARAT PAYLAŞIMI: ORTAK GÜVENLİKTE STRATEJİK FIRSATLAR

İÇİNDEKİLER

TABLO

YÖNETİCİ ÖZETİ

- Türk devletleri arasındaki güvenlik iş birliği, 1992 yılında "Türk Dili Konuşan Ülkeler Zirvesi"yle başlamıştır. Söz konusu iş birliği; 2009 Nahçıvan Anlaşması ile Türk Keneşi olarak kurumsallaşmış ve 2021 İstanbul Zirvesi'nde Türk Devletleri Teşkilatı (TDT) kimliğine kavuşarak çok taraflı güvenlik koordinasyonunun kurumsal temelini oluşturmuştur.
- İstihbarat paylaşımı, 1998 yılında imzalanan "Türk Dilli Devletler İstihbarat Servisleri Konferansı Protokolü" ile kurumsal bir zemine oturmuştur. Her yıl servis başkanlarının toplantılarıyla geliştirilen bu iş birliği, 2019 Zirvesi'nden sonra Ankara'da kurulan Daimî Sekretarya ile organizasyonel nitelik kazanmıştır.
- Türk dünyasının bulunduğu coğrafya; ABD'nin küresel angajmanını daraltması, Avrupa-Atlantik güvenlik mimarisinin Ukrayna savaşı sonrası yaşadığı sarsıntılar ve Çin'in Kuşak ve Yol Girişimi'yle artan projeksiyonu nedeniyle büyük güç rekabetinin odak noktalarından biri hâline gelmiştir.
- Bu bağlamda istihbarat paylaşımı, sadece müşterek tehditlere karşı erken uyarı ve hızlı müdahale imkânı sunmakla kalmayıp stratejik karar süreçlerinde bilgi üstünlüğü sağlayarak Türk dünyasının kolektif caydırıcılığını artırmaktadır.
- Türk devletleri arasındaki istihbarat paylaşımının derinleştirilmesi; var olan birlik ve güven ortamını pekiştirecek ve ortak hareket kapasitesini ileriye taşıyacaktır. Böylece bölgeye yönelen dış ilgi ve rekabetten daha fazla stratejik fayda elde edilebilecek, aynı zamanda ortaya çıkabilecek risk ve tehditlere karşı daha güçlü bir koruma zemini sağlanabilecektir.

GİRİŞ

Türk devletleri arasında istihbarat paylaşımı, son 30 yılda gelişen çok boyutlu iş birliğinin, güvenlik alanındaki en kritik ve stratejik unsurlarından biri hâline gelmiştir. TDT; 2009 Nahçıvan Anlaşması ile başlatılan kurumsallaşma sürecini, 2021 İstanbul Zirvesi'nde konsey formatından, çok taraflı bir uluslararası örgüt yapısına dönüştürerek bu gerekliliğe kurumsal bir karşılık üretmiştir. Güvenlik mimarisinin en kritik bileşenlerinden biri olan istihbarat paylaşımı da bu gelişmelere paralel ilerleme kaydetmiştir. 1998 yılında gerçekleştirilen Türk Dilli Devletler İstihbarat Servisleri Konferansı Protokolü ile kurumsal bir zemine oturan ve 2019 yılında gerçekleştirilen zirve sonrasında Daimî Sekretaryasına kavuşan bu alandaki ortaklık; Türk devletleri arasındaki iş birliğinde öncü bir rol üstlenmiştir. Bu kapsamda:

- Türkiye'nin, çok taraflı ve proaktif dış politika vizyonu çerçevesinde Türk dünyasına stratejik öncelik vermesi,
- Azerbaycan'ın, Karabağ zaferi sonrasında dış politikasının merkezine Türk dünyasını yerleştirmesi,
- Kazakistan ve Kırgızistan'ın, bağımsız dış politika arayışları kapsamında büyük güçlerle olan ilişkilerini Türk dünyası ekseninde dengeleme stratejisi ve
- Özbekistan'ın, Mirziyoyev Dönemi'yle birlikte TDT çalışmalarına aktif ve kararlı biçimde dâhil olması,

TDT'nin güvenlik boyutunu tüm üye devletler açısından vazgeçilmez ve yüksek getirili bir mekanizmaya dönüştürmüştür. Bu gelişmeler, büyük güçler arasındaki rekabetin şiddetlendiği ve küresel dönüşümlerin hız kazandığı gelişmelerin odak noktasına yerleşen Türk dünyasına güç kazandırmaktadır.

İstihbarat paylaşımı; Türk devletleri arasında güvenliği pekiştiren, ortak tehdit tanımlarını ve koordineli risk yönetimini mümkün kılan bir kuvvet çarpanı hâline gelmiştir. Mevcut iş birliği, FETÖ ve DEAŞ gibi örgütlere karşı operasyonlarda somut sonuçlar vermiş; servis başkanlarının düzenli toplantıları, kurumsallaşma sürecini hızlandırmıştır. Türkiye'nin sınır ötesi operasyon ve kapasite geliştirme tecrübesi ile Azerbaycan, Kazakistan, Kırgızistan ve Özbekistan'ın tamamlayıcı yetkinlikleri birleştiğinde, çok boyutlu bir güvenlik mimarisi ortaya çıkmaktadır. Bu kapasite havuzu; bilgi paylaşımının ötesinde kriz

yönetimi, ortak tatbikat ve stratejik analiz üretimi gibi alanlarda karşılıklı öğrenmeyi desteklemekte, ilerleyen kurumsallaşmayla birlikte Türk devletlerini hem bölgesel hem de küresel ölçekte etkili bir güvenlik aktörü konumuna taşıma potansiyeli sunmaktadır.

Bu çalışma, açık kaynaklar üzerinden TDT üyesi devletler arasındaki istihbarat paylaşımını teknik, hukuki ve kurumsal boyutlarıyla analiz etmekte; mevcut durumun güçlü ve zayıf yönlerini belirleyerek sürdürülebilir kurumsallaşma için bir yol haritası sunmaktadır. Çalışmada; literatürdeki modeller, sahadaki uygulamalar ve atılabilecek adımlar bütüncül bir yaklaşımla ele alınmakta, istihbarat paylaşımının Türk dünyasının güvenlik mimarisine ve geniş dış politika hedeflerine katkısı, kapsamlı bir biçimde değerlendirilmektedir.

İSTİHBARAT VE İSTİHBARAT PAYLAŞIMI

İstihbarat; devletlerin güvenlik mekanizmasının ayrılmaz bir parçası olup karar alma süreçlerinde, belirsizlikleri azaltarak tehditlere karşı zamanında ve etkili tepki geliştirilmesine imkân tanır. Doğru yapılandırılmış bir istihbarat döngüsü; riskleri tespit etmekle kalmayıp fırsatların değerlendirilmesine ve stratejik hedeflerin gerçekleştirilmesine de katkı sağlamaktadır. Bu çerçevede istihbarat, ulusal güvenliğin hem koruyucu hem de yönlendirici bileşeni hâline gelmektedir. Günümüzde ise istihbarat; bilgi toplama ve analiz üretme faaliyetleri dışında, devletler arası ilişkilerin yönetiminde bir diplomasi aracı olarak da işlev görmektedir. İstihbarat diplomasisi; farklı ülkelerin servisleri arasında güven inşası, kriz yönetiminde iş birliği ve karşılıklı kapasite paylaşımı yoluyla stratejik etki üretmektedir.

İstihbarat alanındaki uluslararası iş birliği; devletlerin tek başına aşamayacağı coğrafi, teknik ve beşerî sınırlılıkları gidermenin yanı sıra, ortak tehditlere karşı kapasite ve etki alanını genişleten stratejik bir araç niteliği taşımaktadır. Güvenlik mimarisinin en kritik bileşenlerinden biri olan istihbarat paylaşımı yalnızca bilgi transferi değil; aynı zamanda ortak tehdit tanımları, koordineli risk yönetimi ve stratejik karar süreçlerinde bilgi üstünlüğü sağlayan bir kuvvet çarpanı niteliğindedir. İyi yapılandırılmış ve kurumsal çerçeveye oturtulmuş bir istihbarat paylaşımı mekanizması; terörizm, yasa dışı göç, sınıraşan organize suç ve siber saldırılar gibi müşterek tehditlerin önceden tespit edilmesine ve bu tehditlerle mücadele edilmesine imkân tanımaktadır. Aynı zamanda savunma sanayisinden enerjiye, ekonomiden güvenliğin farklı alanlarına derinlemesine iş birliği imkânlarını genişletmektedir.

Uygulamada ikili ve çok taraflı iş birliği örnekleri bulunsa da bilgi teatisinin ötesine geçerek "finansal, teknik ve eğitim destekleri"ni de kapsayan çok boyutlu iş birliği, çoğunlukla stratejik düzeydeki yakınlaşmanın sonucu olarak ortaya çıkmaktadır.[1] Devletlerin sınırsız bilgi toplama/işleme kapasitesini haiz olamaması, onları dış politika hedefleri ve ulusal çıkarları doğrultusunda iş birliğine yöneltmektedir.[2] Belirli teknik olanaklara erişim imkânı da iş birliği motivasyonları arasında yer almaktadır. Faydanın belirgin, riskin görece düşük olduğu bağlamlarda, iş birliği ihtimali artmaktadır. Bazı durumlarda ise iş birliği, karşı tarafın dış politikasını etkilemeye dönük bir araç işlevi de görebilmektedir.[3] Bu çok katmanlı mimari, tek bir devlet dâhilinde yürütüldüğünde dahi yoğun kaynak tüketmektedir; dahası coğrafi, teknik ve dilsel sınırlılıklar sebebiyle kapsama boşlukları ortaya çıkmaktadır. BM Güvenlik Konseyi, bu konuda yayımladığı bir raporda özellikle terörle mücadele açısından istihbarat paylaşımının

önemine dikkat çekmektedir.[4] Bu çerçevede istihbarat paylaşımı sürecinde bulunan devletler, paylaşılan istihbarat karşılığında birbirlerinden istihbari ya da diğer alanlarda fayda sağlayabilmektedir.[5] İstihbarat paylaşımı; söz konusu boşlukları, menzil/uzmanlık çeşitliliği ve farklı devletlerin tamamlayıcı katkılarıyla kapatmaktadır. Aynı zamanda belirsizlik azaltma işlevini, kolektif bir düzleme taşımaktadır.

Bu konuda tarihsel örneklere bakıldığında, özellikle Batı dünyasında ciddi bir kapasite inşası göze çarpmaktadır. II. Dünya Savaşı'nda ABD ile Birleşik Krallık arasında akdedilen BRUSA Anlaşması, bu durumun tarihî prototipini oluşturmuş; farklı dinleme istasyonları ile şifre çözme kapasiteleri birleştirildiğinde Enigma trafiğinin kırılması mümkün olmuştur. Bu tecrübe, 1946 tarihli UKUSA Paktı'na ve daha sonra Five Eyes olarak bilinen çok taraflı SIGINT topluluğuna evrilmiş;[6] Avustralya'daki Pine Gap Tesisi gibi ortak altyapılar, küresel sinyal erişimini geometrik biçimde genişletmiştir.[7] Benzer şekilde, eski Sovyet coğrafyasında da KGB mirası üzerine inşa edilen Bağımsız Devletler Topluluğu (BDT) İstihbarat Servisleri Başkanları Konferansı; terörizm, sınıraşan suçlar ve organize kaçakçılıkla mücadele konularında üye servisler arasında bilgi değişimi, ortak operasyon koordinasyonu ve teknik eğitim programlarını kapsayan bir platform olarak işlev görmüştür.[8]

Bilgi değişimine dayalı iş birliğinde, kaynak ve yöntem paylaşımı ise istisnai bir uygulama olarak ortaya çıkmaktadır. Soğuk Savaş'ta, ABD-SSCB eksenli kutuplaşmanın ve NATO çerçevesindeki ortak stratejik hedeflerin, servisler arası iş birliği için kurumsal bir zemin sağladığı; buna paralel olarak Five Eyes örneğinin kaynak ve yöntem paylaşımını kurumsallaştıran istisnai bir model olarak öne çıktığı görülmektedir.[9] Soğuk Savaş sonrasında kitle imha silahlarının yayılması, organize suç, düzensiz göç ve uyuşturucu ticareti gibi sınıraşan tehditler ile küreselleşmenin yarattığı yeni güvenlik riskleri; Avrupa'da Bern Kulübü etrafında şekillenen ve bugün INTCEN (European Union Intelligence and Situation Center, Avrupa Birliği İstihbarat ve Durum Merkezi) ile Europol'ün (European Union Agency for Law Enforcement Cooperation, Avrupa Birliği Kolluk Kuvvetleri İş Birliği Ajansı) desteklediği ancak merkezî bir istihbarat otoritesine evrilmemiş iş birliği modellerini teşvik etmektedir.[10] 11 Eylül sonrasında "terörizmle mücadele" iddiasıyla Orta Doğu ve Orta Asya'ya uzanan ağların genişlemesi, bilgi paylaşımını kritik bir kuvvet çarpanı hâline getirmekte ve güven inşasını temel ön koşul olarak öne çıkarmaktadır.[11]

Bu genel eğilimler ışığında, siyasal iradenin baskın olduğu mevcut konjonktürde, TDT üyesi servisler arasında iş birliğinin "karşılıklı fayda, ortak tehdit tanımı ve tamamlayıcı yeteneklere dayalı" olarak kademeli biçimde derinleşmesi mümkün görünmekte; "spillover" (yayılma) etkisiyle ikili düzeydeki stratejik yakınlaşmaların, çok taraflı mimariye taşınabilmesi için kurumsal standartlar ve ortak uygulama pratiklerinin güçlendirilmesi gerekmektedir. Literatürde "birlikte büyümek" olarak da tanımlanan istihbarat alanında iş birliğinin ilgili taraflar açısından etkisi, politika yapıcıların stratejik gayelerine ulaşmalarını destekleyen kalıcı bir araç seti sunmaktadır.[12] Aynı zamanda koordinasyon, kapasite/yetenek uyumu ve kurumsal güvenin eş güdümü sağlandığında, uzun vadeli bir güvenlik değeri üretmektedir.

Mezkûr iş birliklerinin çıktıları, bu denli çarpıcı olsa da paylaşım süreci; dört yapısal risk ve engelle sınırlanmaktadır. Bunlardan ilki; tarafların hangi verinin hangi gizlilik bandında, hangi hukuki ve teknik standartla, hangi maliyet paylaşımıyla ve hangi takvimde aktarılacağı konusunda uzlaşmasını gerektiren pazarlık ve etik sorunlarıdır. Örneğin Avrupa Birliği'nin (AB) Yolcu İsim Kayıtları (PNR) direktifi,

---

üye devletlerin başlangıçta istediği 5 yıllık saklama süresini ve tüm uçuş rotalarını kapsama hedefini, Avrupa Adalet Divanının mahremiyet kaygıları doğrultusunda 6 aya ve yalnızca riskli hatlarla sınırlayacak biçimde daraltmıştır. Metin, mahkeme kararlarıyla şekillenen uzun hukuki-siyasal pazarlıkların sonunda yürürlüğe girebilmiştir.[13]

İkinci risk, mutabakat sonrasında taraflardan birinin "hatalı, güncelliğini yitirmiş, eksik veri aktarması ya da bilgiyi üçüncü aktöre sızdırması" biçiminde ortaya çıkan uygulama sorunudur. 2015 yılında Hollanda'ya ait F-16'ların, Musul'da bir ailenin evini "karargâh" zannıyla vurması ve Havice'deki bomba üretim tesisine düzenlenen saldırıda en az 70 sivilin hayatını kaybetmesi, koalisyon içinde paylaşılan yetersiz istihbaratın ağır sonuçlar üretebildiğini göstermiştir. Paylaşım hatası, uluslararası insancıl hukuk bakımından "meşru hedef" kriterini karşılıyor görünse de bilgiyi sağlayan devlet üzerinde ciddi etik sorumluluk doğurmaktadır. Bilginin kaynağa zarar vermeden doğrulanması güç olduğu için hatalı iletimin tespiti, hâlen maliyetli ve zaman alıcı olabilmektedir.[14]

Üçüncü risk ise paylaşılan bilginin üçüncü ülkelere sızması ve riskin dolaylı olarak yine etik boyutta ortaya çıkmasıdır. Verinin üçüncü taraflara sızması, tedarik zincirindeki açıklar veya teknik arka kapılar üzerinden yapılabilecek manipülasyonlar, tüm ağın güvenlik bütünlüğünü tehlikeye atabilmektedir. Bu çerçevede, istihbaratın denetiminde karşılaşılan genel zorlukların da paylaşım mekanizmasının bütünlüğünü tehdit etme potansiyeli bulunmaktadır.[15] Bunların yanı sıra devletlerin tehdit algılarının çeşitliliği de "paylaşılan istihbaratın, paylaşan tarafın aleyhine kullanılma sorununu" beraberinde getirebilmektedir.[16] Geçtiğimiz yıllarda Danimarka Savunma İstihbarat Servisinin (FE), ABD Ulusal Güvenlik Ajansı (NSA) ile Baltık iletişim trafiğini paylaştığına dair iddialar, üçüncü ülkelerin mahremiyetinin ihlal edilmiş olabileceği yönündeki tartışmaları tetiklemiştir.[17] Keza bilgi akışının siyasallaştırılması ve iç politika amaçlarıyla kullanılması sonucu, meşruiyet ve güvenin zayıflaması da riskler arasında sayılabilir.[18] Son olarak Fransa'nın, bazı Kuzey Afrika güvenlik kurumlarına sağlamış olduğu terör izleme verilerinin, muhalif odaklı hedefleme operasyonlarında kullanıldığına ilişkin bulgular, Fransız Parlamentosunda güçlü bir yankı bulmuştur.[19]

Tablo 1: İstihbarat Paylaşımında Fırsatlar ve Riskler

Fırsatlar	Riskler
Ortak tehdit tanımlarına dayalı güven inşası ve tamamlayıcı kapasite kullanımı	Veri paylaşımında gizlilik, teknik standartlar ve maliyet paylaşımı konularında uzlaşma zorlukları
Coğrafi, teknik ve beşerî sınırlılıkların aşılması ve kapsama alanının genişlemesi	Yanlış, eksik veya güncelliğini yitirmiş veri aktarımı ve bunun operasyonel sonuçları
Terörizm, organize suç, yasa dışı göç ve siber saldırılar gibi alanlarda erken uyarı ve caydırıcılığın güçlenmesi	Üçüncü taraflara veri sızması, tedarik zinciri açıkları ve teknik manipülasyon riski
Kurumsal standartlar ve ortak uygulamalar yoluyla çok taraflı iş birliğinin derinleşmesi	Bilgi akışının siyasallaştırılması, iç politika amaçlı kullanımı ve güvenin zedelenmesi

Bu engellerin yaratacağı riskler üç ana düzenek yardımıyla hafifletilmektedir. Birincisi, yüksek karşılıklı güven modelidir. Five Eyes iş birliği, ortak tarihî bağ ve yakın tehdit algısı sayesinde ham sinyal akışının paylaşıldığı derinlemesine entegrasyon örneği sunmaktadır. İkincisi, kurumsal-denetim temelli modeldir. AB'nin INTCEN bünyesindeki Hybrid Fusion Cell; yeniden-paylaşım kısıtları, konsey gözetimindeki bağımsız denetim mekanizmaları ve yeknesak rapor şablonlarıyla veri bütünlüğünü güvence altına almaktadır. Ancak tam şeffaflık beklentisi, istihbarat faaliyetinin gizlilik ilkesini hâlen zorlayabilmektedir.[20] Üçüncü düzenek, hiyerarşik yapılanmadır. ABD-Japonya SIGINT ilişkisi, bu yapıya tipik bir örnek oluşturmaktadır. ABD, Japonya'daki yaklaşık 100 ayrı tesiste yürüttüğü faaliyetler aracılığıyla teknik parametreleri, öncelikleri ve operasyonel çerçeveyi belirleyen baskın aktördür. Katkısı sınırlı olan bir "üçüncü taraf" konumunda yer alan Japonya ise yalnızca HF/VHF yön bulma verileri gibi düşük seviyeli bilgileri paylaşabilmekte, buna karşılık üst düzey kriptolojik materyallere erişim imkânı bulamamaktadır.[21] Uygulamada bu üç model; mutlak biçimde değil, esnek bir bileşim hâlinde karşımıza çıkmaktadır. Güven tabanı zayıfladığında ise kurumsal sıkılaştırma yahut hiyerarşik denetim devreye alınmaktadır. Örneğin BDT istihbarat paylaşım modeli; ortak Sovyet mirasından kaynaklanan kurumsal güven ile Rusya'nın baskın kapasitesine dayalı hiyerarşik unsurlarını birleştiren hibrit bir yapı sergilemektedir.

Tablo 2: Farklı İstihbarat Paylaşım Mekanizmalarının Avantaj ve Dezavantajları

Model	Avantajlar	Dezavantajlar
Yüksek Karşılıklı Güven Modeli (ör. Five Eyes)	▪ Derinlemesine entegrasyon ve ham veri paylaşımı ▪ Ortak tehdit algısı sayesinde hızlı uyum ▪ Operasyonel verimlilik ve güven tabanlı dayanışma	▪ Derin tarihî bağ ve yüksek güven düzeyi gerekliliği ▪ Yeni katılımcılara kapalı, dışlayıcı yapıya sahip ▪ Güven zayıfladığında kırılganlaşma riski
Kurumsal-Denetim Temelli Model (ör. INTCEN)	▪ Standart raporlama ve denetim mekanizmalarıyla veri bütünlüğü sağlama ▪ Şeffaflık ve hesap verebilirlik imkânı ▪ Çok taraflı iş birliği için kapsayıcı çerçeve	▪ Şeffaflık beklentisinin istihbaratın gizlilik doğasıyla çelişme riski ▪ Ağır bürokrasi ve karar alma süreçlerinde hantallık ▪ Acil krizlerde esneklik sınırlı
Hiyerarşik Yapılanma Modeli (ör. ABD-Japonya SIGINT)	▪ Baskın aktörün yönlendirmesiyle yüksek teknik kapasiteye erişim ▪ Görev önceliklerinde netlik ▪ Zayıf aktör için kapasite geliştirme imkânı	▪ Alt ortak için sınırlı katkı ve özerklik kaybı ▪ Erişim, düşük seviyeli veriyle sınırlı kalabilir ▪ İlişki dengesizliğinin yol açabileceği güven sorunu

---

Sonuç olarak istihbarat paylaşımı, hiçbir devletin tek başına ulaşamayacağı bilgi üstünlüğünü sağlayarak güvenlikten diplomasiye kadar uzanan geniş bir alanda, stratejik değerler üretmektedir. Ancak artan hassasiyet, pazarlık ve uygulama kaynaklı riskleri yönetebilecek dengeli bir mimari gerektirmektedir.

TÜRK DEVLETLERİ ARASINDA İSTİHBARAT PAYLAŞIMI

Soğuk Savaş'ın sona ermesiyle bağımsızlığını kazanan Türk cumhuriyetleri ile Türkiye arasında; ortak tarih, dil ve kültürden beslenen siyasi ve ekonomik temaslar, hızla kurumsal bir nitelik kazanmıştır. 1990'lardan itibaren güçlenen bu etkileşim, yalnızca kültürel bağları pekiştiren bir diplomasi hattı değil, aynı zamanda bölgesel jeopolitiğin değişen dengeleri içinde ortak güvenlik çıkarlarını koruyacak bir dayanışma zemini de oluşturmuştur.

Türk devletleri arasındaki kurumsal iş birliğinin temelleri, 1992 yılında Ankara'da Türkiye'nin ev sahipliğinde başlatılan Türk Dili Konuşan Ülkeler Devlet Başkanları zirveleri ile atılmıştır. Azerbaycan, Kazakistan, Kırgızistan, Türkmenistan ve Özbekistan'ın katılımıyla kurulan bu platform, Türkiye'ye Orta Asya ve Azerbaycan'da daha güçlü bir dayanak ve etki alanı oluşturma imkânı sunmuş; aynı zamanda İran ve Rusya'nın bölgesel projeksiyonlarına karşı dengeleyici bir işlev görmüştür. Türk devletleri arasında 2010'larda katedilecek birlik çabalarına mütevazı bir başlangıç teşkil eden bu zirveler; politik, ekonomik ve güvenlik başlıklarında müzakereler için kalıcı bir zemin sağlamış ve birçok güvenlik alanında yoğun iş birliğini teşvik eden bir rol üstlenmiştir.

Bu sürecin istihbarat boyutu, 20 Mayıs 1998 tarihinde Azerbaycan, Kazakistan, Kırgızistan, Türkiye ve Türkmenistan tarafından imzalanan protokol ile kurulan "Türk Dilli Devletler İstihbarat Servisleri Konferansı" ile kurumsal bir zemine oturmuştur. Her yıl dönüşümlü olarak farklı bir üye ülkenin ev sahipliğinde gerçekleştirilen bu toplantılar; terörizm, aşırılık, sınıraşan suçlar, uluslararası ulaştırma koridorları ve enerji hatlarının güvenliği gibi konularda ortak değerlendirme ve uygulamaları gündeme getirmektedir. Bu çerçevede düzenlenen toplantıların, liderler düzeyinde sahiplenildiği de görülmektedir. İstihbarat başkanlarının 2019 yılında Bakü'de Azerbaycan Cumhurbaşkanı İlham Aliyev tarafından kabul edilmesinin ardından, Türk Konseyi İstihbarat Kurumları Konferansı Daimî Sekretaryasının Ankara'da kurulması, bu alandaki çalışmalara ivme kazandırmıştır.[22] Kırgızistan Cumhurbaşkanı Sadır Caparov'un 2022 yılında, benzer bir toplantıda yaptığı "yakın etkileşimin güvenliği güçlendireceği" vurgusu, bu diplomatik hattın geniş bir yelpazede ritme kavuştuğunu göstermektedir.[23] Takip eden yıllarda, istihbarat başkanları seviyesinde başlayan bu süreç, ilgili servislerin farklı birimlerinin iş birliklerine imkân tanımıştır. Bu durum, istihbarat iş birliğinin teknik bir faaliyet olmanın ötesine geçtiğini ve ortak güvenlik vizyonu temelinde şekillenen siyasi bir iradeyle desteklendiğini ortaya koymaktadır. Devlet başkanlarının sürece doğrudan dâhil olması, servisler arası etkileşimi kurumsal bir çerçeveye oturtmakta ve iş birliğinin sürekliliğini güvence altına almaktadır. Böylelikle bölgesel güvenlik tehditlerine karşı kolektif bir refleks geliştirme kapasitesi artmakta; karar alma süreçleri, daha senkronize olmaktadır.

Söz konusu sürece paralel olarak yürütülen somut operasyonlar, istihbarat paylaşımının sahadaki etkisini net bir biçimde ortaya koymuştur. 2016 sonrasında FETÖ ile mücadelede Millî İstihbarat Teşkilâtının (MİT); Kazakistan, Kırgızistan, Azerbaycan ve Özbekistan istihbarat servisleriyle yürüttüğü koordinasyon, "örgütün Orta Asya'daki yapılanmasının tasfiyesi, kritik isimlerin yakalanarak Türkiye'ye getirilmesi ve FETÖ'ye bağlı okulların kapatılması" gibi sonuçlar üretmiştir.[24] Kırgızistan'da 2021 yılında yakalanan FETÖ'nün sözde Orta Asya sorumlusu Orhan İnandı'nın Türkiye'ye getirilmesi,[25] 2020'lerde Azerbaycan'da gerçekleştirilen seri operasyonlarla firari örgüt üyelerinin yakalanması[26] ve 2022 yılında Özbekistan'dan Gürbüz Sevilay'ın iadesi; bu iş birliğinin öne çıkan örnekleridir.[27] Bunun yanında, DEAŞ'ın Azerbaycan'daki yeni yapılanmasının ortaya çıkarılması[28] ve Kazakistan ile yürütülen ortak istihbarat faaliyetleri; iş birliğinin terörle mücadele alanında derinlik kazandığını göstermektedir.[29]

Süreç içerisinde, istihbarat iş birliğinin ihtiyaç duyduğu kurumsal adımlar da paralel şekilde gerçekleşmiştir. Bu alandaki adımların ilk örneklerinden biri, Kazakistan ile Türkiye arasında 5 Ağustos 2022 tarihinde imzalanan ve aynı tarihte yürürlüğe giren "gizli bilginin karşılıklı korunması"na ilişkin protokolle atılmıştır. İlgili protokol, istihbarat ve askerî bilginin yanı sıra uzman değerlendirmelerinin de paylaşılacağını hükme bağlamaktadır.[30] Benzer şekilde Azerbaycan ile Kazakistan arasında imzalanan anlaşma; sağlanan bilginin yazılı izin olmadan üçüncü taraflara devredilemeyeceğini açıkça belirtmektedir. Anlaşma, böylece "yeniden-paylaşım yasağı"nı pozitif hukuka bağlamaktadır.[31] Kurumsallaşan bu temaslar, ortak altyapı oluşturma ve standart belirleme çabalarıyla desteklenerek uzun vadeli stratejik uyumun zeminini hazırlamaktadır. Bu sayede Türk dünyasında kurulan veri temelli güvenlik iş birliği, ortak normlara dayanan sürdürülebilir bir sisteme evrilmektedir.

Sonuç olarak 2010'ların ortasından itibaren Türk devletleri arasında gelişen istihbarat paylaşımı, yalnızca güvenlik kurumları arasında gerçekleşen dar kapsamlı bilgi aktarımının ötesine geçerek çok katmanlı/aktörlü ve kurumsal temellere dayalı bir iş birliği alanına dönüşmüştür. FETÖ ile mücadele gibi acil tehditlerle başlayan bu süreç; zamanla düzensiz göç, siber güvenlik, mali ve organize suçlara karşı ortak refleksler geliştirmeye evrilmiştir. Ortaya çıkan mimari; teknik protokollerle şekillenen bilgi koruma düzenlemelerinden, liderler düzeyinde sahiplenilen stratejik iş birliklerine kadar geniş bir yelpazeye yayılmaktadır. Devlet başkanlarının süreci doğrudan desteklemesi, siyasi meşruiyeti artırmakta ve iş birliğinin sürdürülebilirliğini sağlamaktadır. Tüm bu gelişmeler, Türk devletleri arasında ortaya çıkan istihbarat paylaşımı modelinin sadece güncel tehditlere karşı değil, aynı zamanda uzun vadeli güvenlik mimarisinin inşasında da belirleyici bir rol üstleneceğini göstermektedir. Bu doğrultuda kurumsallaşan iş birliği, Türk dünyasında güvenliğin müşterek bir anlayışla yönetildiği yeni bir dönem başlatmaktadır.

SONUÇ

SONUÇ

Küresel sistemin; çok kutupluluk, bölgesel çatışmaların yayılması ve devlet dışı aktörlerin yükselişiyle sarsıldığı günümüzde, Türk dünyası stratejik konumu nedeniyle büyük güç rekabetinin merkezinde yer almaktadır. ABD'nin küresel angajmanını daraltması, Avrupa-Atlantik güvenlik mimarisinin Ukrayna savaşı sonrasında yaşadığı kırılmalar ve Çin'in Kuşak ve Yol projeksiyonu; Avrasya'yı hem fırsatların hem de risklerin yoğunlaştığı bir coğrafya hâline getirmiştir.

Bu bağlamda, son 30 yılda inşa edilen güvenlik iş birliği yalnızca ikili temaslar veya sembolik toplantılarla sınırlı kalmayıp TDT çatısı altında çok taraflı kurumsal bir çerçeveye evrilmektedir. Bu süreçte istihbarat paylaşımının derinleşmesi, Türk devletleri arasındaki güveni ve koordinasyonu pekiştirmekte; enerji, ulaştırma, savunma sanayisi ve dijital pazar gibi alanlarda geliştirilen iş birliklerini tamamlayıcı bir unsur hâline gelmektedir. Böylece istihbarat paylaşımı, Türk dünyasının müşterek güvenlik vizyonunun asli bileşeni olarak hem bölgesel istikrarı korumakta hem de küresel rekabet ortamında ortak hareket kapasitesini güçlendirmektedir.

Son yıllarda Türk devletlerinin istihbarat servislerinin edindiği tecrübe ve geliştirdiği kapasiteler, istihbarat paylaşımı sayesinde tamamlayıcı bir nitelik kazanarak Türk dünyasını önümüzdeki süreçte karşılaşacağı meydan okumalara hazırlamaktadır. Türkiye'nin istihbarat kapasitesi; PKK ve FETÖ'ye karşı yürütülen mücadele, Irak ve Suriye'de nokta operasyonlar, Somali'de terörle mücadele desteği, "Terörsüz Türkiye" sürecinin koordinasyonu ve siber savunma altyapısındaki ilerlemeler sayesinde TDT bünyesindeki kurumsal istihbarat paylaşımının en güçlü dayanaklarından biri hâline gelmiştir. Azerbaycan, 2020 yılında Karabağ savaşında edindiği harp tecrübesi ile operasyonel koordinasyon konularında birikim elde etmiştir.[32] Kazakistan özellikle Hazar Denizi kıyı güvenliği, Orta Asya-Rusya-Avrupa yönlü kara ve demir yolu hatlarında sınır güvenliği teknolojilerinin uygulanması, CARICC[33] üzerinden uluslararası uyuşturucu kaçakçılığıyla mücadele kapasitesiyle dikkat çekmektedir.[34] Kırgızistan, dağlık ve zor arazi koşullarında isyan ve sınır çatışmaları sebebiyle keşif ve arazi istihbaratı konularında tecrübe sahibidir.[35] Özbekistan ise Afganistan kaynaklı terör tehdidine karşı yürüttüğü operasyonlarında edindiği deneyim ve radikal ağların takibiyle öne çıkmaktadır.[36]

Bu unsurlar; Türkiye'nin gelişmiş teknik ve operasyonel kapasitesi, geniş tecrübesi ve imkânlarıyla birleştiğinde, tamamlayıcı ve çok boyutlu bir güvenlik mimarisinin inşasına olanak tanımaktadır. Geçmiş dönemde atılan adımlar, Türk devletleri arasındaki istihbarat paylaşımının kurumsallaşma sürecine önemli bir zemin hazırlamıştır. Lider düzeyinde sahiplenilen özel servis başkanları toplantıları, gizli bilginin korunmasına yönelik ikili protokoller, ortak tehdit başlıklarında düzenlenen koordinasyon toplantıları ve kriz dönemlerinde yürütülen hızlı bilgi değişimi; bugün daha kapsamlı, standartlaştırılmış ve bütünleşik bir mekanizmanın inşasını mümkün kılacak bir kapasite yaratmıştır. Bu altyapı, bölgesel güvenlik mimarisini yalnızca ulusal çabaların toplamına dayalı dağınık bir yapı olmaktan çıkararak koordineli, senkronize ve karşılıklı bağımlılık yaratan bir nitelik kazanmasına olanak tanımaktadır.

KAYNAKÇA VE NOTLAR

KAYNAKÇA VE NOTLAR

1 Stéphane Lefebvre, The Difficulties and Dilemmas of International Intelligence Cooperation, International Journal of Intelligence and CounterIntelligence, 16(4), 2003: 527-542. Erişim Adresi: https://www.tandfonline.com/doi/abs/10.1080/716100467 [Erişim Tarihi: 04.08.2025].

2 Don Munton ve Karima Fredj, Sharing Secrets: A Game Theoretic Analysis of International Intelligence Cooperation, International Journal of Intelligence and CounterIntelligence, 26(4), 2013: 671. Erişim Adresi: https://www.tandfonline.com/doi/full/10.1080/08850607.2013.807189 [Erişim Tarihi: 04.08.2025].

3 Bk. Stéphane Lefebvre, The Difficulties and Dilemmas of International Intelligence Cooperation, s. 534.

4 United Nations Digital Library, Resolution 2396, Erişim Adresi: https://digitallibrary.un.org/record/1327675/files/S_RES_2396%282017%29-EN.pdf [Erişim Tarihi: 02.08.2025].

5 Julian Richards, Intelligence Sharing in Remote Warfare, E-International Relations, Erişim Adresi: https://www.e-ir.info/2021/02/17/intelligence-sharing-in-remote-warfare [Erişim Tarihi: 04.08.2025].

6 GCHQ, A Brief History of the UKUSA Agreement, Erişim Adresi: https://www.gchq.gov.uk/information/brief-history-of-ukusa [Erişim Tarihi: 22.07.2025].

7 Nautilus Institude, Pine Gap - An Introduction, Erişim Adresi: https://nautilus.org/publications/books/australian-forces-abroad/defence-facilities/pine-gap/pine-gap-intro/ [Erişim Tarihi: 22.07.2025].

8 TRT Avaz, Bağımsız Devletler Topluluğu Ülkelerinin İstihbarat Başkanları Bişkek'te Toplandı, Erişim Adresi: https://www.trtavaz.com.tr/haber/tur/turkistandan/bagimsiz-devletler-toplulugu-ulkelerinin-istihbarat-baskanlari-biskekte-topland/66508018f10b41c67eea57fb [Erişim Tarihi: 04.08.2025].

9 Bk. Stéphane Lefebvre, The Difficulties and Dilemmas of International Intelligence Cooperation, s. 527-542.

10 Şeniz Bilgi, Intelligence Cooperation in the European Union: An Impossible Dream?, All Azimuth: A Journal of Foreign Policy and Peace, 5(1), 2016: 66. Erişim Adresi: https://dergipark.org.tr/en/pub/allazimuth/issue/15907/167342 [Erişim Tarihi: 22.07.2025].

11 Richard Aldrich, Transatlantic Intelligence and Security Cooperation, International Affairs 80(4), 2004: 733-734.

12 Jason Dittmer, Everyday Diplomacy: UKUSA Intelligence Cooperation and Geopolitical Assemblages, Annals of the Association of American Geographers, 105(3), 2015: 611.

13 Kenneth Propp, Why Sharing Passenger Data Doesn't Fly for the EU's Top Court, Atlantic Council, Erişim Adresi: https://www.atlanticcouncil.org/blogs/new-atlanticist/why-sharing-passenger-data-doesnt-fly-for-the-eus-top-court/ [Erişim Tarihi: 22.07.2025].

14 Mehmet Çoban ve Jochem de Hopp, Challenges of Intelligence Sharing in Targeting Operations, Lieber Institute, Erişim Adresi: https://lieber.westpoint.edu/challenges-intelligence-sharing-targeting-operations/ [Erişim Tarihi: 22.07.2025].

15 Bk. Julian Richards, Intelligence Sharing in Remote Warfare.

16 Frank Foley, Countering Terrorism in Britain and France: Institutions, Norms and the Shadow of the Past, (Cambridge: Cambridge University Press, 2013), 248.

[17] BBC, NSA Spying Row: Denmark Accused of Helping US Spy on European Officials, Erişim Adresi: https://www.bbc.com/news/world-europe-57302806 [Erişim Tarihi: 22.07.2025].

[18] Paul R. Pillar, Where Polticisized Intelligence Come From, Brookings Foundation, Erişim Adresi: https://www.brookings.edu/articles/where-politicized-intelligence-comes-from/ [Erişim Tarihi: 04.08.2025].

[19] Reuters, Paris Investigates Leak Purporting to Show Egypt Misused French Intelligence, Erişim Adresi: https://www.reuters.com/business/aerospace-defense/paris-investigates-leak-purporting-show-egypt-misused-french-intelligence-2021-11-22/ [Erişim Tarihi: 22.07.2025].

[20] Artur Gruszczak, Intelligence Fusion for the European Union's Common Security and Defence Policy, Politeja, 4(79), 2022: 131-150.

[21] Nautilus Institude, Pine Gap - An Introduction, Erişim Adresi: https://nautilus.org/publications/books/australian-forces-abroad/defence-facilities/pine-gap/pine-gap-intro/ [Erişim Tarihi: 22.07.2025].

[22] Gülşen Sakarya, Türk Konseyi Ülkelerinin İstihbarat Başkanları Azerbaycan'da, Defence Turk, Erişim Adresi: https://www.defenceturk.net/turk-konseyi-ulkelerinin-istihbarat-baskanlari-azerbaycanda [Erişim Tarihi: 29.07.2025].

[23] Nazir Aliyev Tayfur, Kırgızistan Cumhurbaşkanı Caparov, Türk Dünyasının İstihbarat Başkanlarını Kabul Etti, Anadolu Ajansı, Erişim Adresi: https://www.aa.com.tr/tr/dunya/kirgizistan-cumhurbaskani-caparov-turk-dunyasinin-istihbarat-baskanlarini-kabul-etti/2645866 [Erişim Tarihi: 29.07.2025].

[24] NTV, Bakan Fidan Kazakistan'da: FETÖ İçin Atılması Gereken Adımları Konuştuk, Erişim Adresi: https://www.ntv.com.tr/dunya/bakan-fidan-kazakistanda-feto-icin-atilmasi-gereken-adimlari-konustuk,W02m1o5E7k6UvT2yaSY9oQ [Erişim Tarihi: 29.07.2025].

[25] NTV, MİT'ten FETÖ'ye Ağır Darbe: Orta Asya Sorumlusu Orhan İnandı Yakalandı, Erişim Adresi: https://www.ntv.com.tr/turkiye/mitten-fetoye-agir-darbe-orta-asya-sorumlusu-orhan-inandi-yakalandi,QA44biSW9E-4QPGOZRo-GQ [Erişim Tarihi: 29.07.2025].

[26] Tolga Özgenç, MİT Aranan FETÖ'cüyü Azerbaycan'da Yakaladı, Anadolu Ajansı, Erişim Adresi: https://www.aa.com.tr/tr/dunya/mit-aranan-fetocuyu-azerbaycanda-yakaladi/1351619 [Erişim Tarihi: 02.08.2025].

[27] Anadolu Ajansı, MİT Firari Teröristlere Nefes Aldırmıyor, Erişim Adresi: https://www.aa.com.tr/tr/turkiye/mit-firari-teroristlere-nefes-aldirmiyor/1252971 [Erişim Tarihi: 02.08.2025].

[28] Kırım Haber Ajansı, MİT, DEAŞ'ın Azerbaycan'daki Yeni Yapılanmasını Ortaya Çıkardı, Erişim Adresi: https://www.qha.com.tr/turk-dunyasi/mit-daes-in-azerbaycan-daki-yeni-yapilanmasini-ortaya-cikardi-471691 [Erişim Tarihi: 02.08.2025].

[29] Anadolu Ajansı, Hamzaçebi: FETÖ'nün Kökünü Kazımak İçin Kazakistan ile Ortak Mücadelemize Devam Ediyoruz, Erişim Adresi: https://www.aa.com.tr/tr/turkiye/hamzacebi-fetonun-kokunu-kazimak-icin-kazakistan-ile-ortak-mucadelemize-devam-ediyoruz/694492 [Erişim Tarihi: 02.08.2025].

[30] Aida Haidar, Kazakhstan and Türkiye Expand Cooperation in Military Intelligence Information Sharing, Astana Times, Erişim Adresi: https://astanatimes.com/2022/08/kazakhstan-and-turkiye-expand-cooperation-in-military-intelligence-information-sharing/ [Erişim Tarihi: 29.07.2025].

[31] Kırım Haber Ajansı, Azerbaycan ve Kazakistan İstihbarat Alanında İş Birliği Yapacak, Erişim Adresi: https://www.qha.com.tr/turk-dunyasi/azerbaycan-ve-kazakistan-istihbarat-alaninda-is-birligi-yapacak-492034 [Erişim Tarihi: 29.07.2025].

---

[32] DTX-nin "Zəfər" və "Qarabağ" Ordenli Əməkdaşlarının Sayı - Əli Nağıyev Açıqladı, Oxu.az, Erişim Adresi: https://oxu.az/siyaset/dtx-nin-zefer-ve-qarabag-ordenli-emekdaslarinin-sayi-eli-nagiyev-aciqladi [Erişim Tarihi: 02.08.2025].

[33] Central Asian Regional Information and Coordination Centre for Combating Illicit Trafficking of Narcotic Drugs, Psychotropic Substances and their Precursors - Uyuşturucu Maddeler, Psikotrop Maddeler ve Bunların Ön Maddelerinin Yasa Dışı Ticaretiyle Mücadele İçin Orta Asya Bölgesel Bilgi ve Koordinasyon Merkezi.

[34] O TSARIKS, CARICC, Erişim Adresi: https://caricc.org/index.php/tsarikts/o-tsarikts/o-tsentre Erişim Tarihi: 02.08.2025].

[35] Kyrgyzstan's Intelligence Service Detains a Suspect in Plotting Terrorist Attacks, Regional Anti-Terrorist Structure of Shanghai Cooperation Organisation, Erişim Adresi: https://ecrats.org/en/security_situation/situation/11049/ [Erişim Tarihi: 02.08.2025].

[36] Taliban and Uzbekistan Emphasize Security Cooperation, Counter-Narcotics Efforts, AMU, Erişim Adresi: https://amu.tv/187895 [Erişim Tarihi: 02.08.2025].

TÜRK DÜNYASINDA İSTİHBARAT PAYLAŞIMI:
ORTAK GÜVENLİKTE STRATEJİK FIRSATLAR

EKİM 2025