



(2)

## ABD İSTİHBARATINDA YAŞANAN DEĞİŞİMLER

Yrd. Doç. Dr. Sait YILMAZ\*

### Giriş

Dünyada istihbaratın güvenlik, dış politika, savunma, özel şirketler ve teknoloji ile dansı her gün yeni örnekler ile başımızı döndürüyor. Geçtiğimiz döneme Wikileaks, El Kaide lideri Bin Ladin'in öldürülmesi damgasını vururken, Arap Baharı adı verilen Orta Doğu ayaklanmaları ile savunma-sosyal medya-istihbarat işbirlikleri bir kez daha öne çıkıyor. Siber alanda her gün yeni bir teknolojik gelişme ile karşılaşyoruz. 11 Eylül 2001'den beri Batılı istihbarat servisleri büyük bir değişim geçirmekte, yeni güvenlik ortamına adapte olabilmek için teknolojiyi önlerine katarak yarışmaktadırlar. Görüntü ve sinyal istihbaratı için uzayda yapılan yarışa, ekonomik istihbarat alanındaki yarış eklendi. Son 50 yıldır istihbarat alanındaki reform girişimleri sadece teşkilat düzenlemeleri ile istihbarat örgütlerinin bir yere varamayacağını göstermiştir. İstihbarat reformları sadece prosedürel değişim değil, yeni durumlara kendini adapte edebilecek şekilde kültürel değişimi de gerektirmektedir. Bu makalede önce istihbarat alanında reform çalışmalarına daha sonra CIA'dan başlayarak, Amerikan istihbarat sisteminde son dönemde yapılan çalışmalara yer vereceğiz.

### İstihbarat Alanında Reformlar

Soğuk Savaş sonrası dönemde istihbaratın teknik yöntemlerle sağlanma gayreti ve insan istihbaratının (Humint) ihmal edilmesi 11 Eylül 2001'e kadar olan süreçte ciddi eksiklikler ortaya çıkardı. İstihbarat örgütleri nükleer silahlar ile ilgili teknoloji transferi, ticari istihbarat ve değişen tehdit nedeniyle devlet dışı aktörlere odaklandılar. 11 Eylül ile birlikte istihbarat analizleri ve insan istihbaratı yetenekleri konusunda eskiye dönüş başladı. Soğuk Savaş sonrası dönemi zafiyetini kapatmak için CIA 11 Eylül sonrasında Humint yeteneğini önemli ölçüde artırma gayreti içine girmiş, çeşitli savaş desteği rolleri için bölge operasyonlarına operatörler sağlamış ve Afganistan, Irak, Filipinler, Yemen, Gürcistan gibi ülkelere özel kuvvet askerleri ile birlikte görev yapacak terörle mücadele personeli görevlendirmiştir. Soğuk Savaş'ın bitimi ile Amerikan istihbaratı (başta CIA ve NSA) yeni dinleme sistemleri ve uydu teknolojilerine büyük yatırımlar yaptılar. Sinyal istihbaratı ve genelde teknik istihbarata önem verildi. İstihbarat operasyonları konusundaki kısıtlamalar bir kenara itildi. Hükümetler istihbarat servislerine daha çok kulak vermeye başladı.

Yeni istihbarat görevleri ülke güvenliğinden, ekonomi, uzay, siber-uzay, medya operasyonları ve yurt dışında diplomasiin örtülü faaliyetler ile desteklenmesine kadar geniş bir yelpazede değişmektedir. İstihbarat kabiliyetleri, fonksiyonları, politikaları ve teşkilatları değişen güvenlik ortamının gereklerine uyum sağlamalıdır. İstihbarat servislerinin her şeyden önce kültürel bir değişime, yeni durumlara kendini adapte edebilecek şekilde yeniden organize olmasına gerek vardır. Bu değişim sistemi sorgulayacak, statüko yerine alternatif gelecekler bulacak bir kadro ihtiyacı ortaya çıkarmıştır<sup>2</sup>. Bu organizasyon yapıcı eleştiriye açık ve alternatif çözümler için sorgulamayı teşvik eden bir liderliğe gereksinim duymaktadır. Prosedürel değişimler ise resmi doktrinler çerçevesinde farklı kurumların müşterek beklentilerini karşılamalı ve onların rollerini tam olarak belirlemelidir. İstihbarat

\* Yrd. Doç. Dr. Sait Yılmaz, İstanbul Aydın Üniversitesi Uluslararası İlişkiler Öğretim Üyesi, saityilmaz@aydin.edu.tr

<sup>2</sup> Deborah G. Barger: Toward A Revolution in Intelligence Affairs, Arlington/VA, (2005), 3-4.



alanında yapılacak reformlar toplayıcı ve analizci kadar, bilgi ile istihbarat arasındaki farkı ortaya koyacak bir sistem geliştirmelidir.

İstihbarat örgütleri ve büyük şirketler arasındaki ilişkiler nedeniyle gözetleme ve izleme işlerinin örtülü operasyonlar içerisindeki rolü çok daha büyümüş ve küresel bir hal almıştır. Echelon gibi küresel istihbarat gayretlerine Bilgi Teknolojileri (IT) ve internet kontrol çabaları eklenmiştir. Son iki yıl içinde ortodoks istihbarat kendi mecrasında yeni konseptlerine uyumlu teknolojiler ararken, siber güvenlik alanında ülkeler birer birer teşkilatlanmaya başlamıştır. İş dünyası istihbaratı ve özel güvenlik şirketlerinin istihbarat fonksiyonları baş döndürücü bir şekilde gelişmektedir. ABD ve Avrupa’da ortalık iş istihbaratı ile ilgili şirket kaynamaktadır. Bunlar arasında Amerikan (Kroll, Veracity Worldwide, Global, Phoenix), İngiliz (RISC, Control Risks Group, Hakluyt, DS&S, Stirling, Assynt, Quest), Fransız (Risk & Co, CEIS, Seawell), Kanada (Garda World) başta gelmektedir. İş dünyası, istihbarat dünyası ile işbirliği yapmaktadır. Ticaret görünümü endüstriyel espionaj faaliyetleri de devam etmektedir. Yüksek hızlı bankacılık işlemleri dâhilinde iş dünyası içinde diğer şirketlerin masrafları, yatırımları ve diğer mali özellikleri yakından izlenebilmektedir.

### **CIA’da neler oluyor?**

Obama döneminde CIA’ya ne isterse verildi ve dış politikanın uygulanmasında büyük güç ve geniş bir alan edindi. CIA bugün bir ölüm makinesi haline geldi, makinenin motoru “terörle mücadele merkezi”dir. Elde edilen sonuçlar harika olmaya yakın çok iyi olduğu için CIA, cehenneme gidiş için operasyonel bir alet kutusu olarak tanımlanmaktadır. Ancak terörle mücadelede yapılan iş yenilerinin ortaya çıkmasından daha fazlasını öldürmeye gayret etmektir. İnsan avı işi terörle mücadele merkezi içinde bir birime aittir ve Afganistan-Pakistan için kurulan birimden birer tane şimdi Yemen ve Somali için kurulmuştur. CIA’in Terörle Mücadele Merkezi’nde 2001 yılında 300 kişi çalışırken, 2011 yılında 2000 civarına (CIA mevcudunun %10’una) ulaşmıştır<sup>3</sup>. 11 Eylül 2001’den beri CIA önemli bir dönüşümden geçmiştir. CIA halen istihbarat toplamakta ve pek çok değişik konuda analiz yapmakta ise de görev yoğunluğu ve kaynaklarını terörle mücadeleye tahsis etmiştir. Yeni operasyonel odakta “hedefciler” kritik rol oynamaktadır. Bunlar terörle mücadele merkezi içinde özel hücreler şeklinde tutulmaktadır. CIA’nın “terörle soğuk mücadele” konsepti oldukça basittir; hedefleri bulmak ve ele geçirmek ya da öldürmek. 2004 yılından beri CIA tarafından yapılmakta olan 236 drone saldırısının 192’si Obama döneminde yapıldı.

CIA’nın etkisinin artmasında ordu ile daha fazla entegre olması etkili oldu<sup>4</sup>. CIA’nın Afganistan üzerinde uçan drone’ları Hava Kuvvetleri Harekât Merkezi tarafından izlenmektedir. Irak ve Afganistan kadar Somali ve Yemen’deki gizli savaş alanlarında CIA, ordunun özel kuvvetleri ile çok yakın çalıştı. CIA Karargâhı Yemen’deki El Kaide hedeflerini bulmak için yeni bir terörle mücadele birimi kurdu. Arap Yarımadası’ndaki karışıklıklar için CIA gizli drone pistleri inşa etmektedir. Eğer füze savaşına geçilirse bu CIA’in yeni bir askeri görevlerinin genişlemesi anlamına gelecektir. CIA, drone filolarını genişletmektedir. Drone saldırıları öyle rutin hale geldi ki yüksek düzeyli bir El Kaide lideri ölmekçe kamuoyunun dikkatini çekmemektedir. Drone saldırılarında 2000’den fazla militan ve sivil öldürüldü. CIA analizcilerinin %20’si artık drone’lar için hedef bulmakta ya da yeni eleman temini için verileri taramaktadır. Hedef bulmak CIA elemanları için bir kariyer, terfi veya ödül faktörü haline getirildi. CIA, drone programını resmen kabul

<sup>3</sup> Greg Miller and Julie Tate: CIA shifts focus to killing targets, (September 2).

<sup>4</sup> Micah Zenko: Crumbling Wall Between the Pentagon and CIA, CFR.org., (April 28, 2011).



etmemekte, kimin-kimi-nasıl (hangi yetki ile) öldürdüğünü açıklamamaktadır. CIA, denetimi olmayan bir askeri örgüte dönüşmektedir.

Drone saldırıları terörle mücadelenin sadece bir yönüdür, bunun haricinde sorgulamalar, tutuklamalar gibi pek çok operasyon yapılmaktadır. Obama yönetimi CIA'nın gizli hapishaneler sistemini bozmuş olsa da Somali dâhil pek çok ülkede şüphelileri tutuklamaya devam etmektedir. CIA ve askerler hassas hedefler için Afganistan, Irak ve Yemen'de "omega" veya "çapraz matris" adı verilen melez birimler teşkil etmişlerdir. CIA Analitik Daire çalışanlarının %35'inin işi operasyonları desteklemek iken, %10'u ülke dışında kullanılmaktadır. Kısaca artık analizciler rapor yazmıyor, olaylara öncülük ediyor. ABD, terörle mücadelede 2004 yılından beri farklı sorgulama teknikleri kullanmaya başladı. Bu teknikler Irak'a gönderilen timler tarafından denendi. Bu timlerin içinde CIA, FBI ve NSA'dan elemanlar bulunmakta idi. Irak'ta El Kaide ağının çökmesinde bu timlerin etkili olduğu düşünülmektedir. CIA'da diğer bir yenilik ise El Kaide için geliştirilen ve sorgulamalarda kullanılan yeni işkence metodudur. Suudi Arabistan, Mısır ve İsrail istihbarat örgütlerine danışılarak "su tahtası (waterboarding)" ideal yöntem olarak benimsenmiştir. CIA'nın diğer bir güç gösterisi 2009 yılında örtülü operasyonlar için onay almada Ulusal İstihbarat Direktörü'nü atlayarak Beyaz Saray ile doğrudan bir hat kurması oldu. Ayrıca CIA istasyon şefleri dış görevlerde en üst istihbarat yetkilisi konumu edindi.

### **ABD İstihbaratında Yenilikler**

ABD'nin Irak ve Afganistan'da kullandığı insansız hava araçları (İHA) sensörler, özellikle MQ-1 Predators, MQ-9 Reapers ve RQ-4 Global Hawks gittikçe uzaya dayalı verilere bağımlı hale gelmektedir<sup>5</sup>. Bunun için de geniş bir band ile veriyi alacak uydulara ihtiva eden ABD Uzay Komutanlığı'nın hazırladığı Uzaya Konuşlu Enfrared Sistemi (SBIRS) sistemi kullanılmaktadır. Uzaydaki vasıtaların takibi ABD Hava Kuvvetleri Uzay Komutanlığı sorumluluğunda olup, bilgiler NASA ve ticari sektör ile paylaşılmaktadır. Son gelişme Minyatür IV Roketi ile ilk defa bir Uzayda Konuşlu Gözetleme Uydusu'nun (SBSS) yörüngeye sokulması idi<sup>6</sup>. Akıllı İHA'ların sivil sektöre satışına başlanırken, ABD askeri araştırma kurumu DARPA ve askeri istihbaratı Drone kullanımını gittikçe çeşitlendirmektedir. İ-Phone ile de uçabilen Drone'lar; görüntü alma yanında, keşif, dünyanın çeşitli bölgelerinde (örneğin deniz korsanlarına karşı) devriye gezilmesi, TV yayını, elektronik korumalı bölgelerde güvenlik duvarının kırılması gibi pek çok yeni alanda kullanılmaya başlandı. Drone'lar ve robotları kullanabilmek için cep telefonlarını akıllı telefona dönüştüren ve böylece otomatik pilot ile temas eden yeni bir teknoloji geliştirildi<sup>7</sup>. Propaganda amaçlı Amerika'nın Sesi Radyosu (VOA) da sansür ve engellemelere karşı akıllı telefonları kullanmaya başladı.

ABD istihbarat toplumu gereksiz bilgi sistemlerinden kurtularak, personel ve donanımda büyük indirimler yapmadan bulut bilişime dönmek için çalışmaya başladı. ABD istihbarat teşkilleri bir yandan bulut bilişim'e (cloud computing<sup>8</sup>) ve akıcı bilgi teknolojisi sistemlerine geçerek daha fazla tasarruf yapılmasına katkıda bulunacaklardır<sup>9</sup>. McAfee'nin bulut önerisi güvenlik yazılımının daha otomatik dağılımını öngörmektedir. Ancak bu

<sup>5</sup> Scott Fontaine: Navigating the Crowded Corridors of Space, Defense News, (15 November 2010).

<sup>6</sup> Scott Fontaine: U.S. Begins To Improve Space Surveillance Ability, 20-Year Plan Aims To Chart Objects, Including Space Debris, Orbiting Earth, Defense News, (15 November 2010).

<sup>7</sup> İngiltere'de geliştirilen bir mini GSM anteni ile (Femtocell) mobil telefonların takibi ve dinlenmesi engellenebilir hale geldi.

<sup>8</sup> Bulut bilişim, çalıştırılan yazılımların bilgisayar yerine internet üzerinden erişime açık olan, dünyanın farklı yerlerinde bulunan sunucular üzerinden çalıştırılmasıdır.

<sup>9</sup> Marcus Weisgerber: IT Budget Savings Outlined for Intel Agencies, Defense News, (27 Oct 2011).



sistemde istediğiniz bilgi bulut'un içinde size açık olmakla birlikte başkalarına da açık olmayacağını kimse garanti edemez. ABD hükümeti gizlilik dereceli bilgilerini korumak ve Wikileaks gibi sızmaları önlemek için özel bir komite kurmaktadır. Wikileaks sonrası McAfee ile birlikte bilgilerin dışarıdan yüklenmesine yönelik tedbirler geliştirildi. Bilgi kaybı önleme teknolojisi denilen bir sistem dâhilinde hangi dokümanların kimler tarafından nasıl kullanıldığı izlemeye alındı. Ana sistem olan Müşterek Dünya Geneli İstihbarat İletişim Sistemi (JWICS) yanında her kurum için güvenlik uygulamaları getirildi. Wikileaks türü içeriden tehditlere karşı gizlilik dereceli bilgiyi gizlilik derecesi olmayan medyaya aktarılmasını yani yüklenmesini (download edilmesini) önleyecek bir sistem üzerinde çalışılmaktadır. ABD siber güvenliğini sağlamak yönünde yeni projelerden biri dışarıdan izinsiz girişleri önlemek için Lockheed Martin tarafından geliştirilen güvenlik ağı ile çift anahtar "SecurID" sistemidir<sup>10</sup>.

Ortadoğu'daki ayaklanmalarda kullanılan Facebook ve benzeri sosyal paylaşım siteleri önemli bir istihbarat kaynağı haline geldi. ABD Silahlı Kuvvetleri hedef ülkelerdeki sosyal paylaşım sistemlerine sızmak için Üniversiteler ile birkaç yıldır çeşitli modellemeler ve sızma yöntemleri üzerine çalışmaktaydı. DARPA da sosyal paylaşım sistemleri ve psikolojik savaş unsurlarının ayaklanma hareketlerinde kullanımı ile ilgili çalışmaktadır. İş dünyasında pek çok şirket çalışanlarını Facebook ve Twitter yolu ile espionaja yol açmamak için eğitmeye başladı. Gmail, Yahoo ve Skype'nin kimlik denetim sertifikalarının yakın zaman önce kaldırıldığı da ortaya çıktı. Bu sertifikalar, siber savaşın omurgasını oluşturuyor. Öte yandan savunma bütçesinin yaklaşık üçte birini Özel Askeri Şirketlere harcayan ABD'de şimdi de mantar gibi türeyen Özel Güvenlik Şirketleri yeni iş sahaları edinmektedir. Uluslararası özel güvenlik şirketleri, iş sahalarını genişletmek için insani yardım işine el attılar. NGO'lar ve yardım kuruluşlarının güvenliğini sağlama görüntüsü altında istihbarat çalışmaları yeni oluşumlar edinmektedir. Ulusal güvenlik kuruluşları yanında Savunma Bakanlığı da askeri faaliyetler ile yardım faaliyetlerini birleştiren yeni arayışlar içindedir. Bazı özel güvenlik şirketleri ise korsanlarla mücadele konsepti (Marque System) dâhilinde yeniden teşkilatlanmaktadır.

### **ABD İstihbarat Örgütleri**

ABD'de 16 istihbarat teşkilatının 12'si askerlere aittir ve toplam istihbaratın %80'ini askerler kullanır. Amerikan askeri istihbarat teşkillerinin babası olan Savunma İstihbaratı Ajansı (DIA), bilgi teknolojileri kapsamında kendisi ile çalışacak 11 şirketten oluşan bir havuz oluşturdu. Amerikan askeri istihbaratının son marifeti ise yeraltı GPS'nin geliştirilmesidir. ABD İstihbarat Toplumu Araştırma Merkezi (IARPA), analizcilerin düşünme süreçleri ile ilgili bir model geliştirmek için çalışmaktadır. Amerika'nın üst üste yaşadığı doğal felaketler meteoroloji istihbaratına daha çok önem verilmesine neden oldu. Amerikan istihbarat toplumu küresel ısınma (kıtık, seller vb.) konuların ABD güvenliğine etkileri üzerine çalışmaya başladılar. Amerikan istihbaratının diğer bir araştırma projesi ise güven sağlamak için nörolojik mekanizmalar. Amerikan ordusu sürekli teçhizatını yenilemektedir. ABD, 2011 yılı içinde taktik muhabere ağını geliştirmekte olan en son yazılım ve akıllı telefonlar ihtiva eden yeni bir cihaz teknolojisi ile test etti. Birlik komutanlarının savaş alanında kullanmak istediği Apple, Droid Google ve RIM BlackBerry gibi akıllı telefonların güvenli olduğu test edildi. McAfee, şebekelerden bütün cihazlara güvenli geçme imkânı sağlamaktadır. Kablosuz şebeke için kriptolu Apple iPhone tercih edilmiştir. Bu

<sup>10</sup> Scott Jasper: Protect Global Commons, Leverage Integrated Domain of Cyberspace, Defense News, (19 June 2011).



cihazı kaybettiğinizde onu kilitleyebilir, yerini tespit edebilir ya da kriptosunu bozabilirsiniz<sup>11</sup>.

11 Eylül öncesi önemli olayları önceden haber veremeyen ABD istihbaratının zayıflığının temelinde dil bilen personel ve analizci eksikliği yatmakta idi<sup>12</sup>. Bugün ABD istihbarat teşkilatları gittikçe uzman merkezli hale gelmektedir<sup>13</sup>. 4 yıl önce kurulan istihbarat toplumu uzun dönemli strateji grubu Quad (DIA, NGIA, NRO ve NSA) işbirliğini artırmayı ve gereksiz tekrarları önlemeyi amaçlıyordu. Bu gruba katılmaya yakın zamana kadar gönülsüz olan CIA'in de katılması ile grubun adı "the Quint," olarak değiştirildi<sup>14</sup>. 11 Eylül 2001 sonrası kurulan Ulusal İstihbarat Direktörlüğü dâhilinde 2.600 analist çalışmakta, bunlar 56 istasyon halinde sahada yer almaktadır. CIA, Mart 2009'dan itibaren ekonomik istihbarat brifinglerine başladı. ABD'ye yönelik yakın zamanda espionaj faaliyetlerinin başında 'temiz kömür' gelmektedir. Ulusal Keşif Ofisi (NRO) 2011'in ilk döneminde uzaya altı uydu gönderdi. NRO, işlettiği uydular ile Usame Bin Ladin'e yapılan operasyon, Libya'da NATO ve isyancı güçlere yardım gibi pek çok işe yaradı. Yer istasyonu Denver dışındaki Buckley Hava Üssü olan NRO tarafından geliştirilen Kırmızı Nokta (Red Dot) program dost birliklere hazırlıksız atılan bombaları bulmaya amaçlıyor. Bu teknoloji aynı zamanda sinyal takibi yolu ile Taliban unsurlarının yerini tespit edilmesinde de kullanılıyor.

İstihbarat servislerinin bütçesi geçmiş yıllar itibarı ile sürekli artan bir eğilim izlemektedir. ABD Kongresi, 2011 yılı sivil ve askeri istihbarat faaliyetleri için bütçede 2010 yılına göre küçük (1.8 milyar dolar) bir düşüşle 78.6 milyar dolar olarak belirledi. Bu paranın 54.6 milyar doları sivil istihbarat programları, 24 milyar doları askeri istihbarat faaliyetleri için harcandı<sup>15</sup>. Bununla beraber, istihbarat servisleri hem sivil hem de askeri istihbarat programları yürüttüğünden bu farkı tespit etmek kolay değildir. Amerikan istihbarat servislerinin 2012 bütçesi 80 milyar dolar olarak belirlendi<sup>16</sup>. Yeni kanunla görevde ilen ölen CIA mensupları için cenaze masraflarının karşılanması ve ölenlerin ailesine yardım imkânı sağlanmaktadır. Ekim 2010 itibarı ile ABD'nin siber güvenlik alanındaki ana komuta-kontrol birimi tam operasyonel hale geldi. Bu birimde siber güvenlik alanında potansiyel tehditler için gerekli operasyonel resim ortaya konarak proaktif tedbirler alınmaktadır. Siber Komutanlığı içinde 2.900 subay ve 27.000 diğer personel bulunmaktadır<sup>17</sup>. Bu birim elemanları timler halinde Afganistan'da da kullanılmaktadır. Siber Komutanlığın kurulmasından sonra FBI da 1000'den fazla ajanını dijital iz sürme ve analiz konusunda eğitti.

### **Sonuç Yerine**

Sosyal istikrarsızlıklar, ekonomik krizler, çevre sorunları, insan hayatını tehdit eden felaketler gibi uluslararası güvenlik konuları istihbarat teşkillerinin diğer hükümetler ve

<sup>11</sup> Ben Iannotta: Company Profile, Dave DeWalt, President and CEO, McAfee, Defense News, (23 January 2011).

<sup>12</sup> George Friedman, America's Secret War: Inside the Hidden Worldwide Struggle Between America and Its Enemies (New York: Random House, 2004).

<sup>13</sup> Matthew Frankel: A Response to Ken Lieberthal's Report on the Intelligence Community, The Brookings Institution, (October 19, 2009).

<sup>14</sup> Ben Iannotta: U.S. Intel Director Outlines Budget Strategy, Defense News, (17 Oct 2011).

<sup>15</sup> Marcus Weisgerber: Slight Drop in U.S. Funding for Intel Programs, (28 Oct 2011). <http://www.defensenews.com/story.php?i=8084917&c=AME&s=TOP>

<sup>16</sup> Donna Cassata: House passes intelligence bill for next year, Associated Press, (Friday Sep 9, 2011).

<sup>17</sup> Scott Fontaine: New USAF Cyber Unit Grapples With Data Overload, Defense News, (15 November 2010).



hükümet dışı aktörlerle bir arada çalışmasını dikte etmektedir. Bunun anlamı ise istihbarat teşkillерinin süratle değişen güvenlik ortamlarına adapte olmaya hazır olmaları gereğidir. 21. yüzyıl teknolojinin getirdiğı imkânlar vasıtası ile gözetleme, izleme ve dinleme çağı olacaktır. Bununla beraber dünyadaki istihbarat örgütleri içinde eski moda engelleyici tipte olanlar (Çin, İsrail ve Türkiye örnek verilebilir) hala çoğunluktadır. İstihbarat artık büyük ölçüde istihbarat servislerinin işi olmaktan çıktığından siyasi, ekonomik ve teknik istihbarat kabiliyetlerini artırmak için akademik çevreler, özel sektör ve araştırma kurumları ile daha çok işbirliği yapmak zorundadırlar. Jeostratejik olarak Orta Doğu'daki önemli kırılma noktalarının arasında bulunan Türkiye'nin istihbaratı artık kısır teşkilat düzenlemelerinin ötesinde kendini kültürel ve teknolojik olarak da yenilemek zorundadır. Öncelik uzaya dayalı kabiliyetlere ve özellikle terörle mücadelede askeri istihbarata verilmelidir. Bunun için de her şeyden önce istihbarat kültürümüz değişmelidir.