

21. Yüzyılda İstihbarat

Prof.Dr.Sait Yılmaz

21. Yüzyılda İstihbaratın Deęişen Paradigmaları

Tarihçilere göre 20. yüzyıl “istihbarat yüzyılı” idi. Birçok devlet istihbarat için resmi kurumlar teşkil ettiler ve birbirilerine karşı casusluk yaptılar. Yüzyılın sonunda Batılı ülkeler istihbarat teşkilatlarını yeniden düzenleyerek, kamu denetimine açtılar, diğer ülkelere irtibat personeli gönderdiler. 20. yüzyıl teknolojisi bize istihbarat vasıtası olarak telsiz, radar, katı halli elektronikler, uydular, bilgisayar ve internet kazandırdı. Son yıllarda buna açık kaynak istihbaratı için yeni arama motorları ve semantik web eklendi. Uluslararası istihbarat yöntem ve vasıtaları sürekli gelişmektedir. Önümüzde biyo-bilimsel devrimler var ve insan benzeri makinelerin harekât ortamında yer alması ve istihbaratçının yerine bilgiyi füzyon etmesi bekleniyor. Gerçek istihbarat, gelecek hakkındadır ve ilerideki bir zamanda ne olacağı ile ilgilidir¹. Geleceğin istihbaratında sadece kurumlar ve yöntemler değil, özel ve bürokratik karakterdeki konseptler de değişecektir. İstihbaratın çok daha kullanılması ve entegre edilmesi ile istihbarat yayılması yaşanacak ama aynı zamanda artan ölçüde farklı, caydırıcı ve tanımlanması zor hale gelecektir. İstihbarat hem yaygınlaşacak hem de dönüşüme uğrayacak, yapılanların istihbarat çalışması olduğunu söylemek zorlaşacaktır. Geleceğin daha belirsiz ve karmaşık güvenlik ortamı içinde bir istihbarat teorisi geliştirmek daha zor olacaktır.

Artan bilgi akışı, istihbarat örgütlerini aşırı yükleme nedeniyle bunaltmaya başlamıştır². Bilgi teknolojisinin böyle durumlarda karar verme sürecini basitleştirmeyeceği, gerçekte daha da karışık hale getireceği oldukça açıktır. Dünyanın gittikçe belirsiz bir güç mücadelesine girmesi ve düşük yoğunluklu çatışmaların değişik boyutları eylemlerde ve çatışmalarda ileri teknolojiye sahip silahların kullanılmasını teşvik edecek ve kitlesel ölümler yaşanabilecektir. İletişim teknolojisindeki gelişmeler; ekonomik avantajların yer değiştirmesi, insanların artan dolaşımı ve terörist ağların genişlemesi; toplumsal kırılmaların kolaylaşması, iletişim teknolojilerine bağımlı ülkelerin artan hassasiyeti, daha zor ve çok hedef, hedefe nüfus etmeye daha çok ihtiyaç, daha gelişmiş savaş sistemleri ve anında geri besleme ihtiyacı gibi sonuçlar doğuracaktır. İstihbaratın geleceği ile ilgili şu genel beklentileri yapabiliriz³;

- Ulusal istihbarat paradigması zamanla geçersiz hale gelecek, değişikliklere uyum sağlamak için reform yapmak yeterli olmayacak, yeni istihbarat kurumları ve sistemleri gerekecektir.
- İstihbarat çalışmalarında yeni uzmanlık ve anlama alanları ortaya çıkacak.
- Bugün kullanılan bazı önemli kaynaklar ve yöntemler önemini kaybedecektir.
- İstihbarat üretimi ve temininde yeni aktörler ortaya çıkacaktır.
- Rekabetçi anlama ortamının doğması ile entelektüel tekel olmayacaktır.

¹ Robert M Clarck, Intelligence Analysis, A Target-Centric Approach, CQ Press, (Washington DC, 2007), 172.

² Harp Akademileri Komutanlığı, Geçmişte ve 21 nci Yüzyılda Savaşlar, Stratejiler ve Stratejiler, (Yenilevent-İstanbul, 2002), 184.

³ Wilhelm Agrell, The Next 100 Years? Reflections on the Future of Intelligence, in Isabelle Duyvesteyn, Ben de Jong, Joop van Reijn: The Future of Intelligence Challenges in the 21 st Century, Routledge, (New York, 2014), 144-145.

- Bilginin kırılğan dünyası güvenirlige verilen önemi artıracaktır.

İletişim ve ulaşım teknolojisinin ve yöntemlerinin yaşamı daha da etkisi altına alacağı 21. yüzyılda, propaganda ve psikolojik savaş en önemli güvenlik-tehdit yöntemi olarak karşımıza çıkmaktadır. Hâkim güçler, kendi çıkarlarına tehdit olan unsurları belirleyip, bu temelde ürettikleri güvenlik ve tehdit tezlerini diğer aktörlere benimsetebildikleri ölçüde hegemonyalarını kurup sürdüreceklendir. Ekonomik, siyasal, askeri gücün etkisini artıran güç çarpanı propaganda ve psikolojik savaştır. Propaganda ve psikolojik savaş yolu ile hedef ülkeler, toplumlar ya da gruplar kendilerine yöneltilen tehdit tezlerine sanki kendilerinin güvenliklerini, çıkarlarını sağlıyormuşçasına sahip çıkmakta ve bu tür politikalara “rıza” gösterebilmektedirler. Ya da hâkim güçlerin ulusal politikaları erozyona uğratma girişimleri ve örtülü operasyonlarına karşı duran güçler, yine ulusal düzeyde psikolojik savaşın çeşitli yollarla kullanılmasıyla yıpratılmaya çalışılmaktadır. Aç gözlülük, paranoya, fanatizm ve rekabet sonucu ortaya çıkan düzensizlikler ulus-devlet yapılarını istismara açık hale getirmektedir. Saldırgan istihbarat fonksiyonları medya ve haber kaynakları yanında iletişim ve ulaşım vasıtalarını da hedef almaktadır. Örtülü teşkillerin varlığı demokrasiye zarar verir ve kanunların değil, kişilerin yönettiği bir devlet oluşmasına neden olur.

Soğuk Savaş sonrası yoğunluğunu yitirmiş gibi görünen örtülü faaliyetler de küresel güç mücadelesi veren devletlerin istihbarat servisleri için önemli bir argüman olarak etkinliğini arttırmaktadır. Örtülü faaliyetler, Soğuk Savaş sonrası belirli devletlere karşı, “demokrasi” ve “devlet inşası” gibi özel operasyonlarda kullanılmak üzere yeni yöntemlerle icra edilmektedir. Örtülü operasyonların gelecekte de dış politikanın temelini oluşturmasının dört temel sebebi vardır⁴.

(1) Hala güvenlik ortamında pek çok düşman, tehdit ve çözülmeyi bekleyen sorun bulunmaktadır.

(2) Kurulan örtülü bürokrasiler kendilerine yeni roller bularak var olmaya devam edecektir.

(3) Örtülü operasyonlar geçmişteki nedenlerden dolayı yönetimlere çekici bir seçenek oluşturmaya devam edecektir.

(4) Soğuk Savaş sonrası güvenlik ortamı örtülü operasyonlar için yeni olanaklar ve hedefler sunmaktadır. 11 Eylül 2001 sonrasında örtülü faaliyetler özellikle terörizmle mücadele alanında odaklandı.

Ekonomik istihbarat alanında en önemli görev istihbarat servislerine düşmektedir. İstihbarat çarkının ekonomik istihbarat için de uygulanması, özel sektörle işbirliği ve karşı istihbarat faaliyetleri ekonomik istihbarat alanında istihbarat servislerinin görevlerindedir. Ekonomik istihbarat alanında bir devletin alması gereken en önemli tedbir; bir ekonomik istihbarat sistemi teşkil etmektir. Daha sonra kendisine yönelen ekonomik istihbarat faaliyetlerine karşı saldırgan bir ekonomik istihbarat politikası belirlemelidir. Bunu sağlamak için, ekonomik ve endüstriyel istihbarat faaliyetlerinde bulunan devletlere karşı özellikle ekonomik ve ticari yaptırımların uygulanması ve uluslararası alanda ikili ve çoklu antlaşmalarla ekonomik casusluğun karşılıklı olarak yürütülmemesine dair taahhüt altına girilmesi gibi girişimlerde bulunabilir.

⁴ John Jacob Nutter, CIA'nın Karanlık Operasyonları: Örtülü Operasyonlar, Dış Politika ve Demokrasi, Güncel Yayıncılık, Çev.: Ahmet SARAÇOĞLU, (İstanbul, 2005), 497-498.

Teknoloji ve İstihbarat

1920'lerden itibaren hava araçlarında yaşanan teknolojik gelişmeler nedeni ile Soğuk Savaş boyunca ve hatta 11 Eylül 2001'e kadar güvenlik uzmanlarının genel anlayışı 'havaya hâkim olmak' üzerine olmuştur. Bilgi devrimi ile yaşananlar bu anlayışı tekâmül ettirdi çünkü artan bir şekilde "bilgi ve istihbarat" konuşuyoruz. 21. yüzyılın savaşları politika ve güç, ticaret ve endüstri, sanat ve kültür, bilim ve teknoloji gibi alanlarda internet üzerinden bilgi için yapılacaktır. Dünyada yeni çatışmalar artık Doğu-Batı veya Kuzey-Güney etkisinde kalmayacak, hızlı ve yavaş ülkeler arasında olacaktır. Savaşlarda insanın yerini robotlar alacak, siber savaşlar ile ülkelerin güç kaynakları kesilecek, savaşın boyutları ve sınırları sonsuz hale gelecektir. Başta uydu sistemleri olmak üzere teknolojinin kullanımı, özel olarak ise ekonomik istihbarat çok daha önemli hale gelmiştir. Rakiplerimiz karşısında üstünlüğü belirleyen artık yeni teknolojiler ile istihbaratı toplamak, geliştirmek, analiz etmek ve dağıtmak konusundaki yeteneklerimiz oluşturacak. Rakiplerimize üstünlük sağlamak için birleşik ve adrese özel bir istihbarat sistemi geliştirmeliyiz. Savunma stratejileri için gerekli olan; uzaktan kontrol sistemleri, uzun menzilli isabetli vuruş kabiliyetleri, manevra ve sefer kuvvetlerindeki değişimin istihbarat kabiliyetlerindeki yenilikler ile tamamlanmasıdır. Bilim ve teknolojinin sağladığı istihbarat üstünlüğü daha kısa karar süreçlerini ve istihbarat ile operasyon arasında daha sıkı işbirliğini ve reaksiyon zamanlamalarına odaklanmayı gerektirmektedir.

21. yüzyıl, teknolojinin getirdiği imkânlar vasıtası ile gözetleme, izleme ve dinleme çağı olacaktır. Potansiyel olarak rakip olan ülke ve kurumlar, bilgiye bağımlı kalmadan kendilerine uyan teknolojileri üretme yarışına gireceklerdir. Teknoloji istihbarat toplama vasıtalarının etkinliğini artıracak, özellikle uzaya dayalı, elektronik görüntü ve dinleme istihbarat vasıtaları alanındaki teknolojik üstünlük güvenlik alanında önemli bir kuvvet çarpanı haline gelecektir. Uzaya yayılan her sinyal birileri tarafından dinlenilebilmektedir. Uzaya dayalı kabiliyetlerde önemli gelişmeler olacak ve yüksek çözünürlüklü görüntü temini daha düşük maliyetlerle sağlanacaktır⁵. Teknolojik gelişmeler neticesinde gizlilik kavramı boyut değiştirmiş ve gizli bilgilere nüfuz etme kolaylaşmıştır. Hızlı reaksiyon gösterebilmek için daha esnek istihbarat kabiliyetlerine ihtiyaç duyulacaktır. Teknolojideki gelişmeler öncelikle hedef tespit imkânlarının gelişimi ile örtülü operasyonların etkinliğine önemli bir katkı sağlayacak; cezalandırma, suikast, sabotaj, arama-kurtarma gibi operasyonlara teknolojinin sağladığı imkânlar ile daha sık başvurulacaktır. GPS veya bunun devamı olan uydu yönlendirme aletleri ve uydu iletişimi birçok ülke tarafından kullanılmaya başlanacaktır. Öte yandan, medya ve internet gibi küresel iletişim vasıtalarının yaygınlaşması, bu alanda yapılan yeni çalışmalar; psikolojik harekat için yeni vasıta ve yöntemlerin ortaya çıkmasını sağlayacaktır.

Teknoloji, sadece güç katan bir araçtır ve ne kadar ilerlerse ilerlesin insan, gelecekteki hayatın en önemli unsuru olmaya devam edecektir. İleri teknolojik istihbarat kullanımlarının, araçları da sonuçları da yöntemleri de hala çok açık değildir. Çoğu kez kullanılan yöntem ve araçlardan ziyade, ortaya çıkan olaylar eliyle yaratılan sansasyonlar arka odalardaki çalışmalarını gizlemektedir. Elektronik ortamda her şey dinlenir veya okunur, bunlar manyetik bantlara kaydedilir ve buradan da tercüme, analiz ve kıymetlendirme için ilgili merkeze gönderilir. Bu işleminden sonra

⁵ Zalmaid Khalilzad, Ian O. Lesser, O. Sources of Conflict in the 21st Century: Regional Futures and U.S. Strategy, (Washington D.C., 1998), 21. Public Eye, Scientific American, (August 1996), 18. Charles Lane, The Satellite Revolution, The New Republic, Vol.215, No.7, (August 12, 1996), 22.

tekrar ama farklı disklerle depolanır, özetleri ve indeksleri çıkarılarak karar merciine ulaştırılır. Bu da bilgisayar ve iletişim teknolojisi demektir. Bu bilgisayar sistemlerinin içeriği, güçleri, uyumlulukları, esneklikleri ve dahası uydular gibi iletişim ağı bağlantıları teknik istihbaratın bir parçasıdır. Diğer teknolojik (biyoteknoloji, biyometri, mikroelektronik, nanoteknoloji ve materyal teknolojisi) gelişmelerin ise; DNA, kan ve genetik analizlerinde gelişme, toplum sağlığına zarar veren maddeleri tespit edecek yeni sensörler bulunması, espionaj ve siber suçlarda artış, nanoteknoloji ile ürün dizaynında değişim gibi güvenlik kapsamlı sonuçlar yaratabileceği değerlendirilmektedir. Askeri teknolojideki gelişmelerin ise özellikle sensör ağı ile vuruş kabiliyetinin artması, istihbarat ve harekât arasında daha yakın ilişki gibi gelişmeler sağlaması beklenmektedir. Uzun vadede istihbarat anlayışını değiştirecek önemli teknolojik beklentiler şunlardır⁶;

- 2030'da 90 milyar alet internete bağlı olacak, her şey birbirine irtibatlanacak, internetten çıkmak suç olacaktır. Bugünkü ikinci nesil polislerin yerini elektronik olarak her ortamı izleyen ve kayıt altına alan, robotlar vasıtası ile suç mahalline müdahale eden polis sistemi alacaktır.

- 2040'lardan itibaren beyine yerleştirilen çipler ile suçlular izlenecek, insanlar sadece işlediği değil işleyeceği suçlar için de tutuklanacaktır.

- 2050'den itibaren DNA bilgi bankaları ile insanın evrimi kontrol altına alınacak, biyokrimonoloji çalışmaları ile insanları suç işlemeye iten nedenlere önlem getirilecektir.

- Nükleer devletler ve nükleer malzemelerin terörist maksatlar ile kullanımını gittikçe artacak, 2060'da dünyadaki devletlerin %25'inin açık ya da gizli nükleer programları olacak, 2080'de nükleer silahların yerini daha örtülü kitle imha silahları alacaktır.

- Bütün insanlığı tehdit eden en önemli olgulardan biri iklim değişikliği ve beraberinde getirdiği küresel ısınma, ozon delinmesi, çölleşme ve ormanların yok olması, büyük göçler, içilebilir su kaynaklarının azalması gibi çevre sorunları olacaktır.

Siber & Açık İstihbarat

Önceki yüzyıllardaki toprak, demir, petrolün yerine, 21. yüzyılın stratejik kaynağı satabileceğimiz, saklayabileceğimiz ve hala elimizde tutabileceğimiz "bilgi" olacaktır. Bilgi; zenginlik ve güç, başkalarının hayatlarını kontrol, sürpriz saldırgan yöntemler için kullanılacaktır. Bilgisayarlar, bilgi ağları ve uydular artan bir şekilde, endüstri üretimini ve modern silah teknolojisini belirleyecektir⁷. Siber yollardan ekonomik casusluk istihbaratta öncelik kazanacaktır. NSA'nın açık olarak sadece tüm Amerikalıların değil, tüm dünyanın dijital yaşamlarına direkt erişimi olduğu açıktır. İstihbaratçıların işini sokaklardan masa başlarına taşıyan daha çok bilgisayar teknolojisindeki gelişmeler olmuştur. Dönem artık bilgisayarlarla casusluk dönemidir. Apple, Google, Facebook, Twitter, MSN şirketleri ABD'dedir ve uzun zamandır ABD istihbaratı ile işbirliği yapmakta, sizin hakkınızda hiçbir yasal temeli olmadan özel bilgilerinize ulaşım sağlamaktadırlar. Bunu da terör ya da çocuk pornosu ile mücadele gibi insani gözükken nedenler kisvesi altında yapmaktalar. Dijitalleşmenin güvenliğe iki önemli etkisi; mesafelerin yok olması ve özel bilgilerin ortadan kalkması,

⁶ Sait Yılmaz, 2070 Sonrası Dünya; İnsan 2.0, Academia.edu, (22 Nisan 2015).

⁷ Alvin ve Heidi Tofler, 21. Yüzyılın Şafağında Savaş ve Savaş Karşıtı Mücadele. Çev.Mehmet Harmancı, Sabah Kitapları, (İstanbul, 1994), 181.

elektronik ortamda her türlü bilginin edinilebilmesi ya da çalınabilmesidir. Bugün terörle mücadele yasası maskesi altında banka işlemlerimiz, alışverişlerimiz, internette gezdiğimiz sayfalar, sohbetlerimiz, sağlık durumumuz, seyahatlerimiz, telefon konuşlarımız kaydediliyor, izleniyor. Yeni casus yazılımları ile telefonunuz uzaktan kontrol ile açılabilmekte, kapalı olsa bile bilgisayarınızın kamerası ve mikrofonu ile haberiniz olmadan konuşmalarınız kaydedilmekte, resimleriniz ya da videonuz çekilmektedir. OnStar sistemi dâhilinde arabanıza yerleştirilen mikrofonlar ile konuşmalarınız takip edilmektedir.

Yazılım programları ile klavyenizdeki vuruşlar takip edilerek şifreleriniz ve diğer özel bilgileriniz kaydedilmektedir. İnternetteki hareketleriniz, kullandığınız telefonlar uzun zamandır izleniyor olabilir ya da en azından istendiği zaman konuşma arşivinize girilebilir. PRISM programı sürekli genişliyor, Hotmail veya Google gibi servislerdeki hesaplarınız kontrol altındadır. Eğer Apple, Google veya Microsoft üzerinden izleniyorsanız, takip edilmekten kaçınmanın en iyi yolu akıllı telefonlardan kurtulmaktır. Yakın gelecekte kara kutuların arabalara da konulması zorunlu olacak, halka açık yerlerde detektör kullanılacak, milyarlarca kamera her açıdan sizleri izleyecek, dünya genelinde DNA örnekleriniz tutulacak, özel hayat bitecektir. Önce, bilgisayarlarda klavye, maus kalkacak, doğrudan beyin-makine etkileşimi sağlanacak, bu gelişme beyin kontrolünde de kullanılacaktır. Her şeyiniz internette kayıt altında olacak, çorabınızın bile IP no.su olduğundan dolapta hangi renkte kaç çorap kaldığını izleyebileceksiniz, herkes de sizin tam kimliğinizi, yerinizi ve statünüzü gerçek zamanlı olarak takip edebilecektir. Güvenlik olmadan özgürlük tehlikelere açıktır ama özgürlük olmadan güvenlik ise baskı rejimidir. Snowden ifşaatları ortaya çıkınca, ABD istihbaratının en büyük üzüntüsü insanları yasal olmayan izleme yöntemlerinin ortaya çıkması değil, bu yöntemlerin öğrenilmesi nedeni ile hedef kişilerin davranışlarını değiştirmesi olmuştu. Yakın bir gelecekte arkamızda dijital bir iz bırakmadan çalışmamız, seyahat etmemiz, haberleşmemiz mümkün olmayacaktır.

Açık kaynak istihbaratının önemi önümüzdeki yıllarda artarak devam edecektir. Örneğin 'amazon.com' da bir tık ile ulaşamayacağınız akademik kaynak kalmadı⁸. İstihbarat servislerindeki sürekli bilgi akışı, toplanan verilerin tamamının analiz edilememesi bir tür 'analiz felci'ne yol açmıştır. Yeni dönemin istihbarat faaliyeti; elektrik süpürgesi gibi hiçbir ayırım yapmadan her şeyi toplamak yerine, isteğe göre bilgi toplamak ya da analizleri seçerek yapmak olmalıdır. Bununla beraber açık istihbaratın 'çok gizli' dünyasına pek fazla katkısı yoktur. Özellikle internet yolu ile sağlanan açık kaynak bilgileri giderek daha yoğun hale gelirken istihbarat toplayıcıları aşırı yükten ziyade işe yarar bilginin azlığından şikâyet edeceklerdir⁹. Bilgi teknolojilerinin gelişmesi açık istihbaratın önünü açmaktadır. Bir süre sonra parası olan özel kişiler veya şirketler, devletlerin kullandığı bazı teknik istihbarat süreçlerini kullanmaya başlayacaklardır. Hatta bazı şirketler uydu istihbaratının sağladığı görüntülerden faydalanmaya başlamışlardır. Bu süreç istihbarat toplama ve analiz için merkezi olmayan, yatay yapılanmaları da beraberinde getirmiştir ve eğilim bu yönde artacaktır.

İstihbarat Servisleri

⁸ Stephen C. Mercado, Sailing the Sea of OSINT in the Information Age, Studies in Intelligence, Vol.48, No.3, (2004). <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article05.html>

⁹ James R. Clapper, How 9/11 Transformed The U.S. Intelligence Community, Wall Street Journal, (7 September, 2011).

İstihbarat artık sadece istihbarat teşkilatlarının oyun alanı olmaktan çıkmakta, çeşitli özel, kamu, kolektif ve ticari ajanlar artan ölçüde alana dahil olmaktadır. İstihbarat teşkilatları bilgi toplama servisi olmaktan 'anlama doğrulama (teyit)' ve anlama (knowledge) yönetimi örgütlerine dönüşebilir. Yeni dönemde istihbarat servisleri sadece bilgi toplayan ve analiz eden statik konumundan çıkarak, sorunlu ülkelerde demokrasi ve hukuk kurallarının tesisi ve geliştirilmesi konularında aktif roller alan dinamik bir yapıya kavuşacaktır. Eski istihbarat organizasyonları; çok büyük boyutlu, merkezi ve çok gizlilik yanlıydılar. Bu tür organizasyonların, ekonomide olduğu gibi istihbaratta da modaları geçmiştir. Tıpkı büyük şirketler gibi istihbarat dünyasının kurumları da temel görev ve fonksiyonlarını sorgulamak zorunda kalmışlardır. Güvenlik pazarı harekete geçip genişledikçe yeni ortaya çıkan sorunları çözümlmek için yeni ürünler gerekecektir¹⁰.

21. yüzyılın operasyonları için istihbarat profesyonelleri, pratik ama yenilikçi, hızlı ama karara etki edecek kalitede bilgi temin edecek bir sistem geliştirmelidir. Yenilikçilik ve yaratıcılığın öne çıkacağı bu yapılar, yeni durumlara süratle adapte olacak, kısa sürdüğü oluşturduğu timlerle teşkilat içi ve dışı tüm tecrübe ve yeteneği kullanacaktır. Bu, 20. yüzyılın sonunda barış zamanında bir hükümetin uzun zamanda başardığı bir işi, yeni yapının savaşta çok kısa sürede başarması anlamına gelmektedir¹¹. İstihbarat, bir silah sistemi gibi olmalı; kaynaklar gerektiğinde bir araya getirilmeli, manevra yapmalı, geleneksel ve kinetik sistemlere adapte olabilmelidir. Bu yüzden yenilikçi ve cesur düşünme gereklidir. Bütün bunlar yapılırken karmaşık ve belirsiz operasyon alanında bilgiyi ayırt etmek, korumak ve kontrol etmenin önemi de unutulmamalıdır. İstihbaratçıların yapması gereken bir kez daha yeni güvenlik ortamının şartlarına ve ihtiyaçlarına adapte olmak, yeni durumun gerektirdiği düşünsel ve yapısal değişimleri gerçekleştirmektir. Yani modası geçmiş ile adapte olunması gereken arasında mantıklı tercihler yapmaktır. Bu yapılmadığı takdirde önce ortamın kontrolünü kaybedersiniz nihayetinde onlar sizi kontrol etmeye başlar. Sınırsız sayıda rakibin olduğu, çalkantılı ortamın karmaşıklığı istihbarat örgütünün de karmaşık bir yapıda olmasına neden olacaktır. Yeni güvenlik ortamında istihbarat örgütleri daha akıcı ve yatay olmak zorundadır. Yeni görevler ve karmaşıklığın getirdiği iş yükü bürokratik engellerin azaltılmadığı takdirde işleri daha da çıkmaza sokacaktır. Yapılan işlerin stratejik önemi bazen mikro yönetim isteyen işlerin en tepeden gerçek zamanlı takibini gerektirebilir. Bu örneğin terör örgütü liderine yapılan baskının veya insansız hava aracı ile bir hedefin vurulmasının etkilerinin görülmesi için Ulusal Durum Merkezi'nde en üst düzey devlet liderlerinin durumu takibi şeklinde olabilir.

İstihbarat örgütleri sürekli bir değişim ve arayış içinde bir yandan yeni teknolojilere adapte olurken, diğer yandan yeni yüzler edinmektedirler. İstihbarat servisleri 'kimleri izlemekle yükümlüüz' sorusunun cevabını aramaktadır. Dolayısıyla, Soğuk Savaş sonrası ortaya çıkan çeşitli jeopolitik teoriler bu gözlükte bakıldığında istihbarat açısından anlam kazanacaktır. Yeni istihbarat görevleri ülke güvenliğinden, ekonomi, uzay, siber-uzay, medya operasyonları ve yurt dışında diplomasinin 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

¹⁰ Toffler, a.g.e., (1994), 153.

¹¹ Gregory F. Treverton, The Future of Intelligence Changing Threats, Evolving Methods, in Isabelle Duyvesteyn, Ben de Jong, Joop van Reijn: The Future of Intelligence Challenges in the 21 st Century, Routledge, (New York, 2014), 25.

önce kültürel bir değişime, yeni durumlara kendini adapte edebilecek şekilde yeniden organize olmalarına gerek vardır. Bu değişim, sistemi sorgulayacak, statüko yerine alternatif gelecekler bulacak bir kadro ihtiyacı ortaya çıkarmıştır¹². Öncelik yelpazesinin genişliği istihbarat servisleri içinde uzmanlaşmayı ve dışarıdan tedarik usullerini de beraberinde getirmiştir. Güç, gittikçe devlet dışı aktörlere (NGOs, terör örgütleri vb.) kaymaktadır.

İstihbarat servislerinin teşkilat yapılarının gözden geçirilmesi gereklidir. Pek çok ülke kendi içinde güçlü gelenekleri, kadroları ve sadakatleri olan farklı istihbarat örgütlerine sahiptir. Bunlar kendi dünyalarından kendi çözümlerini geliştirdiler. Bunu yaparken bazen bürokrasi ve siyasi nedenlerle uyarmak istediklerinden daha kötü sonuçlar doğurdular. Bugün ise örgütler arası uyum için yatay bilgi kullanıcıları dönemindeyiz. 11 Eylül sonrası gelişmeler istihbaratın dört fonksiyonunu ön plana çıkardı¹³; dış istihbarat, örtülü faaliyet, karşı istihbarat ve iç istihbarat. İç ve dış tehditler arasındaki ayırım gittikçe yok olmaktadır. Teoriye Soğuk Savaş sonrası istihbarat servislerinin raporlarında en sık kullanacakları kelime belki de “karşı” terimi olacaktır. Karşı istihbarat, kontr terörizm, karşı narkotik ve karşı silahlanma, modern servislerin kendi devletlerine yönelik saldırıları engellemek için gerçekleştirecekleri en önemli faaliyetler olacaktır. İstihbarat servislerinin Weber tarzı yapılanması, üretim sürecinin bürokratik engellere takılarak zaman, para ve kalite kaybına uğraması sonucu, istihbarat analistleri ile karar vericiler arasındaki hiyerarşik yapılanma kaldırılmış ve karar vericilerin de üretim sürecine aktif olarak katılmaları sağlanmıştır. Ancak, analistler ile karar vericilerin bir araya gelmesi istihbaratın politize olmasını, yani politikacılara karar verme aşamasında destek olmak yerine, politikacıların vermiş oldukları kararları destekleyici yönde istihbarat üretimi sorununu çözememiştir. Önemli olan siyasi karar vericiye en iyi ürünü sunmak olduğuna göre bunu zamanında ve en doğru yapacak yatay entegrasyon sağlanmalıdır.

Güç konseptlerindeki değişimler ve güç dağılımı geleceğin istihbarat servislerinin gelişimine de etki edecektir. İstihbarat servisi için oyunun yeni kuralları şu şekilde sıralanabilir;

- Gizli bilgi toplamak yerine politika yapıcıyı bilgilendirme.
- Sert hedefleri küresel kaplama ile aşındırmak.
- Öncelik 28 dilde olmak üzere bütün dillerde çeviri kabiliyeti.
- Devletin iki aşağı kademesine (devlet altı istihbaratı) odaklanmak.
- Kültürel istihbaratın temel olması.
- Jeouzaysal ve zaman sınırlaması.
- Küresel açık istihbaratı güç çarpanı yapmak.
- Karşı istihbarat satrancını kazanmak.
- İnsan & teknik istihbarat arasında verimlilik çekişmesini çözmek.
- Merkezi olmayan bilgi bankası (NGO, Özel vb.) kurmak.
- İstihbarat için; “Değer = İçerik + Şartlar + Hız” formülü.
- Öncelikler yerine bilgi açığı kapama amaçla istihbarat toplaması.

¹² Deborah G. Barger, Toward A Revolution in Intelligence Affairs, Rand Corporation, (Arlington/VA, 2005), 3-4.

¹³ Barger, a.g.e., (2005), 108-109.

- İhtiyaca dayalı üretim & kabiliyetler
- Stratejik istihbarata daha çok önem verilmesi.
- Etkili bütçe yönetimi.
- Kamu istihbaratının kamu diplomasisine etki etmesi.
- Analizcilerin yönetici olarak çalışması.
- Uluslar arası işbirliği için çoktarafli masraf paylaşımı.

İstihbarat örgütlerinin gelecekte en büyük zorluklarından biri istihbaratın dağıtımında olacaktır. Bugünün ve geleceğin istihbarat örgütleri bulmaca çözmeye daha az, sırları ya da cevabı kolay olmayan büyüklü problemlere daha çok angaje olacaklardır. İstihbarat analizcileri artık düşman füzelerinin menzilin ölçülmesi, denizaltılarını rotaları gibi analitik sorunlardan çok algı yönetimine odaklanacaklar ve algı için önemli olan bilgi için toplayıcı ile yakın çalışacaktır. İstihbarat analizcisi, kendi halkı için rakipleri, teröristleri, ayaklanmacıları, sosyal hareketleri, dini fanatikleri tanımlayan algı-yapıcı olacaktır. Bu nedenle, açık kaynaklar kullanmaya eğilimli karar vericilere angaje olabilecek iyi bir iletişimci olmalıdır. Analizciler ve karar vericiler gerçekleri inşa etmek (yeniden inşa değil) için birlikte çalışmalıdır. Anlamaya dayalı alanı olan istihbarat analizcisi, değere dayalı alanı olan politikacı ve diğer karar vericiler bir araya gelerek insanlara gerçekleri anlatacakları hikâyeleri yazmalıdırlar. Bu yüzden istihbarat artık politikanın sadece destekleyen bir süreç değil, analizcilerin algı yaratma işlevi ile aynı zamanda politika şekillendiricisi de oldular. Bu yeni işlev, istihbarat toplumunun görev alanını da genişletmektedir. Ancak, algı yönetimi; demokratik bir toplumda halka gerçekleri söylemek, şeffaflık ve yapılan işlerin meşruiyeti konusunda sorunlar çıkaracaktır. Öte yandan, istihbaratçı ve politikacı arasındaki bağlar böylesine sürekli ve yakın hale gelirken, istihbaratın siyasallaşmasının önüne geçilmesi ve bunun kamu denetimi de ciddi bir tartışma konusu haline gelecektir.

İstihbaratın Askerileşmesi

Uluslararası arenada söz konusu olabilecek ve geçmişte de yaşanmış güvenlik riskleri ile baş edebilmenin en ekonomik ve etkin yolu zorlayıcı diplomasi ile desteklenen örtülü yöntemler ve gizli savaşlar olacaktır. 21. yüzyılda politikanın gizli ve örtülü yöntemlerle devam ettirilmesi teknolojinin sağladığı yeni avantajlar ve yöntemlerle çeşitlenerek devam edecektir. İstihbarat fonksiyonlarının uluslararası güç mücadelesi içinde daha yaygın ve etkin kullanımı ile örtülü operasyonlar ve düşük yoğunluklu çatışmalar bazen değişime uğrayarak yaygınlaşacaktır. İstihbarat fonksiyonları ile güvenlik ortamını şekillendiren güçlerin sağladığı bölgesel etkinlik küresel etkinliğin de kapısını açacak, çokkutuplu ve rekabetin genellikle örtülü yöntemlerle sertleşerek sürdüğü bir uluslararası ortam yaşanacaktır. İstihbarat fonksiyonları ve ileri teknoloji konusunda ön plana çıkan ülkeler, ittifaklar sistemi ile dünya liderliğine oynayacaklardır. Askeri güç bu tür sorunlarla başa çıkmak için tek başına uygun bir araç olmadığından istihbarat fonksiyonları ile desteklenen diplomasi veya müdahale biçimleri daha uygun yöntemlerdir. Bu gelişmeler; ülkelerin dış güvenliklerinin daha etkin ve gelişmiş yapılanmalara, imkânlara ve yöntemlere sahip olmalarını gerektiğini göstermektedir. Günümüzde siyasi-stratejik ve ekonomik istihbarattan çok askeri-stratejik istihbarata odaklanılmaktadır. Bu istihbaratın yeni oryantasyonu oldu. İstihbarat sadece sivilleşmedi, son 20 yılda oldukça özelleşti ama bir yandan da yeşilleşti yani askerileşti.

2000'lerin istihbarat paradigmasının tarifi 11 Eylül sonrası dönemde yapılmaya başlandı. İstihbarat, belirli bir alanda ve taktik kullanıma uygun olmalıydı. 11 Eylül 2001 sonrası CIA geleneksel görevi olan ordu ile ortak görevlere başlarken, ajanlar askerlere dönüşüyordu. Askerler ise timler halinde Amerikan dış politikasının karanlık boşluklarına dağılıyordu. Yeni Amerikan savaş metodu için askeri-istihbarat kompleksi yaratılmıştı. Birbirinden ayrı ve paralel yürüyen pek çok savaşta özel kuvvetler ve istihbaratçılar yan yana çalışmalı idi. Sözleşmeciler özel şirketlere gizli casusluk ağı kurularak görevi verildi ve bölgedeki diktatörler, güvenilir yabancı istihbarat servisleri ve vekilli savaş güçleri ile işbirlikleri geliştirildi¹⁴. ABD, terörle gizli savaşta en önemli vasıta olarak silahlı insansız hava aracını (Predator) keşfetti ve halen onun yanına bir şey koyamadı. ABD'deki istihbarat servisleri gittikçe askerileşiyor hatta yapıları askeri modele kayıyor; daha merkezi ve yukarıdan aşağı liderlik. Geleneksel espionaj yani ajan kullanımı ile insan istihbaratı açık kaynak istihbaratında daha az değerli olacak, sosyal medya istihbaratı genişleyecektir¹⁵. Siber savaş, drone ve robotlar, özelleşmiş savaş, teknoloji ile güçlendirilmiş kişi ve küçük gruplar savaşın doğasını değiştirecektir.

Düzensiz savaşlar; fiziksel, entelektüel ve moral olmak üzere üç alanda yapılır. Modern savaş ise çifte bir vizyon krizi yaşıyor. Birincisi entelektüel vizyon sorunudur. Gerçek bir teknolojik devrimle karşı karşıya olduğunu kabul etmek istemiyor. Diğer sorun alanı ise yeni teknolojilerin yarattığı çözülemeyen problemlerdir; komuta-kontrol ve istihbarat krizi. ABD'nin terörle mücadelesi 5 yıl içinde iki büyük savaşta sonra İŞİD'a yönelik hava harekâtına, özel kuvvet operasyonlarına ve CIA'nın vekilli savaşlarına indirgenmiş durumdadır. Çare "akıllı savunma" ama bu çok para ve çok güçlü ordu anlamına gelmiyor. Yeni durumları önceden görmek, adapte olmak yani akıllı istihbarat ile operasyonel zorlukları yenecek eğitim ve kabiliyetlere sahip olmaktır. Ancak, Soğuk Savaş'tan kalma yapılara sahip istihbarat servisleri terörle mücadele için yeni yaklaşımlara ihtiyaç duyuyor. 21. yüzyılın istihbaratı için saldırgan avcı stratejisi gerekli ancak bu sadece teröristleri avlamayı yani öldürmeyi değil, yerel istihbarat ve güvenlik servisleri ile birlikte çalışmayı ve yerel hassasiyetleri dikkate almayı gerektiriyor¹⁶. Küresel terörün geldiği aşama yeni, saldırgan ve Ortodoks olmayan taktikler gerektiriyor¹⁷. Bir istihbarat teşkilatı olmasına rağmen CIA, ABD'nin terörle mücadelesinde ana vasıtalarında biri oldu¹⁸. Bu amaçla örtülü faaliyet alet kutusu (psikolojik savaş, bilgi savaşı, aldatma, siyasi-ekonomik ve paramiliter örtülü operasyonlar) koordineli bir şekilde kullanılmalıdır. Son yıllarda paramiliter programlar içinde eğitim-donat, hedefli öldürme programları öne çıktı.

İstihbaratın Öncelikli İş; Terörle Mücadele

Uluslararası güvenlik çevrelerinde gene kabul gören anlayışa göre, tehdidin doğası, dolayısıyla istihbaratın hedefi büyük ölçüde, ulus-devletlerden devlet dışı aktörlere kaydı. Devlet dışı aktörler, öncelikli hedef oldu. Ulus-devletler coğrafidir yani belirli bir coğrafya içindedir ve adresi bellidir. Onların uzun bir hikâyesi vardır ve

¹⁴ Mark Mazetti, *The Way Of The Knife, The CIA, A Secret Army, And A War At The Ends of The Earth*, Penguin Books, (New York, 2013), 4-5.

¹⁵ Jane Harman, *Disrupting the Intelligence Community*, Foreign Affairs, March-April 2015, <https://www.foreignaffairs.com/articles/united-states/2015-03-01/disrupting-intelligence-community>

¹⁶ Cogan Charles, *Hunters not Gatherers: Intelligence in the 21st Century*, *Intelligence and National Security* 18, No. 2 (Summer 2004), 316.

¹⁷ William Akin, *The Secret War*, Los Angeles Times, (27 October 2002).

¹⁸ Commission on the 9-11 Terror Attacks, *Intelligence Policy*, Staff Statement No.7, (Washington DC, 2004). http://govinfo.library.unt.edu/911/staff_statements/staff_statement_7.pdf

istihbarat, bu hikâyelerden yola çıkarak kendi liderlerine yön verecek çalışmalar yapar. Hikâye olmadan, yeni bir bilgi sadece boş bir bilgidir. Devletlerarası ilişkiler hiyerarşik ve bürokrattır, tehdide dayalıdır. Devletlerin çıkarları ve hedeflerini anlamak için savunma yeteneklerine bakılır; tanklar, füzeler, ordunun büyüklüğü vs. Teröristler (bireyler, şebekeler ve örgütler) ise her yönden devletlerden farklıdır. Küçük yapılardır ama bir intihar bombacısı bile büyük sonuçlar doğurabilir. Dönüşen, akıcı ve gizli yapıları hakkında istihbarat toplamak zordur. Ne adresleri vardır ne de sadece oradadırlar. Teröristler genellikle bir halkın içinde saklıdır ve onlar hakkında bilgi toplarken sivil halkın özgürlüklerine zarar vermemelisinizdir. Onlarla ilgili çok az hikâye vardır ya da yoktur. 11 Eylül 2001'den beri hala El Kaide'nin hiyerarşisi, şebekesi, eylemleri, ideolojisinin ne olduğu tartışılıyor.

Bütün bu gelişmeler istihbarat örgütlerine de etki ediyor ve geleceğe ilişkin çalışmalara önem kazandırıyor. İlk yaşanacak etki bugün bahsettiğimiz "istihbarat" ya da "gizli istihbarat" kavramı ile 20 yıl sonra aynı şeyi mi kastedeceğimiz sorusunun cevabıdır. Gizli istihbarat, başkasının sizin bilmenizi istemediği ve vermediği bilgiyi elde etmek başarısıdır. Bunun için hala ajanlar eğitiliyor, yabancı ülkelerde irtibat personeli kullanılıyor ve özel haberleşmeler elektronik olarak takip ediliyor. Bilgi ve haberleşme teknolojileri şirketleri halen uluslararası çatışmalarda çok önemli roller oynuyorlar. Arap hareketlerindeki devrimlerin alt yapısını kurdular¹⁹. Örneğin Suriye'de muhalif gruplar şirketlerden istifade ederek (Google Map Maker) bölgenin haritasını çıkardılar, insan kaynağı temin ettiler (crowd-sourcing program) ve rejim üyelerinin ailelerine kadar tüm bağlantılarını ve yerlerini öğrendiler. Protestolar başladığında yerel olarak muhaliflerin elinde Google editörleri tarafından onaylanmış isim listeleri vardı²⁰. Protestocular, Google sayesinde sadece elektronik haritaları değiştirmediler, cadde ve sokaklara kendi isimlerini verdiler. Böylece muhtemel bir barış anlaşması için Google sayesinde kendilerine göre bir meşru harita geliştirdiler. Suriye hükümeti BM'de Google'dan şikâyetçi olunca, şirket yetkilileri bu bilgileri yetkili (!) kaynaklardan aldıklarını söylediler²¹. Ayaklanmacılar ile teknoloji şirketleri işbirliği içinde bu tür oyunları Ortadoğu genelinde, Güney Asya ve Latin Amerika'da da oynuyorlar.

21. yüzyılın tehditleri artık devletlerden çok devlet dışı aktörlerden, teröristlerden, ayaklanmacılardan, aşırılık yanlılarından, organize suçlardan, siber hacker'lardan, korsanlardan kaynaklanıyor. İletişim ve haberleşme alanındaki teknolojik gelişmeler açlık, kıtlık, insan hakları, göç, hastalıklar gibi tehditleri daha görünür hale getirdi. Dış politikada ulusal hükümetlerin ikna edilmesi için gene kendi halkı kullanılacaktır. Bu amaçla, bölgesel güvenlik aracı olarak "ikna" yöntemi için yenilikçi yaklaşımlara başvurulabilir. Uzmanlaşmış, yüksek teknolojiye sahip gizli faaliyetler yerel hareketlerin desteklenmesinde rol alabilir. Küresel kamuoyu, stratejistlerin dikkate alması gereken gerçekten önemli bir faktör olarak ortaya çıkmaktadır. Küresel iletişim "kopyacılığı" mümkün kılmaktadır. Anında ve yoğun küresel haberleşme; ülkelerin, kendi vatandaşlarının (veya diğer ülke vatandaşlarının) neyi duyması, görmesi, okuması, bilmesi ve inanması gerektiğini etkileyecek kabiliyetlerini erozyona uğratmıştır. Teknoloji insanların hayatının kalitesini artırır ve toplum yaşamını dönüştürürken, özel hayatın gizliliği endişe konusu oldu.

¹⁹ Sims, ibid, (2014), 58.

²⁰ Column Lynch, Syrian Opposition Seeks to Wipe the Assad Name Off the Map -via Google, Washington Post, (14 February 2012).

²¹ Lynch, ibid, (14 February 2012).

İstihbaratın Özelleşmesi

17. yüzyıldan beri özel şirketler ülke kaynaklarının (İngilizlerin Doğu Hindistan Çay Şirketi ya da Amerikalıların Standart Oil'i gibi) sömürülmesinde kullanılırdı. Bugün teknoloji şirketleri ile ülke egemenlikleri ve kendini savunma hakları ellerinden alınıyor. Şüphesiz bu şirketlerin istihbarat servisleri ile iç içe çalıştığını düşünüyorsunuz ama bu bile yetersiz çünkü daha da ötesinde birçok devletten ya da devletler grubundan daha etkili bir "istihbarat silahı" olarak kullanılıyorlar. Tarihte hiç olmadığı kadar uluslar arası politikada bir güç çarpanı haline geldiler. Soğuk Savaş döneminde çok büyük, çok yavaş ve çok katı bir rakip vardı. Bugün ise rakiplerimizden daha hızlı karar alma ve harekete geçme kabiliyetine sahip değiliz. Özel ticari şirketler ve akademik ortaklar hükümetlerin daha hızlı hareket etmesine yardım edecektir. Soğuk Savaş döneminde istihbarat gizli bilgi demektir ve karşı tarafın sakladığı bu bilgiyi almak istihbarat servislerinin işi oldu. Toplanan bilgiler bir süreçten geçirilir ve gene gizli kanallardan üst makamlara rapor edilirdi. Bugün bu sistem ne yeterli ne de kabul edilebilir. Artık özel sektörü kaynak olarak kullanma dönemindeyiz. Örneğin ticari bir şirketin uzaydan aldığı bir görüntü ile Çin'de bir havaalanına park etmiş bir askeri uçak resimlenmektedir. Dış kaynağa başvurmak işi başkasına yani özel sektöre yıkmak değildir. Ticari ve akademik dünya ile birlikte stratejik ortaklıklar ve müşterek projeler içinde iyi düşünülmüş süreçlerin kullanılmasıdır. Resmi ve özel istihbarat üreticileri ve tüketicileri farklı ürünler için artan şekilde iç içedirler. Haber analizinden kamu diplomasisine, dezenformasyondan aldatmaya ortak projeler uygulanmaktadır.

11 Eylül 2001 sonrası ABD istihbarat toplumunda sessiz bir devrim oldu ve pek çok büyük çaplı iş, dış kaynak kullanımı (outsourcing) ile sözleşmeli özel şirketlere verildi. Artık istihbarat servislerinin temel fonksiyonları özel şirketler tarafından yerine getirilmektedir. 2007 yılında ABD hükümeti kabaca 2.8 trilyon dolar olan federal bütçesinin yaklaşık 1 trilyon dolarını güvenlik işlerine harcadı²². ABD'de özel sözleşmeli şirket çalışanı sayısı 7.5 milyondan fazla olup, bu federal işgücünden dört kat daha fazladır. Bütçe açığının 10 trilyon doları geçtiği ABD'de, sözleşmeli şirketlere yılda yarım trilyon dolar verilmektedir²³. Mayıs 2007'de yayınlanan ODNI'nin bütçesinin %70'inin sözleşmelere gittiği görüldü. NSA'nın işlerini özel şirketler olmadan yapması mümkün değildir. Pentagon'un yeni istihbarat birimi Terörle Mücadele Sahra Hareketi (CIFA²⁴) personelinin %70'i gene sözleşmeli şirket elemanıdır. DIA'nın 2007'deki çalışanlarının %51'i aynı durumda idi. CIA'da da durum farklı değildi. CIA iş gücünün %50-60'ı, özellikle Ulusal Gizli Servis (NCS) ve insan istihbaratı bölümü çalışanları özel şirketlere mensuptur²⁵. Özel şirket çalışanları, CIA içindeki adı ile "Yeşil Porsuklar", Irak'ta örtülü operasyonlardan casusları işe alma ve çalıştırmaya kadar pek çok hassas hizmet verdiler. CIA adına insan istihbaratı toplayıp analiz ettiler ve istihbarat ürünlerini diğer ülke istihbarat servisleri ve hükümetin diğer daireleri ile paylaştılar. Lockheed Martin, Raytheon, Booz Allen Hamilton, SAIC ve diğer şirketlerin istihbaratçı profesyonelleri, ODNI ve diğer istihbarat servislerinin analitik bölümlerine entegre oldular.

²² Christopher Hellman, U.S. Security Spending: How Much Do We Really Spend?, Center For Arms Control and Non-Proliferation, (Oct. 1, 2007), http://www.armscontrolcenter.org/policy/security_spending/articles/how_much_do_we_spend/.

²³ Shane Scott, Ron Nixon, In Washington, Contractors Take on Biggest Role Ever, New York Times, (Feb. 4, 2007).

²⁴ CFA: Counterintelligence Field Activity.

²⁵ Raelynn J. Hillhouse, Outsourcing Intelligence, The Nation, (July 24, 2007).

Güvenlik ve istihbarat şirketleri, iç içe her gün pek çok yeniliğe yol açmakta ve siyasi arenada sözü geçen birer aktör haline gelmeye başladılar. Lobicilik ya da danışmanlık gibi görüntüler altındaki bu şirketlerin yönetiminde çalışanlar ve elemanlarının çoğu eski istihbarat servisi ya da özel kuvvetler çalışanlarıdır. Hemen her gün istihbarat dünyasından iş dünyasına bir transfer haberi rutin hale geldi. İstihbarat servislerinin bütçe detayları gizli olduğu için hangi serviste ne kadar özel şirket elemanı olduğunu net olarak söylemek mümkün değildir. Sözleşmeciler şirket kullanımı bir seçenek olmaktan giderek zorunluluk hale geldi. Gittikçe yasal ve yasal olmayan güç kullanımı arasındaki çizgi de kayboldu. Ulusal güvenlik ya da devlet istihbaratının temel amacı, ulusal çıkarları geliştirmektir. Ancak, özel şirketler gittikçe istihbarat, güvenlik ve savunma politikalarında etkili olmaya başlıyor. Özel şirketlerin istihbarat alanına da yoğun şekilde girmesi ile bu çıkarların belirlenmesinde şirketlerin hissedarları da söz sahibi olmaya başladı. Devletin özel istihbarat şirketlerine ait personel, bilgi ve uzmanlığı ne kadar kontrol edebildiği tartışılmaya başlandı²⁶. Bu yabancı kaynakların gizlilik dereceli bilgiye nüfuz etmesine imkân sağlayabilir. İstihbarat örgütleri ve büyük şirketler arasındaki ilişkiler nedeniyle gözetleme ve izleme işlerinin örtülü operasyonlar içerisindeki rolü çok daha büyümüş ve küresel bir hal almıştır. ABD ve Avrupa'da ortalık iş istihbaratı ile ilgili şirket kaynamaktadır. İstihbarat servisleri ve özelde istihbarat şirketleri kendilerine iş dünyasında finans ve yatırım danışmanlığı işlerinden sonra yeni pazarlar bulmak ve görünümelerini kamufle etmek için lobicilik, güvenlik ve kriz yönetimi alanlarına da el attılar. Önemli ölçüde güç kaybeden istihbarat servisleri çare olarak emekli personelinin özel şirketlere gitmesini yasaklamayı düşünüyor.

İstihbarat Fonksiyonlarında Yeni Trendler

İstihbarat, örtülü operasyonlar, propaganda ve koruyucu güvenlik kabiliyetleri; birer istihbarat fonksiyonu olarak ulusal güvenlik önlemlerinin daha belirgin bir ögesi haline gelmiştir. İstihbarat dün olduğu gibi bugün de bir insan gayreti olarak kalmaktadır. Örgütler ve teknolojiler gelişirken yeni vasıtalar ve yöntemler bulmakta ama eski moda olanlar göz ardı edilemeyecek kadar geçerli olmaya devam etmektedir. Düşük teknolojilerin tek başına yeterli olmayacağı durumlarda vardır ve bu yüzden istihbaratçı her türlü vasıtayı birbirini tamamlayacak şekilde kullanmak zorundadır. Bilgi çağında istihbarat planlama süreci, modern yönetim şekillerinin uygulanmasını zorunlu kılmaktadır. Daha esnek, daha uyumlu ve daha sorumluluk sahibi bir planlama süreci oluşturulmalıdır. İstihbarat için değişim alanları şu şekilde sıralanabilir²⁷;

- Toplama,
- Değerlendirme,
- Uyarı,
- Güvenlik,
- Dağıtım,
- Bütçe ve Programlar,

²⁶ Janine R. Wedel, Is the intelligence Community Out of Control? Washington Post, (July 25, 2010).

²⁷ Douglas H. Dearth, Intelligence in the 21 st Century Re-focusing INtelligence to Shape Strategic Environment, Joint Military Intelligence Center, (March 1, 2016). http://www.oss.net/dynamaster/file_archive/040319/cb248eb2338cc18756bdf71de8db26a0/OSS1999-P2-30.pdf

- Organizasyon,
- İnsan gücü,
- Uyum gösterme,
- Radikal çözümler.

Toplama kabiliyetleri ile ilgili değerlendirmeler şu şekildedir;

HUMINT; eskisi kadar önemli çünkü teknoloji her yere gidemez. İnsan istihbaratının öncelikli amacı hedefin niyetini öğrenmek. Örtü sağlamak ve dokümantasyon gittikçe zor hale geliyor. Espiyonaj gittikçe dijital hale geliyor. Ajan tipi değişiyor.

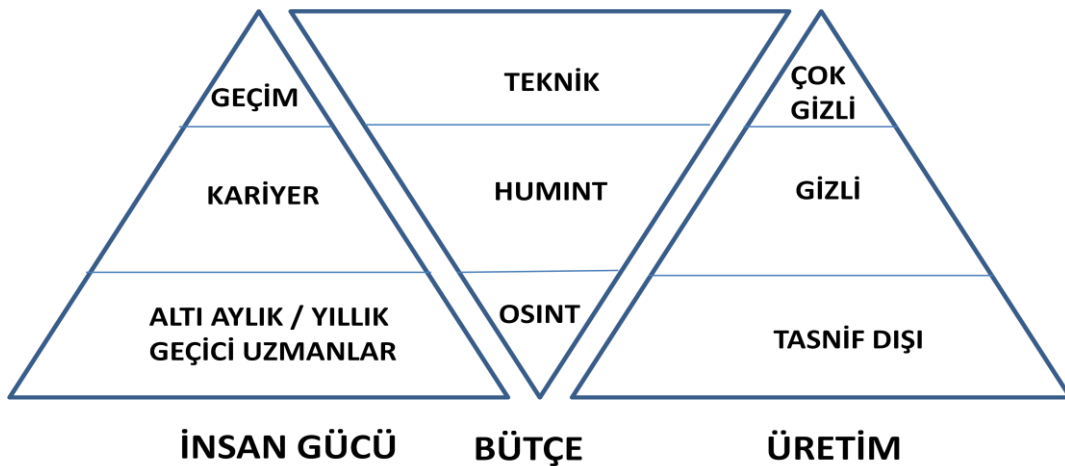
SIGINT; en önemli güç çarpanlarından biri haline geldi. Özel kriptolama kullanımı kritik bir kabiliyet.

IMINT; rolü değişiyor, istatistik geliştirmek artık çok önemli değil. Ticari hale gelirken, operasyonel güvenliğe etkileri konusunda dikkatli olunmalıdır.

OSINT; bütün yararlı bilgiler açık değildir, bütün gizli bilgiler de yararlı değildir. Kaynakların güvenilirliğini araştırmak önemli ama zordur.

ABD istihbaratı teknik istihbarata özellikle GEOINT, SIGINT ve MASINTa yöneliyor, HUMINT gittikçe kayıp tarafta kaldığı için analizciler büyük resmi haberleşmeler, gazeteler ya da ölçülen emisyonlardan okumaya çalışıyor²⁸. HUMINT olmadan bu verilerin teyit edilmesi, rakibin niyet ve kabiliyetleri anlaşılması zordur. Taktik istihbarat alanında da aynı sıkıntı yaşanıyor. 21. yüzyılın operasyonel istihbarat ihtiyacı insansız hava araçlarına bağımlılığı oldukça artırırken, insan istihbaratı da tersi bir trend izliyor. İstihbarat başarısızlıklarının çoğunun arkasında HUMINT eksiği yatıyor. 21. yüzyılda gizli istihbaratın rolü dönüşüm içindedir. İstihbarat ve güvenlik konularının politikadaki yeri ve bu konuda kamuoyu bilinci daha arttı.

Şekil 1: İstihbaratın Yeni Dengesi



Robert David Steele, The Evolving Craft of Intelligence, in Robert Dover, Michael Goodman, and Claudia Hillebrand (eds.). Routledge Companion to Intelligence Studies, Routledge, (Oxford, 2013).

Analiz ve değerlendirme; rakamlar çok önemli olmaktan çıkıyor, gizli bilginin kullanımı azalıyor. Büyük bilgi yığını içinde neye baktığımız, neyi aradığımız önemli

²⁸ Gabriel Margolis, The Lack of HUMINT: A Recurring Intelligence Problem, Global Security Studies, Volume 4, Issue 2, Spring 2013, p.4-7.

hale geliyor. Devlet-dışı aktörlerle ilgili analiz yapmak farklı yetenek setleri gerektiriyor. “Yeterli olmak” yerine “zamanında bilgi”, bazen de “konuya özel istihbarat” öne çıkıyor. Kültürel istihbarat geliştirilmelidir.

İstihbarat kaynaklarının çokluğu, operasyonel ihtiyaçlar için gerçek zamanlı bilgi ihtiyacı istihbaratın entegrasyonunu gerekli kılmaktadır. Toplanan bilgi işlem görmedikçe istihbarat değildir ve bundan dolayı potansiyel olarak yararsızdır. İstihbarat servisleri, toplama ve analiz konusunda kendi özel yöntemlerini geliştirmek zorundadır. Yeni teknolojiler entegre ederek toplama kaynakları ve analiz için uzmanlaşma geliştirilmelidir. Günümüzün karmaşık istihbarat ürünleri için iş ve akademi dünyası ile işbirliği ve ortaklıkların gayri resmi olarak sürdürülmesi artık olanaksızdır.

Bilgiyi nasıl işlediğimiz de değişmelidir. Evrensel olarak pek çok bilgi sıradan insanlar gibi tüm istihbarat servislerine de açıktır ve internet yolu ile ülkelerin iç istikrarı takip edilmektedir. Güvenilir özel şirketler varken istihbarat toplama, işlem ve sunma görevlerini sadece resmi makamlara bırakma fikri artık geride kaldı. Bu tür işbirliklerinin büyük avantajları görülmektedir.

Uzun dönemli analiz ve temel araştırmalar azalma sürecindedir. Uygulanan politikaların desteklenmesi için gerekli günlük talepler artık analitik kabiliyetlerin ötesine geçmektedir. Uzun vadeli analizler için gerekli kaynaklar ve analitik programlar yetersizdir. Analiz konusuna yatırım artırılmalıdır. Stratejik izleme ve terörle mücadele klasik bütçe uygulamaları ve sınır kontrolleri ötesinde ihtiyaçlar doğurmaktadır. Ulusal güvenlik, iç güvenlik, suç ve yolsuzluklar, uzay ve havacılık teknolojisi, gelişmiş malzemeler, biyografik bilgiler, askeri doktrin ve strateji alanında edinilen devasa bilgi yığınının analiz edecek yeterli analiz kabiliyeti yoktur. Açık kaynaklar arttıkça kültür, tarih ve dil daha önemli hale gelmektedir. Gerçek zamanlı istihbarat için analizciler yabancı kaynaklardaki bilgileri hızlı bir şekilde arayacak, sınıflandıracak, depolayacak ve yeniden ilave edecek makine tercüme kabiliyetlerine sahip olmalıdır.

İkinci Dünya Savaşı’ndan beri hava tahminler bir istihbarat işlevi olarak görüldü. Bugün bu işlev kamu hizmeti olarak görülüyor. Ancak, istihbarat alanındaki değişim ihtiyaçları yeni görev bölümleri getirebilir.

İstihbarat analizi hala entelektüel bir iş ve analizcilerin beyninde oluşmaktadır. İstihbaratçılık gittikçe kötümser bir eğilimde gidiyor. Bob Gates bir zamanlar şöyle demişti; CIA analizcisi çiçekleri koklamayı bıraktığında daima etrafına bir cenaze için bakmalıdır. Eğer politika yapıcı iyimser değilse o işini yapamaz. Gerçeklere dayalı, tümevarımlı, mevcut dünyaya kötümser bir bakış ile vizyona dayalı, tümdengelimci, dünyayı hayal ettiği gibi iyimser görmeye çalışan iki anlayıştan biri içindeyizdir. İstihbarat politika üretmez ama doğru yapıldığında onun sınırlarını belirler, işte katkısı budur.

İkaz istihbaratı; erken uyarı için emareler geliştirilmelidir. Risk yönetimi problemin özüdür. İkaz istihbaratı gittikçe taktik hale geliyor ama bazen tüm uyarılar stratejik olabiliyor.

Güvenlik; güvenlik geçmişte hiç olmadığı kadar önemli hale geldi ve paranoya ile karışmaya başladı. Ekonomik güvenlik, fiziksel güvenliğin önüne geçti. İstihbarat Karşı Koyma ve Karşı Espiyonaj dijital hale geliyor.

Dağıtım; kâğıt ürünler kalkıyor, yerini gayri resmi konuşmalar alıyor. Zamanındalık içerikten önemli hale geliyor. Hem bizim hem de rakibin karar verme

sistemine göre davranmak zorundayız. Gizlilik derecesi ile sınıflandırma minimal hale geliyor.

Bütçe ve programlar; teknolojinin ömrü aylarla sınırlı olmaya başladı. Özel şirketlere bağımlılık arttıkça hükümetler de iş adamı gibi davranmak zorundadır.

Organizasyon; “düşündüğümüz şekilde mi organize olmalıyız, organize olduğumuz şekilde mi düşünmeliyiz çelişkisi yaşanıyor. Kendi konumlarını her zaman korumaya çalışanlar ve bürokratlar en büyük engel.

İnsan gücü; eğitim ve profesyonellik öne çıkarken kaliteli personeli tutmak veya işe almak özel teşvikler ve tatmin gerektiriyor. Dil bilen, yerli eleman temini ihtiyacı hassasiyet oluşturuyor.

Uyum gösterme; stratejik U dönüşleri için gerekli, keskin uçlarda çizgide oynamak zorunlu ama sıkıntılıdır.

Radikal çözümler; reform içerden gelmeyecek, sivil memur sistemi kalkmalı. Sürekli kriz ortamında yaşamaya alışkın ama paranoya içinde olmayan bir ortamda çalışmaya dayanıklılık gerekli. İstihbarat, kötü politikayı kurtarmaz, işin köküne gidilmelidir.

Sonuç

İstihbarat, belirsizliğin azaltılması ile ilgilenir, yani belirsizlik arttıkça istihbarata olan ihtiyaç da artacaktır. Soğuk Savaş sonrasında artan belirsizlik ortamı ve karmaşık ilişkileri iddia edildiğinin aksine istihbarata olan ihtiyacı arttırmıştır. 21. yüzyılda istihbarat tarihte hiç olmadığı kadar dünya politikaları için önemli hale geldi. Körfez Savaşı, 11 Eylül 2001 saldırıları, Afganistan ve Irak Savaşları'nın ardından yaşanan Renkli Devrimler ve Arap Hareketleri istihbaratın gerek resmi, gerek akademik ve gerekse popüler medya içinde güvenlik ve uluslararası ilişkiler bakımından önemini artırdı. Geleceğin kriz ve çatışmaları için artan bir şekilde ilave ve yeni istihbarat kabiliyetleri gerekmektedir. Tehditteki değişim kadar savaş alanındaki değişim de istihbarat toplumunda değişiklikleri zorunlu kılmaktadır. Bugünün cevap bekleyen soruları ise şunlardır; terörle mücadelenin istihbarat faaliyetlerinin diğer alanlarını nasıl etkilediği, erken ikazın hala istihbaratın öncelikli işi olup olmadığı, savaşın değişen doğasının istihbarata olan etkileri, Ortadoğu başta olmak üzere bölgesel olarak istihbaratın çatışma yönetimine katkısı, istihbarat vasıtalarının kriz yönetiminde en etkili nasıl kullanılabileceği, demokrasilerde istihbaratın karşılaştığı sınırlamalar. İstihbarat ve güvenlik teşkilatları için istenen bilginin doğası gittikçe hükümetlere ve kuruluşlarına muhalif olan bireyler ve devlet dışı aktörlere doğru kaymaktadır. Bu ihtiyaç seyahatlerinden bankacılık işlemlerine kadar SIGINT ya da HUMINT yolu ile bu kişilerin özel bilgilerine nüfuz etmeyi gerektirmektedir. Böylece kişilerin özel bilgilerinin korunmasının ahlaki önemi yanında devletin modern teknolojiyi kullanarak gittikçe daha çok insan hakkında bilgi toplaması, özel hesaplarına nüfuz etmesi, bilgi madenciliği yapması “gözetlenen toplum” korkusu artmaktadır. Bugün tüm dünya, uluslararası izleme ve insan avına dur demek için hala durum farkındalığı ve tepkimizi belirleme aşamasındadır.

Soğuk Savaş sonrası dikkati çeken bir diğer husus, artık ulus devletlerin dünya uluslararası ilişkilerinde tek aktör olmadıkları ve hatta egemenliklerinin bir kısmını devlet dışı aktörlere gönüllü ya da zorunlu olarak devretmek zorunda kaldıklarıdır. İstihbarat servisleri, hem bu örgütlerle hem de bu örgütlere karşı yeni eylem stratejileri geliştirmişlerdir. Özellikle istihbaratın toplanması ve örtülü faaliyetlerin yürütülmesi safhalarında bu örgütlerden faydalanılmaktadır. Soğuk Savaş sonrası

ticarî şirketler, hükümet dışı organizasyonlar, devlet dışı örgütler, yardım kuruluşları, gönüllü teşkilatlar ve misyoner okulları gibi enstrümanları da dahil ederek, espionaj ağını resmi ajan dışı unsurlarla genişleten istihbarat servislerine karşı farklı metotlarla mücadele edilmelidir. İstihbarat teşkillerinin üç temel dinamiği aynıdır; müşteri kimdir, ne istemektedir, ne zaman istemektedir. İstihbarat kullanıcıları başta ülke liderleri ve danışmanları olmak üzere politika yapıcı daire ve teşkiller ile teknik istihbarat ile ilgili analiz unsurlarıdır. 21. yüzyılın operasyonları için istihbarat profesyonelleri, pratik ama yenilikçi, hızlı ama karara etki edecek kalitede bilgi temin edecek bir sistem geliştirmelidir. İstihbarat, bir silah sistemi gibi olmalı; kaynaklar gerektiğinde bir araya getirilmeli, manevra yapmalı, geleneksel ve kinetik sistemlere adapte olabilmelidir. Doğru şekilde hareket eden, kolayca kaçmayan, uzun vadeye odaklanan bir istihbarat sistemi ve güç projeksiyonu tasarlamalıyız. Şimdi 21. yüzyıl paradigmasını yakalamak, uyum sağlamak, fırsatları değerlendirmek için yeniden yapılanmalara gitmek ve anlaşılması zor, yeni yöntemler bulmak zamanıdır. Geleceği öngörmenin en iyi yolu geleceği kendimizin tasarlamasıdır. İstihbarata düşen ise ülkenin önünün açılması, yani geleceğinin hazırlanmasıdır.