MUHABERAT MUHAREBATI

BİLGİ HARBİ

GENEL DEĞERLENDİRMELER
VE
ABD, RUSYA, ÇİN ÖRNEKLERİ

RUŞEN EŞREF YAZGAN

Ankara

Ekim 2012 – Ekim 2013

İçindekiler

ÖNSÖZ

. . . . . yazılacak . . . . . .

GİRİŞ

Bilgi ile çevrili, iç içe yaşadığımız bu çağda bilginin faydalı amaçlar doğrultusunda yönetiliyor olması hayati önem taşımaktadır.

Uğrunda savaşılacak kadar hayati önemi olan bilginin kendisi zamanla yaşam ortamı haline gelmiş ve yaşam ortamı bilgi olunca tabii ki savaş ortamı da bilgi olmuştur. Günümüzde bilgi savaşları bilgiyi kullanarak, bilgi ortamında yapılmaktadır artık. Aradaki çizgi çok ince olsa da bilgi için yapılan savaşların ötesinde bilgi ortamında yürütülen savaşları *bilgi harbi* terimiyle ayrıştırmak daha doğru olur.

Bilgi harbinin konu edildiği bu derlemede bilginin hayatımızdaki önemi vurgulanmakta, bir harp aracı olarak bilginin kullanımı ve tarihsel gelişiminden bahisle uygulamalardan örnekler verilmekte, bilgi harbinin en temel uygulamalarından kriptoloji ilmi (sanatı) ve bilgi güvenliği hakkında ilgi çeker konulara değinilmektedir. Genel bilgilendirmeye ilaveten, bu harp yöntemini geliştiren ve uygulayan ABD, Rusya Federasyonu ve Çin Halk Cumhuriyeti'nin bilgi harbi doktrinleri ve uygulama örnekleri de bu derlemede yer almaktadır. Özellikle ABD kaynaklı dokümanlara geniş yer verilmiştir, çünkü konu ile ilgili birçok kavram ve terminoloji bu kaynaklarda yer almaktadır. Rusya ve Çin doktrinleri ile ilgili bilgiyi batılı kaynaklardan, özellikle İngilizce yazılmış veya tercüme edilmiş dokümanlardan edinmek durumunda kaldığımı belirtmeliyim. İster istemez bu kaynakların bakışını veya yanlışını yansıtmış olabilirim.

Bilgi harbi üzerine birçok kitap ve makaleye ilaveten internette bir dolu bilgi mevcuttur. Öyleyse, bilinenleri tekrarlayan, yeni bir şey söylemeyen, özgün kaynak olmayan bir çalışmaya daha gerek var mı diye sorduğumda kendime, hayır cevabını veriyordum. Yeni bir şey söylemeyecekse ne gerek var ki diye düşünüyordum. Öte yandan, Türkçe kaynakların ve tek tük tercümenin yetersizliğinin farkında olarak, mevcut yerli ve yabancı kaynaklardan bir derleme yapmanın ilgilenenler için yararı olabileceğini düşünmüyor da değildim. (Yetersiz derken, nitelik değil nicelikten söz ediyorum; nitekim, birçoğu bu derlemeden çok daha niteliklidir. Bu kaynakları Türkçemize kazandıranlara teşekkür borçluyuz.) Birbirine zıt düşüncelerimin mücadelesinde, böyle bir derlemeyi yapmamın faydalı olacağı görüşü galebe geldi ve bu derlemeyi hazırlamaya karar verdim. Birçok yerde özgün fikirlerimi dile getirse de nihayetinde bu -intihal sınırında gezinen- bir derlemedir; içerdiği bilgiler başka kaynaklardan derlenmiştir. Benim bakış açım, algılamam ve yorumlamamla derlenmiş olsa dahi bilhassa vurgulamak isterim ki özgün kaynakların sahipleri, araştırmacılar, yazarlar asıl övgüyü hak etmektedirler. Eksikler, hatalar, tutarsızlıklar varsa bilinsin ki tamamen bana aittir.

Hangi bilgiyi hangi kaynaktan derlediğimi belirtmemiş olsam da az veya çok yararlandığım veya ilgilenen için yararlı olacağını düşündüğüm kaynakları derlemenin sonundaki kaynakçada listeledim.

Derlemeyi kurgularken hangi alıntıyı hangi kaynaktan yapmış olduğumu belirtmememin sebepleri var:

Birincisi; üşendim.

İkincisi; bilimsel ve teknik çevrelere değil, genel okuyucuya hitap ediyorum. Kolay okunabilir, anlaşılabilir olmasına özen gösterdim.

Üçüncüsü; bu derleme bir bakıma belgesel tadında film veya film tadında belgesel gibi olsun istedim. Nasıl ki her sahnede kaynak belirtilmiyor; yararlanılan kaynaklar, müzikler, yapımda yer alanlar filmin sonunda sıralanıyor; işte öyle olsun istedim.

Ve en önemlisi; ilgi duyanların bu bakir coğrafyada benim almış olduğum keyfi tadarak benzer bir yolculuk yapmalarını istedim. Amacım, farkındalık yaratmak, mümkün olduğunca fazla gezgini bu yolculuğa davet etmekti. Eminim ki onlar da benim aldığım keyifle bu yolculuğu yapacak; bazıları yararlı sonuçlara ulaşacak veya özgün eserlere imza atacaklar. Makale veya kitap yazmasalar dahi, yapacakları çıkarımlarla uygulamada yarar sağlayabilirlerse ne mutlu bana.

İlk ve en önemli çıkarımı yapmada yardımcı olabilirim: matematik. Okul öncesinden sonuna kadar icraatta, fikriyatta ve hatta hissiyatta matematik…

İkincisi; hani bilinen sözdür, "Siz de parçasıysanız devrimin farkına varabilir misiniz?" Birçoğumuz farkında olmadan yaşıyoruz bilgi çağı devrimini. Farkına varmadan gelip geçen devrimleri, sonradan tarih kitaplarında okumaktansa, zamanında idrak ederek içerisinde yer almalı ve geleceğe yönelik konum belirlemeli, çaba harcamalıyız.

Özellikle vurgulamak isterim ki birkaç ülkenin bilgi harekâtı doktrinlerinin ele alındığı ikinci bölümde yer alanlardan yola çıkarak paranoya yaratmak veya mevcut paranoyaya katkıda bulunmak, komplo teorisyenlerine malzeme sunmak niyetinde değilim, kesinlikle. İlginç bulduğum konunun tarihsel gelişimi ve güncel konumu ile ilgili elimden geldiğince doğru bilgi ve kendi kişisel görüşümü ortaya koyuyorum, sadece. Yapılması gereken; tespitleri dikkate alarak akıllıca değerlendirmek, usluca tedbir almak ve doğru hareket etmek olmalı. Katkım olursa, ne mutlu…

Birkaç söz de derlemenin dili hakkında söylemek isterim. Farkındayım, biraz eski; hatta arkaik bile denebilir. Ama askeri kavramlar, terimler söz konu olduğunda, hatta uçağa hâlâ tayyare dendiği göz önüne alındığında bu dili kullanmak kaçınılmaz oluyor. Dahası, eski kelimeleri kullandıkça gördüm ki hoşuma da gidiyor. Yaşatmak gerek.

Son olarak belirtmeliyim ki İngiliz matematikçi G.H. Hardy'nin özellikle altmışlı yaşlarda yapılan bu tür çalışmaları küçümsemesine rağmen keyifle yaptım. Umarım araştırırken ve yazarken aldığım keyfi okurken siz de alırsınız.

Teşekkür ve saygılarımla,

Ruşen Eşref YAZGAN Ankara, Ekim 2012 - Ekim 2013

BİRİNCİ BÖLÜM

Bu bölümde, bilginin bir harp vasıtası, hatta harp ortamı olarak kullanılması değerlendirilmekte; bilgi hakkında genel değerlendirmenin yanı sıra bilgiye yönelik, bilgiyi kullanarak, bilgi üzerinde yürütülen harbin vasıtalarından söz edilmektedir.

- . -

BİLGİ

Çağımız, birçokları tarafından *Bilgi Çağı* olarak tanımlanmaktadır ki bu bir bakıma doğru kabul edilebilir. Bilgi, çok değerli olmanın ötesinde, en yaygın olgu olarak günlük yaşantımızda yer almakta; fiziksel, kültürel hatta duygusal çevremizin şekillenmesinde önemli rol oynamakta, varlığımızı anlamlandırmaktadır.

Sadece çağımızda değil, geçmiş çağlarda da her zaman çok değerliydi bilgi. Eski çağlardan beri insanoğlu bilgiye ulaşmak, onu çoğaltmak ve ondan yararlanmak için çabaladı. Tarih öncesi çağlarda hangi bitkinin besleyici olduğu, hangi hayvana nasıl tuzak kurulacağı bilgisi ne denli değerliydiyse; yüksek verim için tarlanın nasıl sürüleceği, savaşkan atların nasıl yetiştirileceği, uzak mesafelere suyun nasıl aktarılacağı bilgisi ilkçağda; korunaklı kalelerin nasıl inşa edileceği, sert çelikten keskin kılıçların nasıl dövüleceği, sağlıklı ipekböceğinin nasıl yetiştirileceği ve değerli ipeğin nasıl dokunacağı bilgisi orta çağda; canlı renkli fresklerin nasıl yapılacağı, etkili ateşli silahların nasıl imal edileceği, dünyanın öbür ucundaki zenginliğe ulaşmak için engin denizlerin nasıl aşılacağı bilgisi yeni çağda; kimyasal reaksiyonların nasıl gerçekleştiği, buhar gücünden, elektrikten nasıl yararlanılacağı, çok uzaklarla nasıl haberleşileceği bilgisi yakın çağda çok değerliydi. Sonra, elektromanyetiği anlamak, atomu parçalamak, uzay sınırını zorlamak, ses ve görüntü işlemek, genetik kodları çözmek ve daha neler…

Bilgi her çağda değerliydi; şimdiyse çok değerli; gelecekte daha da değerli olacak.

Sahip olan tarafından mümkün olduğunca korunmaya, başkalarından sakınılmaya çalışılsa da, bilgi sahip olana yarar sağlaması için mutlaka kullanılmak durumundadır. Bilgi kullanıldıkça -ister istemez- yaygınlaşır, elde edilebilirliği kolaylaşır, maliyeti düşer, sahip olanın tekelinden çıkar. Birçokları tarafından kullanılan bilgi, yaygınlaştıkça değerini kaybetse de daha başka, yeni ve değerli bilginin oluşmasına yardımcı olur. Bir öncekinin ve birbirinin üzerine eklenerek, daha doğrusu bir öncekinden ve birbirinden yaratılarak çoğalan bilgi geometrik bir artış süreci izler. Bu yüzdendir ki bin sene önceki bir yüzyılda elde edilen bilgi ile son yüzyıl içerisinde elde edilen bilgiyi nitelik ve nicelik bakımından kıyaslamak dahi mümkün değildir.

> Bir arkadaşımın babası yıllar önce, "Evladım," demişti, "Benim dedem bez topla oynarmış, babam da… Ben, meşin topla, tahta oyuncaklarla oynardım; oğlum teneke oyuncaklarla, kardeşi pilli oyuncaklarla oynadı; torunum şimdi bilgisayarla oynuyor."
>
> Benzer şekilde, kırk, elli yüzyıl boyunca taşımacılık hayvanlarla, hayvanların çektiği arabalarla ve kürekli teknelerle yapılıyordu. Sonra, on sekizinci yüzyılın sonuna doğru buharlı tekneler, on dokuzuncu yüzyılın başında buharlı lokomotiflerle çekilen trenler, yirminci yüzyılın başında içten yanmalı motorlarla hareket eden arabalar ve takip eden birkaç onyıl içerisinde uçaklar, hızlı gemiler, hızlı trenler, hızlı otomobiller, daha hızlı uçaklar, roketler… Birkaç binyıl, saatte en fazla kırk, bilemedin elli kilometre süratle gidebilen insanoğlu, son iki yüzyıl içerisinde önceleri saate yüz kilometre sürate ulaştı, şimdi ise saatte bin kilometre sürate bana mısın demiyor. İşte, süratte ulaşılan bu geometrik artışın itici gücü esasında bilgide elde edilen geometrik artıştır ki buna artık artıştan da öte, *sıçrayış* demek daha doğru olur. Böylesi sıçrayışlar hemen her alanda olagelmiştir. Süratteki artış bir bakıma mesafe aşımında kolaylık anlamına gelir ki bu sayede bilginin paylaşımı ve tabii ki çoğalması kolaylaşmaktadır.

Çağımızda *Bilgi Toplumu* olarak tanımlanan modern toplumların bireyleri çok fazla ve yoğun bilgiye ihtiyaç duymakta, kullanmakta ve üretmektedir. Bireylerin birbiriyle, sosyal ve fiziksel çevreleriyle iletişim kurmaları bilgi alışverişi vasıtasıyla olmaktadır. Bilginin üretilmesi, toplanması, kullanılabilir hale getirilmesi, kullanılması, değerlendirilmesi, analizi, sentezi, çoğaltılması, aktarılması, depolanması, korunması günümüzde hemen herkes tarafından yapılan sıradan işlemler haline gelmiştir. Sosyal ve ekonomik etkileri bakımından bu denli güçlü ve çeşitlilik arz eden bir olgunun geometrik süreçte çoğalarak yaygınlaşması, bireysel yaşama ve toplumsal kurumlara derinden nüfuz etmesi kaçınılmazdır.

Bilgi çağında, bilgi dünyasında, bilgi toplumunda yaşayan bireyler, hepimiz, bilgi ile var oluyor, bilgi ile şekilleniyor, bilgiyi kullanıyor ve bilgi üretiyoruz. Elde edilişi, kullanılışı, toplum ve birey üzerindeki etkisi itibariyle farklı disiplinlerde üretim aracı, sermaye, emek, hammadde, rant, kâr, birikim, değer, fikir, yaratıcılık, güç, saygınlık, tecrübe olarak tanımlanabilir bilgi. İnsanoğlu, yaşamak için nasıl ki havaya, suya, besine ve çevresel kolaylıklara ihtiyaç duyuyorsa, modern dünyada var olabilmek için mutlaka bilgiye de ihtiyaç duymaktadır. Modern insan için içtiği su, soluduğu hava kadar değerli ve gereklidir bilgi; yaşam kaynağıdır. Bir nevi yaşam kaynağı olan bilginin diğer kaynaklardan farkı: bir, sınırlı değildir; iki, kullanıldıkça, tüketildikçe azalmaz, aksine çoğalır; üç, daima yenisi üretilir. Var olan bilgi, birçok kişi tarafından kullanıldıkça, her seferinde daha gelişkin şekilde kendini yeniden yaratarak çoğalır.

İnsanoğlunu diğer canlılara üstün kılan en önemli özelliği, ürettiği veya elde ettiği bilgiyi başkalarına ve sonraki nesillere aktarabilmesidir. Ciddi çaba ile üretilen veya elde edilen bilgiye sahip olmak için herkesin, yeni nesillerin benzer çabayı göstermesi (enerji harcaması) gerekmemektedir. Onlar, kendilerine aktarılmış olan bilginin de yardımıyla, enerjilerini yeni bilgi üretmek için yönlendirebilirler. Zihinsel ve fiziksel enerjinin ve kaynakların böyle etkin kullanılması insanlığın gelişimini mümkün kılan en önemli kolaylaştırıcı olmuştur.

BİLGİ HARBİ

Neyle yaşıyorsak onun uğrunda savaşırız.

Uğrunda savaştığımızı tanımalı; ne için, niçin ve nasıl savaştığımız bilmeliyiz.

° Bilgi, Bilgi, Bilgi

Medeniyetin gelişiminde önemli rol oynayan ve insan yaşamının her anını dolduran, günlük lisanda kullanıldığı haliyle *bilgi*, aslında birçok anlamı barındırmaktadır içerisinde: *Bilgi*, *veri*, *enformasyon*, *malumat*, *haber*, *ilim*, *irfan*, *hikmet* gelmektedir akla.

Bilgi, en temel, basit hali ile *veri* (*data*) olarak meydana çıkar; ancak, bu ham haliyle pek anlam ifade etmez. İşlenerek *ne*, *ne zaman*, *nerede*, *kim* sorularına cevap verir hale geldiğinde ise *enformasyon* (*information*) yani *malumat* veya *haber* olur. Biraz daha işlemden geçirilip bir üst düzeye eriştiğinde artık *nasıl* sorusunun cevabını verir hale gelir ki işte bu aşamada gerçek anlamıyla *bilgi* (*knowledge*), *ilim*, *irfan* söz konusudur. Ancak, *niçin* sorusuna cevap bulunduğunda bilgiyi var eden sebep de anlaşılmış olur ki bu aşamada *hikmet* (*wisdom*) doğru bir tanım olur. Bu kavramları tek kelimeyle ifade etmek için gündelik lisanda genellikle "*bilgi*" kullanılmaktadır; ancak bu tek kelime -yerine göre- veri, malumat, bilgi, hikmet gibi anlamları üstlenmektedir.

Mesela, diyelim ki suyu buldunuz. Sudan en iyi şekilde yararlanmak için onu iyi anlamanız gerekir. Nasıl bir şey olduğunu anlamak amacıyla çok soğuk bir kış günü laboratuarda birtakım deneyler yapıyorsunuz. Suyu bir kaba koyuyor ve kabı ateşin üzerine oturtuyorsunuz; kabın içine de bir termometre daldırıyorsunuz. Bakıyorsunuz ki su gittikçe ısınıyor, ısındıkça termometrenin gösterdiği sıcaklık yükseliyor, yükseliyor... Termometrenin gösterdiği sıcaklık değeri 100 ^{O}C'ye geldiğinde yükselme duruyor; su fokurduyor, buhar çıkmaya başlıyor. Bu duruma *kaynama* diyorsunuz. İşte bu 100 ^{O}C sizin için bir veridir (data). Sonra bir başka deney daha yapıyor, su dolu kabı dışarıya, dondurucu soğuğa koyuyorsunuz. Bu kez, termometrenin gösterdiği sıcaklık hızla düşüyor ve 0 ^{O}C'ye ulaştığında duruyor; su buza dönüşüyor. Bu duruma ise *donma* diyorsunuz. Bu 0 ^{O}C bir başka veridir (data) sizin için. Elde ettiğiniz verileri değerlendirip laboratuar defterine, "Su 100 ^{O}C'de kaynar, 0 ^{O}C'de donar" diye yazdığınızda artık malumat, enformasyon (information) söz konusudur. Bu malumatı kullanabilir, saklayabilir veya başkasına söyleyebilir, hatta telgrafla Bilim Araştırma Kurumu'na bildirebilirsiniz. Kurum konuya ilgi duyar, kaynama ve donmanın nasıl meydana geldiğini araştırmanız için sizi destekler ve siz suyun moleküler yapısındaki değişmeyi inceleyip bunun cevabını bulursanız artık malumattan öte bilgi, ilim, irfan (knowledge) sahibisinizdir su hakkında. Sahip olduğunuz bilgiyle yetinmeyip, olur ya, su niçin kaynar, niçin donar, donmasa olmaz mıydı, kaynamasa ne kaybederdik gibi soruların cevabını aradığınızda -bulamasanız dahi- hikmet (wisdom) sahibi sayılırsınız. Hele bir de bu soruların cevabını bulup, suyun niçin kaynadığını veya donduğunu anlarsanız gerçek bir hikmet sahibi olursunuz.

Tabiidir ki bu kavramlar arasında sınırlar keskin değildir; geçişler, kesişmeler vardır.

Türkçemizin zenginliğini görmezden gelerek günlük dilde sadece *bilgi* kelimesini kullandığımızda, karşılık olarak İngilizcede *data*, *information*, *knowledge*, *wisdom* kelimelerini bulabiliriz. Bu derlemenin başlığında *Information Warfare (IW)* karşılığı *Muhaberat Muharebatı (MM)* kullanıldı, zengin dilimize abartılı bir selam olsun diye. Bir farkındalık yaratabilirse ne ala ama asıl amaç konu bütünlüğünü ve anlatım sürekliliğini korumak olmalı. Bu sebepledir ki metin içerisinde günlük kullanımda daha yaygın olan *bilgi* ve *bilgi harbi* deyimleri kullanılmaktadır.

Teknolojiyi -dahası kavramı- icat eden ister istemez dili de geliştiriyor. Mesela, hemen her dilde radyo ve televizyon kelimeleri kullanılırken, Almanlar radyoya *Rundfunk*, televizyona *Fernsehen* derlerdi; hâlâ diyorlar. Yapabiliyorlardı, çünkü kavramın ve teknolojinin geliştirilmesinde önemli katkıları olmuştu. Ama günümüzde bilgisayar teknolojisi ile ilgili herhangi bir Almanca makale İngilizce kelimelerle doludur. Niye?.. Almanca yetersiz bir dil olduğundan mı; Almanlar teknolojide yetkin olmadıklarından mı?.. Herhalde, bilgisayar teknolojisinin öncüsü, kavramların mucidi ve dolayısıyla dilin belirleyicisi Amerika olduğundan olsa gerek.

Bilinen ama gerçekliği müphem hikayedir; yine de hoştur: 1950'lerde Amerikalılar ve Ruslar arasında uzay yarışı tam hızla sürüyordu. Amerikalıların birçok denemesinin başarısızlıkla sonuçlandığı dönemde, Ruslar 1957 ekiminde Sputnik-1 uydusunu yörüngeye yerleştirmeyi başardılar. Bu başarı Amerikalılar üzerinde yeterince sürpriz -daha doğrusu şok- yaratmamış gibi, bir ay sonra içerisinde Laika adlı köpek bulunan Sputnik-2 uydusunu yörüngeye yerleştirdiler. Her ne kadar Laika yörüngede sadece birkaç saat yaşayabildiyse de Rusların bu başarısı dönemin ABD başkanı Eisenhower'e şu soruyu sordurur: "Nasıl oluyor da Ruslar roket teknolojisinde bizden daha ilerideler?" Cevap çok güzeldir: "Efendim, onların Almanları bizim Almanlarımızdan daha iyi." Roket teknolojisinde Almanların öncülüğü ve yetkinliği o zamanlar tartışılmazdı. O tarihte Amerikalılar veri ve malumatla uğraşırlarken, Almanlar bilgi, ilim, irfan sahibiydiler; roket teknolojisinde ve daha birçok konuda.

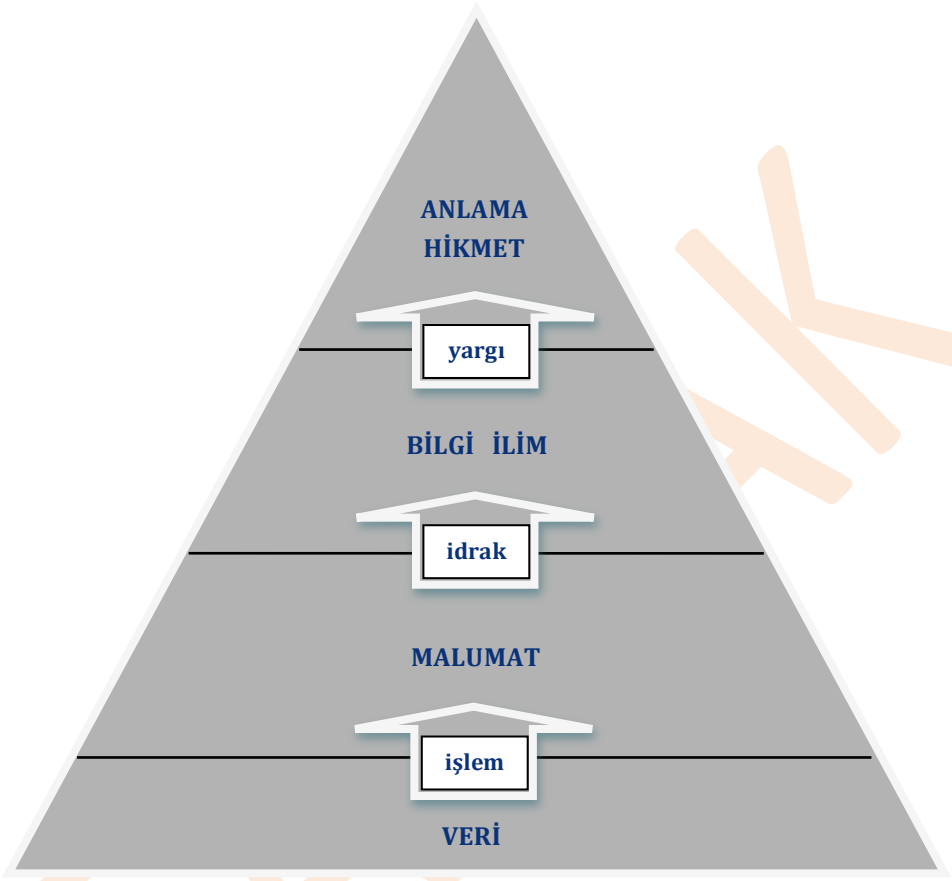
Los Alamos'takilerin geçmişi incelendiğinde, 1940'larda nükleerde de vaziyetin pek farklı olmadığı görülür. Alman kökenli veya geçmişte Almanya'daki araştırma laboratuarlarında çalışmış bilim adamları vurmuşlardır damgalarını nükleerdeki gelişmelere. Eğlenceli anekdottur: Erken soğuk savaş döneminde McCarthy rüzgarının şiddetle esip savurduğu, hatta kavurduğu günlerde, soruşturma komisyonundaki bir senatör şikayet ediyordu, "Anlamıyorum, nasıl oluyor da veriyorlar atomla ilgili sırları şu fizikçilere?" O fizikçilerin arasında atom bombasının babası olarak tanınan Oppenheimer ve daha birçoğu güvenilmez bulunuyorlardı, komünizm sempatizanı oldukları suçlamasıyla.

Konu kavramların ifade edilişinden açılmışken: kavramlar her dilde aynı derecede ayrıntılı ifade edilmemektedir. Misal, *aşk* ve *sevgi*, Türkçemizde ayrı anlamlar yüklü kelimelerken İngilizcede her ikisi için de *love* kullanılmaktadır. Veya Türkçemizdeki *sinir hastası*, *ruh hastası*, *akıl hastası* üçlemesindeki nüans başka hangi dilde var? Buradan yola çıkarak İngilizcenin anlam fakiri olduğu sonucuna varabilir miyiz? Hayır, varamayız; varmamalıyız. Muhakkak ki farklı kültürlerde kavramların çeşitliliği farklı olabilir. Toplumların kavramları nasıl ve ne kadar içselleştirdikleri ve nasıl anlamlandırdıkları farklı olabildiği için bu kavramları dillendiren kelimelerin anlam çeşitliliği de farklı olabilir. Bu yüzden, transistör veya kübizm karşılığı Türkçe kelime arayışlarını garipserim.

Her daim kıymetli ve uğrunda savaşmaya değer olan bilginin değişik şekilleri arasında hiyerarşik ilişkiden söz edilebilir.

Bilginin değişik şekilleri arasındaki bilişsel hiyerarşi, bilgi piramidi veya üçgeni şeklinde gösterilebilir:

> İrfan, ilime değil; ilim, irfana itibar eder.



> [Birinci bölümü derlerken bahsini etmiş olduğum hiyerarşik ilişki, daha sonra ikinci bölümü derlerken yararlandığım ABD bilgi harekâtı doktrini dokümanında neredeyse aynı şekil ve tanımla karşıma çıkınca sevindim. Demek ki doğru yoldayım. Pek girilmemiş bir coğrafyada dolaşırken işaret taşlarına rastlamak güven veriyor insana.]

Bilgi, *veri* halindeyken pek anlam ifade etmez; ancak işlenip *malumat* haline geldiğinde anlam ve değer kazanır. Doğruluğu test edilen, değerlendirilen ve kabul edilen malumat ise artık *bilgi* veya *ilim* olmuştur. Bu geçiş *idrak* vasıtasıyla olur.

> Bu noktada bilgi veya ilim ile inanç arasındaki farkı vurgulamakta yarar var. Denenmemiş, değerlendirilmemiş *inanç*, ne kadar yaygın olursa olsun, *gerçek* değildir. İnanç, nihayetinde bilgi değil bir düşünce şeklidir ki herhangi bir zamanda yanlışlığı ispatlanabilir. [Burada, dinî veya başka inanışları değil, İngilizce *opinion* karşılığı olan fikir, düşünce, zan anlamında olan inanç kastedilmektedir.]

° Bilgi Ortamının Güvenliği

Bilgi ortamı, bir başka deyişle bilgi uzayı (information space), bilginin dolaşımda olduğu ortamdır. Dolaşımdan kasıt: elde edilmesi, iletilmesi, depolanması, işlenmesi ve kullanılmasıdır.

Günümüzde bireyin, toplumun, hatta devletin gelişiminde bilgi ortamı en belirleyici etkendir; dolayısıyla, güvenliği önemlidir. Bilgi ortamı iki tehlike içermektedir: bir, bilgi kaynaklarının izlenmesi, ele geçirilmesi (espiyonaj); iki, düzenin bozulması için bilgi yayılması (dezenformasyon). Günümüzün teknolojik imkânları ile bilgi akışının sınır tanımıyor olması bir yandan bilgi ortamını hızla genişletirken öte yandan tehlikelerini gittikçe ciddi hale getirmektedir.

Bilgi ortamının güvenliği sosyal anlamda da bir güvenlik meselesidir. Bir tarafta bireylerin, kurumların ve devletin hakları, mahremiyeti ve bütünlüğü söz konusuyken, diğer tarafta bunları kolayca ihlal etmeye imkân tanıyan teknoloji ve kolaylıklar bulunmaktadır. Ve ayrıca, kamuoyunu yönlendiren yazılı ve görsel medya, sosyal medya, internet, sinema, edebiyat, bilgisayar oyunları vesaire…

> Eğitim de bilgi ortamını oluşturan en temel ve önemli unsur olarak değerlendirilebilir.

Bilgi ortamını manipüle etmekle bireylerin toplumsal farkındalıkları, algıları, kararları etki altına alınabilir ki bu durum nihayetinde ulusal güvenliği etkiler hale gelebilir.

> Ulusal güvenlik tabiri, milli güvenlik ile özdeş olduğundan çoğu kişi bu meseleyi resmi jargonda devletin güvenliği olarak algılayabilir; halbuki burada söz konusu olan **ulusun güvenliği**dir. Devletin güvenliği bunun bir alt kümesi olarak değerlendirilebilir.

° Eski Paradigma

Savaş stratejistleri, iki bin beş yüz yıl önce de, şimdi de tüm savaşların kazanılmasında düşman ve ortam hakkında bilgi sahibi olmanın elzem olduğunu vurgulamışlardır. Milattan beş yüz sene evvel Çinli general Sun-Tzu tarafından konulan stratagemler ile on dokuzuncu yüzyılda Prusyalı general von Clausewitz tarafından konulanlar temelde pek farklı değildir. İkisi de düşman ve ortam hakkında bilgi sahibi olmanın önemini vurgular. Sun-Tzu, "Düşmanını tanı!" der. Çok bilinen, klasik, *Savaş Sanatı* adlı eserinin bir bölümünü tamamen casusluk üzerine ayırmış olmanın ötesinde, diğer bölümlerde de düşman ve savaş alanı ile ilgili bilginin savaşı kazanmak için ne derece gerekli olduğunu vurgular. Von Clausewitz ise savaşı yöneten komutanın karmaşık ve güvenilirliği şüpheli bilgi ile donatılmış olduğunu, dolayısıyla bilginin güvenilir hale getirilmesi gerektiğini söyler. Her halükarda, gerek muharebe, gerekse harbi kazanmak için bilgi üstünlüğünü elde etmek ve elde tutmak gerekir.

Pek tabiidir ki savaşta bilgi üstünlüğünü elde edebilmek, barış zamanında da bilgi üstünlüğüne sahip olmayı gerektirir.

> La Fontaine'in meşhur, *Ağustosböceği ile Karınca* fablını hatırlayalım.

Eski paradigmada bilgi harbi, süregelen veya çıkması muhtemel savaşı kazanabilmek için düşmanın durumu ve savaş ortamı hakkında doğru ve yararlı bilgiye sahip olmaya ve düşmanın benzer bilgiyi elde etmesini önlemeye yönelik, daha ziyade askeri bir faaliyetti. Bu bakış açısı askeri bakımdan hâlâ geçerlidir; ancak, Bilgi Çağı olarak adlandırılan günümüzde bilgi harbine yeni bir bakış açısı ile yaklaşmak daha doğru olur.

° Yeni Paradigma

Bilgi, çoğu zaman, sahip olanı -olmayana nazaran- avantajlı konuma getirir. Bu yüzdendir ki sahip olmayan onu elde etmeye, sahip olan ise elindekini korumaya çalışır. Bilgi veya malumat veya enformasyon harbinin (Information Warfare - IW) temeli işte bilginin hemen her halinde, her seviyesinde yürütülen bu mücadeledir.

Doğadaki yaşam kaynakları, madenler ve fosil yakıtlar gibi *sınırlı* iken veya besin kaynakları gibi *aritmetik* artarken, insanoğlu -doğal felaketler ve salgınlar müstesna- *geometrik* olarak çoğalmaktadır. Dolayısıyla, bir süre sonra kaynakların yetmezliği durumu kaçınılmaz olur ki tarih boyu süregelen çatışmaların temel sebeplerinden biri -belki de esası- budur. Bilgi ise, kaynakların aksine, geometrik bir artış süreci izleyerek çoğaldığından, eski çağlarda değilse bile modern dünyada her zaman herkese yetecek kadar, hatta daha fazla bilgi mevcuttur. Geometrik olarak çoğalan insan topluluğu, tamamen sınırlı olan veya ancak aritmetik olarak artabilen kaynakları tüketmekle bir bakıma kendini de tüketmekte, sonunu hızlandırmaktadır. Bilgi, işte burada yardımcı olmaktadır. Geometrik olarak çoğalan, daima yenilenen, hep daha gelişkini üretilen bilgi sayesinde kaynakların artış hızlandırılmakta, sınırları zorlanmakta, üretim ve tüketim dengesi iyileştirilmekte, topyekun verim -dolayısıyla fayda- artırılmakta ve böylece insanoğlunun kaçınılmaz sonu ötelenmektedir.

> İlkçağda bilinen yöntemlerle tarımsal üretim yapılagelseydi bugün acaba en fazla kaç milyon kişi beslenebilirdi? Petrolü hâlâ Albay Drake'in yöntemiyle çıkarıyor olsaydık şimdi acaba kaç kişi ondan yaralanabilirdi? Peki ya hastalıkları ortaçağdaki yöntemlerle iyileştirmeye çalışıyor olsaydık acaba siz bunları okuyacak kadar hayatta kalabilir miydiniz; ben yazabilir miydim?

Bilgi harbinin en ilkel ama temel hali bilgiyi ele geçirmek ve eldeki bilgiyi muhafaza etmek şeklinde ortaya çıkmakta; ancak, ele geçirmenin ve muhafaza etmenin ötesinde, bilgiyi yönetmek çok daha etkili sonuçlar veren bir işlem olarak öne çıkmaktadır. Bilgi, doğası gereği, (olumlu anlamda) *yönetilebilir* olmakla birlikte, (olumsuz anlamda) *manipüle edilebilir* bir olgudur. Bu yüzden, bilginin amaca uygun, etkin şekilde yönetilmesi veya manipülasyonu veya manipülasyonunun önlenmesi fazlasıyla önemli, acil bir ihtiyaç haline gelmektedir.

İşte bu yeni paradigmada, bilgi -eskiden olduğu üzere- sadece sahip olana üstünlük kazandıran bir araç olmanın ötesinde, farklı ve önemli başka kimlikler taşımaktadır.

Birinci kimlik: Taktik anlamda muharebenin, stratejik anlamda harbin sürdüğü ortamı oluşturmaktadır bilgi. Savaş artık karada, denizde, havada, cephede, sektörde değil, bilgi ortamı üzerinde yürütülmektedir. Çeşitli seviyede, çeşitli formdaki bilginin yanı sıra,

bilgiyi üreten, aktaran, taşıyan ve muhafaza eden donanım ve yazılım bilgi harbinin ortamıdır.

İkinci kimlik: Bireyin günlük yaşamına ve toplumun kurumlarına derinlemesine nüfuz etmiş olan bilgi, aynı zamanda bir silah haline gelmiştir. Bireyin, toplumun, devletin sivil ve askeri kurumlarının, sınai ve ticari işletmelerin bu denli yoğun bilgi ağı ile sarılmış ve bilginin kolaylıkla yönetilebilir veya manipüle edilebilir olduğu gerçeği göz önüne alındığında, bu silah en maliyet etkin araç olarak öne çıkmaktadır.

Bilginin bir harp vasıtası, bir silah olarak değerlendirilmesi birçok sebepten ötürüdür:

İLERİ DERECE NÜFUZ: (PENETRATION)	Bilgi ihtiyacı, kullanımı ve üretilmesi bireyin ve toplumun yaşamına ve kurumların işlevine ileri derecede nüfuz etmiştir.
HASSAS OPERASYON: (ACCURACY)	Belirli bir kişi, toplumun bir kesimi, herhangi kurumun bir organı veya işlevi üzerinde etkili olabilecek hassasiyette operasyon yapılabilir.
GİZLİLİK, YANILTMA: (ANONYMITY, IDENTITY DECEPTION)	Operasyonu yapan taraf kimliğini tamamen gizleyebilir veya yanıltıcı kimlik kullanabilir.
UYARLANABİLİRLİK: (ADAPTABILITY)	Değişen koşullara göre çabucak uyarlanabilir ve daima güncel tutulabilir. Ekipman sürekli yenilenmekte ve personel eğitimi güncellenmektedir.
UYGULANABİLİRLİK: (APPLICABILITY)	Kolay temin edilebilen çok sayıda personel ve ekipman vasıtasıyla uygulanabilir.
ELVERİŞLİLİK: (AVAILABILITY)	Ekipman mevcut veya kolay temin edilebilir; personel yeterli temel eğitim almış durumdadır. Halen başka amaçla kullanılmakta olan mevcut ekipman ve personel çok kısa süre içerisinde bilgi harbine yönlendirilebilir.
MALİYET ETKİNLİK: (COST EFFECTIVITY)	En düşük maliyetle en etkin sonucu almak mümkün olmaktadır.
	MORE BANGS FOR LESS BUCKS

Bu sebeptendir ki bugüne dek konvansiyonel harbin bir destek unsuru olarak yararlanılmakta olan Bilgi Harbi, bundan böyle harbin ana unsuru haline gelmiştir; dahası, harbin yürütüldüğü ortamı da artık bilgi oluşturmaktadır.

> Ülkesinin siber altyapısının güvenli hale getirilmesi ile ilgili olarak 2009 yılında Beyaz Saray'da yapmış olduğu konuşmada, ABD Başkanı Barack Obama'nın konu ile ilgili yorumu bilgi harbinin günümüz dünyasındaki ehemmiyetini çarpıcı şekilde ifade etmektedir.

> Başkan Obama, günümüzde bilginin üretildiği, işlendiği, muhafaza edildiği, aktarıldığı bilgisayarlar ağının oluşturduğu siberuzaya (cyberspace) atıfta bulunarak, diyor ki, "Siberuzay gerçektir. Bilgi Çağının büyük ironisi, yaratmamızı ve yapmamızı mümkün kılan teknoloji aynı zamanda parçalamamıza ve yıkmamıza da imkan veriyor."

Günümüzde ve yakın gelecekte hem harbin yürütüldüğü ortam, hem de çok etkili bir silah olan bilgi, bu çifte kimliğiyle planlamacıların, stratejistlerin ve politikacıların (hem policy makers hem de politicians anlamında) birinci derece ilgi alanındadır.

° Bilgi Harbinin Çok Kısa Tanımı

Bilgi Harbi (IW), genel tanımıyla, bilgi üzerinde ve/veya bilgiyi kullanarak yürütülen harptir.

Daha belirgin olarak, *Bilgi Harbi*, kendi sahip olduğu bilgiyi, bilgi sistemlerini, bilgi tabanlı süreçleri muhafaza etmek ve hasmın sahip olduğu bilgi, bilgi sistemleri, bilgi tabanlı süreçler üzerinde etkili olmak şeklinde tanımlanabilir. Daha popüler tanımla, *siber savaş* (*cyber warfare*) olarak da adlandırılmaktadır.

> Bilgi Harbi için birçok tanım bulunabilir ilgili kaynaklarda. Bu tanımlar oldukça ayrıntılıdır; ancak, bu derlemede tüm tanımlardan söz etmek mümkün olmamıştır, ilgilenenler bu kaynaklara başvurabilirler.

Ancak, tanımı nasıl yapılırsa yapılsın, özellikle vurgulanması gereken husus şudur ki bilgi harbi, sınırlı muharebeden topyekun harbe kadar yayılan çok geniş bir yelpazede değerlendirilmelidir.

° Bilgi Harbinin Çok Kısa Tarihçesi

Bilgi ile birlikte bilgi harbi de geçmişten bu yana var olagelmiştir. Sahip olunan bilgi değerli olduğu için her daim muhafaza edilmek istenmiş; elde olmayan bilgi ise elde edilmeye çalışılmıştır.

> *Yalan*, insanlık tarihinin olmasa da bilgi harbinin ilk ve en önemli buluşudur. Belki de buluştan öte, içgüdüdür. Bilgi harbi, her ne kadar teknolojik çağrışım yapsa da bir bakıma içgüdüsel başlamıştır

Tarım toplumlarında da, sanayi toplumlarında da, bilgi toplumlarında da bu böyle süregelmiştir; ancak harp edenlerin ve harp araç gereçlerinin niteliği değişmiştir. Tarım toplumlarında, çiftçiler aynı zamanda mevsimlik askerlerdi; savaşın amacı tarım arazilerinin ele geçirilmesiydi. Sanayi toplumlarında ise seri imalat silahlar ve sebep oldukları kitle imhası söz konusuydu. Bilgi toplumu olan çağımızda ve yakın gelecekte bilgi savaşçıları gerekli donanım ve yazılım sayesinde düşmanın bilgi altyapısına ve bilgi varlıklarına saldırarak çok daha etkili sonuçlar alacaklar.

° Neokorteks Harbi

Bilgi harbinin birçok formu aslında yüzyıllar boyu kullanılagelen, kadim olduğu kadar doğal savaş yöntemlerinin modern teknolojiye uyarlanması ve modern kavramlarla yeniden tanımlanmasından öte bir şey değil. Neokorteks harbi (Neocortical Warfare) de öyle...

> Nörologların ve ilgili uzmanların müsamahasına sığınarak kısa bilgi vermek isterim. İnsan beyni, evrimsel olarak üç ana bölümden meydana gelmiştir: beyin sapı, limbik beyin, neokorteks. Beyin sapı, omuriliğin hemen ucunda yer alan, sürüngenler kadar ilkel hayvanlarda dahi bulunan, en temel yaşamsal işlevleri yerine getirmemizi, yaşamsal tepkiler vermemizi sağlayan ve sürüngen beyin olarak tabir edilen bu bölüm nefes almamızı, kalp ritmimizi ayarlamamızı sağlar. Sürüngen beyni çevreleyen limbik beyin duygularımızı idare eden bölümdür. Beslenmek, dövüşmek, kaçmak, üremek gibi yaşamsal fonksiyonların yanı sıra ödüllendirilme veya cezalandırılmayı hissetme, eş seçme, bağlanma, toplu göç ve önderi izleme, zayıf olana saldırma, avlanma, oynama gibi sosyal eylemleri yönlendirir. En dışta yer alan neokorteks ise davranışlarımızı, düşüncelerimizi, algılarımızı ve karar mekanizmamızı idare eden bölümdür. Düşünmemizi, anlamamızı, algılamamızı, yaratmamızı, hayal etmemizi, seçim yapmamızı, organize olmamızı, değişime uyum sağlamamızı mümkün kılar. Neokorteksin beynin diğer bölümlerine oranı, o yaratığın düşünsel bakımdan ne denli gelişmiş olduğunun bir göstergesidir. (Evrimsel olarak en son gelişen, en yeni bölüm olduğundan, neo- önekini almıştır.)
>
> İnsan beyninin yaklaşık yüzde seksenini neokorteks oluşturduğu için, *neokorteks harbi* yerine *beyin harbi* de diyebiliriz. Nihayetinde algılayan, düşünen, değerlendiren, karar veren ve uygulayan organdan bahsediyoruz. Beyin harbi, sırf bu tanımla bile geleneksel harpten farklı konumlandırmaktadır kendini. Geleneksel harpte harbeden vücuttur, hedef de... Düşmanın vücudu işlevini yapamaz hale gelir (yaralanır, ölür) veya galip tarafın yararına kullanılmak üzere esir alınır. Beyin harbinde ise harbeden de hedef de beyindir. Beyin işlevini yapamaz hale getirilir veya esir alınır.

Neokorteks, duyuların işlendiği, algıların oluştuğu, kararların alındığı, üst düzey zihinsel faaliyetin sürdürüldüğü bölümdür beyinde. İnsanoğlu, neokorteks sayesinde bir araya gelme, organize olma becerisini geliştirmiştir ve bu beceri sayesinde düşmanına karşı savaşmak üzere organize olabilir. İnsanoğlunun savaşma yetisi, sürüngen beyin ve limbik beyinin çok ötesinde, neokorteks beyin tarafından geliştirilen ve yürütülen bir faaliyettir.

> Tabii ki içerisinde limbik ve sürüngen beyin tarafından yönetilen unsurlar da bulunmaktadır. Kim bilir; belki bir gün limbik harbe geri döner insanoğlu.

Siyaset, zihinsel bir faaliyettir; hem uygulayan hem de uygulanan bakımından. Siyasetin amacı, bireyin kendi halinde almayacağı kararları almasını, göstermeyeceği davranışları göstermesini sağlamaktır. Bunun için "güç" gerekir. Güç, bir bakıma, etkilenmek istemeyenleri etkileme yetisidir. Bu yetinin zorlayıcı unsurlar içerdiğine inanılır ki genellikle doğrudur. Geleneksel anlamda savaş, bu zorlayıcı unsurların kullanıldığı, zorlayıcılığın öne çıktığı bir etkileme şeklidir. Savaşın amacı, düşmanın sizin istediğinizi tercih etmesini sağlamak; bir başka ifadeyle, düşmanın iradesini bastırmaktır

Amaç düşmanın iradesini bastırmak ve istenen şekilde davranmasını temin etmek olduğunda düşmanı sadece bir sistemler topluluğu değil, irade sahibi organizmalar olarak değerlendirmek daha doğru olur. Bugüne dek düşmanın iradesini zayıflatmak için zorlayıcı yöntemlerin ve silahların kullanıldığına aşina olduğumuzdan zorlayıcı yöntemler ve silahlar üzerine yoğunlaşmaktayız. Halbuki, iradeye yoğunlaşmak gerekir, iradenin oluştuğu beyin bölgesine. İşte, neokorteks harbinin esası budur.

Düşmanın iradesini yenmenin, ona boyun eğdirmenin birçok yolu, yöntemi olabilir. Tabii ki en az maliyetli olan tercih edilmeli. (Doğal ekonomi bunu gerektirir.) Ne de olsa, hem yenilen hem de yenen taraf için fiziki harp oldukça maliyetlidir. Geleneksel fiziki harp için çeşitli silahlar geliştirilir ki bu önemli maliyet unsurudur. Öte yandan, yenilen tarafın iradesi yenen tarafa karşı bilenir ve bu durum ileride sorunlara yol açabilir. Bu sebepledir ki birçok savaşçı usta ve teorisyen, savaşı kazanmada karşı tarafın iradesinin bastırılmasının önemini vurgulamışlardır.

> Hiç savaşmadan düşmana boyun eğdirmek mükemmeliyetin zirvesidir.
>
> Sun Tzu

Neokorteks harbi, çok düşük maliyetle, hatta neredeyse hiç savaşmadan düşmanı alt etmenin yolunu açabilir. Bu açıdan bakınca ciddi olarak değerlendirilmesi gereken bir harp sanatıdır. Neokorteks harbi, düşmanın önderliğinin algısını, bilincini ve iradesini etkileyerek, düşman organizmaları yok etmeden onların davranışlarını denetim altına alan harp şeklidir. Bunu yapmak için düşmanın OODA çevrimine girmeye çalışır. (OODA: observation, orientation, decision, action - izleme, yönlendirme, karar verme, eylem)

Savaş, organize kavgadır ama başladıktan sonra gittikçe daha az organize, hatta kaotik bir hal alır. Bu yüzden, savaşlar başlamadan daha kolay sonlandırılabilir. (Fiziki evrende anlamsız gelen bu cümle neokortikal düzeyde anlamlıdır; çünkü, fiziki olarak henüz başlamamış olan savaş zihinlerde çoktan başlamış veya başlamak üzeredir veya tohumları atılmaktadır.)

Neokortikal boyutta yürütülen savaşta düşmanın önderlerinin algıları, hayalleri hatta rüyaları veya kâbusları etki altına alınarak düşmanın savaşmamayı tercih etmesi ve teslim olması sağlanır. Ancak bu demek değildir ki neokorteks harbi pasif bir yöntemdir ve tek amaç muharebeyi engellemektir. Fiziki boyutta atılan ses getirici adımların neokortikal boyutta yarattığı sonuçların birçok örneği vardır tarihte. (Bu bakışla diyebiliriz ki Hiroşima ve Nagazaki'ye atılan bombaların fiziki boyuttaki yıkıcı etkilerinde daha ziyade neokortikal boyutta etkisi olmuştur.)

Neokorteks harbinin dört belirgin karakteristiği vardır: Öncelikle kabul etmek gerekir ki yarışma, çatışma ve çözüm insan doğasının gereğidir; çatışma, olağan dışı değil aksine olağan bir durumdur; asla sona ermez. (Biri bitse bir diğeri başlar.) Dolayısıyla güvenlik, silahlanmanın sonucu değil; maalesef silahlanma, güvensizliğin sonucudur. Güvensizlikse zihinde (neokortekste) oluşmaktadır.

İkincisi, düşman bize karşı sürdürmektedir neokorteks harbini; farkında olsak da, olmasak da. (Genellikle farkında değilizdir.) Dili, görüntüyü ve bilgiyi kullanarak

zihinlere saldırmakta, morali zayıflatmakta, iradeyi zorlamaktadır. Durum böyle olduğunda zihnen yetersiz, psikolojik bakımdan zayıf yöneticiler, önderler olmamalı yönetimde.

Buna karşın, düşman üzerinde şiddet içermeyen etkiyi sürdürmeye daha fazla ağırlık vermek, kaynakları buna göre yönlendirmek gerekir. Amaç, onun neyi, niçin seçtiğini anlayacak ve yönlendirecek kadar düşmanı iyi tanımak olmalı. Düşmanın dilini, sentaksını, temsil sistemlerini iyi bilmek, anlamak gerekir ki onun izleme-yönlendirme-karar-eylem (OODA) çevrimine sızmak ve müdahale etmek mümkün olsun. (Burada bahsi edilen "temsil sistemleri" kişilerin bir olguyu algılamada kullandıkları duyuları, sembolleri ifade eder.)

Dördüncüsü, neokorteks harbe destek olacak, neredeyse limbik düzeyde basit, sert ve çabuk hareket edebilen hançerimsi kuvvetler hazır bulundurulmalı. Neokorteks etkiyi pekiştirmek için düşmanın dünyasında zaman zaman sürpriz, şok hatta terör yaratmak gerekebilir. Bu türden, küçük ama etkili saldırıların olabileceği ihtimali asla göz ardı edilmemeli.

> Neokorteks harbi bir bakıma psikolojik harekât, aldatma, istihbarat, halkla ilişkiler gibi geleneksel harp unsurlarının ve kadim öğretilerin bir başka başlık altında yeniden değerlendirilmesi, organize edilmesi ve uygulanmasıdır. Hem uygulayıcı olma hem de maruz kalma bakımından dikkate alınmasında yarar vardır.

BİLGİ HAREKÂTI - (IO)

Bilgi harbinin yürütülmesinde kullanılan beceriler, yöntemler, eylemler *Bilgi Harekâtı* veya *Bilgi Operasyonu (IO)* olarak adlandırılır ve genellikle malumat, haber, enformasyon (information) üzerinde etkili olacak şekilde yürütülür.

> Bilgi Harbi (*Information Warfare - IW*) ile Bilgi Harekâtı (*Information Operations - IO*) arasında belirgin fark aramak, bulmak kolay değil; zaten pek yok da.

Üretilen veya elde edilen bilgi, yararlı olması için başkaları ile paylaşılmalı, başkalarına aktarılmalı, ileride kullanılmak üzere muhafaza edilmelidir. Bilgi, daha ziyade malumat, haber, enformasyon seviyesinde iken ele geçirilir; çünkü bu aşamada bilgi aktarımı, bilginin bir yerden başka bir yere iletilmesi söz konusudur ve ortam dışa açık, nispeten güvensiz haldedir. Tabii ki veri (data) veya bilgi (knowledge) halindeyken bilginin ele geçirildiği veya manipüle edildiği durumlar da söz konusu olabilir.

Bilginin (olumlu) yönetilmesi ne denli önemli ise, (olumsuz) manipülasyonunun engellenmesi de o derece hayati önem taşımaktadır. Dolayısıyla, bilginin ele geçirilmesi ve değerlendirilmesinin yanı sıra değiştirilmesi, manipüle edilmesi de bilgi harekâtının çerçevesi içerisinde değerlendirilmektedir.

Bilgi harekâtının amacı bilgi üstünlüğünü elde etmek ve muhafaza etmektir ki sonuçta daha doğru karar almayı ve etkin uygulamayı sağlar. Bilgi Harekâtı (IO), gerek harpte gerek sulhta, farklı kademelerde, muhtelif hedeflere yönelik, çeşitli yöntemlerle yürütülmektedir. *Kriptoloji*, *Elektronik Harp (EW)*, *Ağ Merkezli Harp* (*Network Centric Warfare*), *İstihbarat* (*Intelligence*), *Propaganda*, bu amaçla kullanılan önemli araçlardır.

° Kamuflaj

Kamuflaj, fiziksel bir yöntem olması sebebiyle her ne kadar bilgi harbi kapsamında değerlendirilmese de gerçekte belki en eski bilgi harbi yöntemidir. Her türlü bilgi üzerinde yürütülen her türlü işlem bilgi harbinin kapsamında değerlendirilir. Nihayetinde, görsel bilginin saklanması veya değiştirilmesi ve bu yolla yaratılan algı söz konusudur. Görsel bilgi dahil birçok türde bilgi kamufle edilebilir. Elektronik harp vasıtası olarak düşmanın radarını yanıltmak amacıyla kullanılan maketler (decoy) dahi bu çerçevede değerlendirilebilir.

Aslında, elektronik veya diğer otomatik algılayıcıları, işlemcileri ve karar vericileri yanıltmak çoğu zaman daha kolaydır. Bu sebepledir ki kamuflaj her ne kadar zamanı geçmiş bir uygulama olarak görülse de layıkıyla uygulanması hayli zordur; günümüzde ve gelecekte *yanıltma*, *aldatma* gibi başka tanımlar altında sürdürecektir varlığını.

İkinci Dünya Savaşı sürerken ABD'de birçok askeri tesis ve fabrika kamufle edilmişti.

Aşağıda fotoğrafını gördüğünüz kır manzarası hiçbir bombardıman uçağının ilgisini çekmezdi.

Halbuki, gerçekte şu tesis vardı orada:

California eyaletindeki, Lockheed Burbank Uçak Fabrikası

Gözlerine inanmakta zorluk çekenleri ortadaki üç küçük beyaz bina, öndeki küçük beyaz bina ve pistin izi ikna edebilir.

° Kriptoloji

Kriptoloji, matematiktir; başka giz aramaya gerek yok ardında.

Kriptoloji, en basit tanımıyla, gizleme ilmidir; gizlenen ise bilgi, malumat, enformasyon olur. *Kriptoloji*, yani *bilgi gizleme ilmi*, iki bileşenden meydana gelir: *kriptografi (gizli yazma)* ve *kriptanaliz (giz çözme)*… (kripto analiz diyenler de vardır.) Kriptografi, aynı zamanda *şifreleme* olarak da bilinir ki gizliliği sağlayan *anahtar*, çoğu zaman *parola* veya *şifre* olarak adlandırılır. Şifreleme karşılığı, *encoding (kodlama)*, şifre çözme için *decoding* ifadeleri de çoklukla kullanılmaktadır. Bu iki ana bileşen -kriptografi ve kriptanaliz- haricinde, bilgiyi açık ortam içerisinde saklama ve saklanan bilgiyi açığa çıkarma anlamına gelen steganografi ve steganaliz de kriptolojinin ilgi alanına girer.

Kriptoloji, kriptografi, kriptanaliz karşılığı *gizbilim*, *gizyazım*, *gizçözüm* tercih edilebilir. Ben ki bilgisayara bile zor alıştım; bu derlemede genellikle *kriptoloji*, *kriptografi*, *kriptanaliz* kelimelerini kullanmayı tercih ettim. Tercih sizin…

Bilgi var olduğu sürece kriptoloji de var olmuştur, değerli bilgiyi korumak veya açığa çıkarmak için. Yüzyıllardır birileri bilgiyi korumaya, gizlemeye çalışırken, birileri de gizleneni açığa çıkarmaya çalışmakta. Bu amaçla sanatın, bilimin, teknolojinin çeşitli disiplinlerinden fayda umulmuş; bazılarında bulunmuştur da. Ancak gerçek şu ki kriptoloji bir matematik uygulamasıdır aslında.

Gizli şifrelemede açık bilgi (P), şifrelenmiş bilgi (C); şifrelemeyi ve şifreyi çözmeyi sağlayan anahtar (K) ve onun fonksiyonu olan algoritma (f) söz konusudur. Matematiksel olarak şöyle ifade edebiliriz:

Şifreleme $\mathbf{C=f_K(P)}$ Şifreyi kırma $\mathbf{P=f_K^{-1}(C)}$

Matematik formüllerin yanı sıra, zaman zaman eğlenceli benzetmeler de kullanılır, kriptolojide. Her zaman bir *A* (*Alice*) ve *B* (*Bob*) vardır birbiriyle haberleşen. Bazen, *C* (*Carol*) de katılır aralarına. Öte yanda, meraklı *E* (*Eve*) *-the eavesdropper-* kulak kabartır diğerlerine. Bundan rahatsız olan Alice, Bob ve Carol, aralarındaki haberleşmenin Eve tarafından ele geçirilmesini engellemek için kriptografiden yararlanırlar. Buna karşın Eve, kriptanalizden yararlanır. İşte bu mücadele kriptolojinin ana temasıdır. Gökten üç elma düşer, biri Alice'in, biri Bob'un, biri Carol'ın başına; Eve ise bu elmaları yakalamaya çalışır. Mesele; kim yiyecek elmaları?..

°° Steganografi ve Steganaliz

Mutlaka daha eski uygulamalar vardı, ancak Herodot tarihinde sözü edildiği haliyle kriptolojinin bilinen en eski örnekleri daha ziyade *steganografi* uygulamalarıydı. Steganografi, saklı yazı anlamına gelir -ama saklanan mesaj her zaman yazılı olmayabilir.

Steganografi yerine stenografi demeyelim, diyenleri uyaralım.

Herodot tarihinde anlatılan Perslerle Ispartalılar arasında M.Ö. 500 civarında yapılan savaşlarda steganografi uygulamalarına rastlanır. En bilineni: Perslerin idaresi altındaki Miletlileri isyana yönlendirme mesajını onlara iletmek için Isparta kralı Demaratus'un

bir habercinin saçlarını kazıtıp, mesajı kafasına yazdırması ve saçları uzadıktan sonra haberciyi Milet'e göndermesidir.

> Tüm bilgi operasyonu uygulamalarında maliyet etkinlik ve zamanın doğru kullanılması çok önemlidir. Altı ay sonraki bir operasyon için habercinin saçlarının uzamasını beklemek veya ertesi günkü operasyonu haber vermek için düşmanın elindeki imkânlarla bir haftada çözebileceği basitlikte bir şifre kullanmak hiç de yanlış değildir.

Görünmez mürekkep, hatta limon suyu ile yazılan mesajlar; haşlanmış yumurtanın kabuğuna yazıldığında görünmez olan ama kabuk kırıldığında, haşlanmış yumurta beyazı üzerinde okunur olan mesajlar; bir yazı veya fotoğrafın çok ama çok küçültülerek nokta (microdot) haline getirilip bir kitabın bir yerine yerleştirilmesi; televizyondaki mülakatta göz kırparak Mors alfabesiyle mesaj vermek çok bilinen yöntemlerdir.

Şimdilerde ise şifrelenen mesaj ile alakası olmayan bir sayısal görüntü iletilirken her pikseli oluşturan sayısal bilgi bloğunun en önemsiz birkaç biti saklı mesajı iletmek amacıyla kullanılabilir. Görüntüyü izleyen farkı anlamaz ama iletilen mesaja basit teknoloji yardımıyla kolaylıkla ulaşılabilir. Saklı iletilen mesaj mutlaka yazı veya rakam olmayabilir, sayısal formda her türlü bilgi, resim veya ses bu şekilde iletilebilir.

> Bir Monet resmine çok şey saklanabilir.

Steganografinin bir önemli avantajı, bilginin yanı sıra gönderenin ve alanın kimliğinin de salklanabilmesidir. Mesela, İkinci Dünya Savaşı boyunca İngiltere'den yapılan radyo yayınlarında saklı mesajların muhataplarını kim bilebilirdi, muhatapların kendilerinden başka?

Steganografi, her ne kadar bir nevi ilüzyon gibi görünse de, modern yöntemlerle yapıldığında ciddi matematik gerektirir. Saklanan (steg) bilginin açık ortam (medium) içerisinde ne şekilde saklanacağı, saklamadan evvel steg bilginin hangi formda olması ve saklama ortamının özellikleri gibi birçok parametrenin yer aldığı modelleme teknikleri uygulanır. Ayrıca, eğer kırılması zor bir şifrelemeden geçirilmişse, steg bilgi saklandığı ortamdan ayrılsa bile bilgiye ulaşmak kolay olmayabilir. Bu yüzden, genellikle steganografi ve kriptografi birlikte uygulanır.

> Kriptografik yöntemle şifrelenmiş bir metin daha sonra microdot (nokta) haline getirilip bir turizm broşürünün içerisindeki tanıtım yazısının üçüncü paragrafındaki beşinci cümlenin noktası halinde normal posta ile gönderildiğinde, tespit etmek hayli zordur.

°° Kriptografi ve Kriptanaliz

Kriptoloji (gizbilim) konu olduğunda, temel ögeleri kriptografi (gizyazım) ve kriptanaliz (gizçözüm) özel ve ayrıntılı ilgi hak eder.

°°° Kriptografi

Kriptografi (gizyazım), gizli yazı yöntemi olarak bilinse de aslında bir matematik uygulamasıdır. Mesela, en eski kriptografi yöntemlerinden biri sayılan *Sezar şifresi*, alfabedeki harflerin yerinin ileri veya geri, belli sayıda kaydırılmasıdır. Roma imparatoru Julius Sezar önemli mesajlarını bu şekilde şifreleyerek gönderirmiş. Harflerin kaydırılma sayısı anahtardı; ancak bu sayıyı bilen biri şifrelenmiş mesajı çözebilirdi.

> Stanley Kubrick'in kült filmi "*2001: A Space Odyssey*"deki meşhur, akıllı bilgisayar ***HAL*** neydi veya kimdi acaba?

Bu tür şifreleme yöntemi, *yerine koyma* (*substitution*) olarak tanımlanır. Yerine koyma yönteminde mutlaka alfabenin sırasını kaydırmak gerekmez, bazen harflerin yerine sayılar veya işaretler de konabilir.

Çok kullanılan bir başka şifreleme yöntemi ise *yerini değiştirme* (*transposition*) olarak tanımlanır. Yerini değiştirme yönteminde harflerin kelime ya da metin bloğu içerisindeki yerleri değiştirilir.

Yerini değiştirme yönteminde harfler aynı kaldığı için, olası permutasyonları çok hızlı gözden geçirebilen bir kişi -veya makine- şifreyi çözebilir.

> Üç harfli KAR kelimesi, harfleri yer değiştirdiğinde, **n!**=6 farklı şekilde yazılabilir: KAR, KRA, AKR, ARK, RKA, RAK. Şifrelenmiş hali **RKA** olarak yazılmış olsa bile, dikkatli, tecrübeli biri tarafından makul bir süre içerisinde düz metnin KAR olduğu bulunabilir.

Yerine koyma (substitution) yönteminde harfler değişir ama kelime içindeki yerleri aynı kalır. Yerini değiştirme (transposition) yönteminde ise harfler aynı kalırken kelime içerisindeki yerleri değişir. Her ikisinin birlikte, karma (kompozit, hibrit) olarak kullanıldığı şifreleme yöntemleri de vardır.

> Düz metindeki KOYUN kelimesi, yerine koyma (substitution) yöntemiyle şifrelendiğinde **HLVRK**; yerini değiştirme (transposition) yöntemiyle şifrelendiğinde **YUONK** olabilir. Önce yerine koyma yöntemi, bilahare yerini değiştirme yöntemi uygulandığında ise **VRLKH** olur.

Yerine koyma (substitution) şifrelemenin en basit hali tek alfabeli (monoalphabetic) olanıdır.

> Sezar şifresinde olduğu gibi alfabe üç adım ileri kaydırılarak yeni bir alfabe yaratılabilir.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

> Anahtar: 3

> Düz metin: acil muhimmat lazım

Şifreli metin: **DFLO PXKLPPDW ODCLP**

Mono alfabetik şifreleme için bir başka örnek:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

Anahtar: *DIYARBAKIR* tekrar eden harfler çıkarılır: *DIYARBK*
alfabenin başına bu harfler yazılır, kalan harfler sondan başa doğru yazılır

D	I	Y	A	R	B	K	Z	X	W	V	U	T	S	Q	P	O	N	M	L	J	H	G	F	E	C

Düz metin: acil muhimmat lazim
Şifreli metin: **DYXU TJZXTTDL UDCXT**

Tek alfabeli (monoalphabetic) yerine koyma (substitution) şifrelemede, düz metindeki her harf her seferinde aynı harfe dönüşmektedir. Frekans analizi, çok kullanılan iki veya üç harfli kelimeler, bilinen hitap şekilleri gibi ipuçları vasıtasıyla kolayca çözümlenebilirler.

Çok kullanılan hitaplar, selam ve saygı, veda sözcükleri, askeri kısaltmalar kriptanalistler için çok değerli ipuçları olagelmiştir.

Harflerin kullanım sıklığı (frekans), yaygın ikili veya üçlü harf grupları, hitap şekilleri gibi düz metnin yazıldığı dilin özellikleri bilindiğinde olası çözümlere ulaşmak mümkün hale gelir. Tüm olasılıkları çabucak hesaplayabilecek bilgisayar donanım ve yazılımlarını kullanarak ve tabii tecrübe, sezgi ve biraz da şans ile bu tür şifrelemelerin kırılması, kriptanalizi mümkündür.

İngilizce metinlerde kullanılan harflerin olası sıklığı:
en sık kullanılan harfler: **e t a o i n s h r d**
en sık kullanılan ilk harfler: **t a s h w i o**

Türkçe metinlerde kullanılan harflerin olası sıklığı:
en sık kullanılan on harf: **a e i n r l ı k d m**

Harflerin kullanım sıklığı, metnin yazılmış olduğu döneme veya metnin konusuna, hatta kurumsal niteliğine göre farklılık gösterebilir.

Örneğin, Paul-Louis-Eugène-Valerio'nun 1893 tarihli *De la Crypographie* adlı kriptanaliz çalışmasında belirtildiği üzere, dönemin İngilizce metinlerde en sık kullanılan harfler: **e t o a n i r s h d l c**
(Arkadaşım Prof. Ömer Eğecioğlu'na teşekkürlerimle. *Mathematical Recreations and Essays*)

(Yeri mi değil mi, bilmem; linotip dizgi makinelerinin kullanıldığı zamanlardaki *ETAOIN SHRDLU* ve şimdilerde internette sıkça rastladığımız *LOREM IPSUM* geliyor akla, ister istemez.)

Vigenère şifresi:

Her harf için aynı şifrelenmiş karşılığın bulunduğu tekli (mono) alfabetik yöntem yerine, kriptanalizi zorlaştırmak için çoklu (poly) alfabetik yöntemler geliştirilmiştir. On beşinci yüzyılın ortalarında, *tek alfabeli* (*monoalphabetic*) *yerine koyma* yönteminin zaaflarını gidermek amacıyla *çok alfabeli* (*polyalphabetic*) *yerine koyma* yöntemini geliştiren Leon Battista Alberti, birkaç kelimeden sonra yerine koyma alfabesini değiştiriyor, ancak hangi alfabenin kullanılması gerektiğini yine şifrelenmiş metin içerisinde belirtiyordu. Bu yöntem güvenlik zaafı yaratıyordu.

İki yüzyıl sonra, Giovan Battista Bellaso şifrenin anahtarının metinden ayrı gönderilmesini önerdi.

Ne yazık ki yüzyıllar boyu oldukça yaygın kullanılan bu yöntem, aynı dönemde yaşamış olan Blaise de Vigenère tarafından bulunmuş olduğuna dair bir yanlış kanı nedeniyle *Vigenère şifresi* adıyla yanlış anılmaktadır. Yanlış adlandırılmış olsa da bilgisayarların ve modern algoritmaların kriptografide kullanılmaya başlandığı yakın zamana dek çok kullanılan bir şifreleme yöntemiydi Vigenère.

Vigenère Tablosu

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**
2	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**
3	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**
4	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**
5	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**
6	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**
7	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**
8	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
9	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**
10	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**
11	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**
12	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
13	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**
14	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**
15	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**
16	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**
17	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**
18	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**
19	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**
20	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**
21	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**
22	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**
23	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**
24	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**
25	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
26	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**

Vigenère tablosu, yerine koyma yönteminin biraz daha karmaşık örneği olan çok alfabeli (polyalphabetic) kriptografide kullanılan bir araçtır. (Yukarıdaki tablonun benzeri başka tablolar da kullanılabilir.) Çok alfabeli şifrelemede, şifre anahtarı olarak bir kelimeden ziyade uzunca bir ifade kullanılması tercih edilir. (anahtar kısaysa tekrarlanır)

Düz metin: yarın sabah hava bozacak

Anahtar: *SERT KAYA*

Anahtarı tekrarlayalım ve altına düz metni yazalım, artanı xxxx ile tamamlayalım. Düz metindeki her harfe karşılık anahtar satırındaki harfle başlayan satırı dikkate alarak düz metindeki harfin karşılığını bulalım.

Düz metnin ilk harfi *y* karşılığı şifrelenmiş harfi bulmak için anahtarın ilk harfi *S* ile başlayan 17. satıra gidelim; *y* harfini, şifre karşılığı olan **Q** ile şifreleyelim. Benzer şekilde, düz metindeki *a* karşılığını bulmak için *E* ile başlayan 3. satıra giderek *a* karşılığı olan **E** ile şifreleyelim. Yine, düz metindeki *r* karşılığı için *R* ile başlayan 16. satıra giderek *r* karşılığı olan **I** ile şifreleyelim. Düz metindeki *ı*(*i*) karşılığı için *T* ile başlayan 18. satıra giderek, *i* karşılığı olan **B** ile şifreleyelim. Düz metindeki *n* karşılığı için *K* ile başlayan 9. satıra giderek, *n* karşılığı olan **X** ile şifreleyelim. … … …

S	*E*	*R*	*T*	*K*	*A*	*Y*	*A*	*S*	*E*	*R*	*T*	*K*	*A*	*Y*	*A*	*S*	*E*	*R*	*T*	*K*	*A*	*Y*	*A*	*S*
y	a	r	i	n	s	a	b	a	h	h	a	v	a	b	o	z	a	c	a	k	x	x	x	x
Q	**E**	**I**	**B**	**X**	**S**	**Y**	**B**	**S**	**L**	**Y**	**T**	**F**	**A**	**Z**	**O**	**R**	**E**	**T**	**T**	**U**	**X**	**V**	**X**	**P**

Yukarıdaki Vigenère tablosunu ve SERT KAYA anahtarını kullanarak, "yarın sabah hava bozacak" mesajını şifrelediğimizde **QEIBXSYBSLYTFAZORETTUXVXP** olur. Bu karmaşık harf dizinini yazarken gözle takip kolay olsun diye beş harfli gruplar halinde ayırdığımızda **QEIBX SYBSL YTFAZ ORETT UXVXP** şeklinde bir metin elde ederiz.

Tek alfabeli yerine koyma yöntemi ile şifrelendiğinde, düz metindeki belirli bir harf, şifrelenmiş metinde hep aynı harfe dönüşür ama *çok alfabeli yerine koyma* yöntemi uygulandığında, düz metindeki belirli bir harf şifrelenmiş metinde farklı harflere dönüşür.

Yukarıdaki örnekte iki *h* harfi, şifrelendiğinde biri **L**, diğeri **Y** oluyor; *a* harfi, yerine göre, **E, Y, S, T, A** oluyor; *b* harfi, **B** ve **Z** oluyor.

Çok alfabeli yerine koyma yöntemi ile şifrelenmiş metinlerde frekans analizi -işe yaramaz olmasa da- kolaylıkla uygulanamaz. Onun yerine, tekrarlayan kalıplar daha yararlı olur kriptanaliz için; özellikle, sık kullanılan üç veya iki harfli kelimeler, hitaplar, kısaltmalar.

Düz metin: bir kuzu, bir tilki ve bir aslan…

Anahtar: *ELMAS*

E	*L*	*M*	*A*	*S*	*E*	*L*	*M*	*A*	*S*	*E*	*L*	*M*	*A*	*S*	*E*	*L*	*M*	*A*	*S*	*E*	*L*	*M*	*A*	*S*
b	i	r	k	u	z	u	b	i	r	t	İ	l	k	i	v	e	b	i	r	a	s	l	a	n
F	**T**	**D**	**K**	**M**	**D**	**F**	**N**	**I**	**J**	**X**	**T**	**X**	**K**	**A**	**Z**	**P**	**N**	**I**	**J**	**E**	**D**	**X**	**A**	**F**

Şifrelenmiş mesajda tekrar eden **NIJ** üçlü harf grubu dikkat çekmektedir. On karakterde bir tekrarladığına göre bu bize anahtarın uzunluğu hakkında fikir verebilir -ki bu ipucu şifreyi çözmede çok yararlıdır. Anahtarın uzunluğu on veya beş harfli

olabilir. Öte yandan, düz metinde yer alabilecek üç harfli kelimeler elden geçirildiğinde, bunların içinde "bir" önde gelir. Düz metin "bir" ve şifreli metin "**NIJ**" ise buradan anahtara ulaşmak an meselesidir. Anahtarın üç harfinin *MAS* olduğunu bulduktan sonra, üç harfi *MAS* olan beş ve on harfli kelimeler arasında on harfli olanlar kolayca ayıklanabilir. Kaç tane on harfli kelime var ki? On harfliler olmuyorsa beş harfliler denenir. Her neyse, biraz çalışma ve biraz şansla anahtar bulunabilir: *ELMAS*. Anahtarı buldukta sonra düz metne ulaşmaya engel ne kaldı? (Bilgisayar ve iyi bir yazılım vasıtasıyla yapıldığında tüm bu işlem birkaç saniyeden fazla sürmez.)

Çok alfabeli yerine koyma yönteminde şifre anahtarı olarak daha ziyade uzunca bir ifadenin tercih edildiği dikkate alındığında, çok anahtarlı yerine koyma yönteminin esası şöyle izah edilebilir: Anahtar eğer tekrarlanan tek bir harften ibaret olsaydı, bu durumda hep aynı tek alfabeli şifre kullanılıyor olurdu. Eğer iki harften ibaretse, iki farklı; on harften ibaretse, on farklı tek alfabeli şifreleme söz konusu olur. On harflik bir anahtar kullanarak iki yüz kelimelik bir metin şifrelendiğinde on ayrı alfabenin her birinin yirmi kez kullanılıyor olması söz konusudur.

Kriptografların kaçınması gereken, kriptanalistlerin aradığı şeydir, tekrar. Gerek düz metin içerisinde, gerekse şifre anahtarındaki tekrarlar şifrelemenin zayıflamasına sebep olmaktadır. Bu yüzden askeri veya resmi dilde yazılmış metinler daha kolay çözülür, çünkü tekrarlayan veya kolay tahmin edilen hitaplar, rütbeler, kalıplar, kısaltmalar içerirler.

Çok alfabeli yerine koyma yöntemi Vigenère bir zamanlar *kırılamayan şifre* (*chiffre indéchiffrable*) diye biliniyordu; ta ki on dokuzuncu yüzyılın ortalarında İngiliz bilim adamı Charles Babbage tarafından kriptanaliz yöntemi bulunana kadar. (Babbage bu çalışmasını yayınlamamıştır; yüz yıl sonra çalışma notları incelendiğinde ortaya çıkmıştır.) Vigenère şifresini kıran kişi olarak, Babbage ile aynı dönmede yaşayan bir Prusya ordusu subayı olan Friedrich Wilhelm Kasiski bilinir. Kasiski bu buluşunu *Gizli Yazı ve Şifre Kırma Sanatı* (*Die Geheimschriften und die Dechiffrir-kunst*) diye yayınlamış ve o dönemde kırılamaz diye bilinen çok alfabeli yerine koyma yönteminin üstesinden gelinebileceğini göstermiştir.

Babbage, her ne kadar başladığı işi zamanında bitirmeyen, projeleri aksatan, çalışmalarını yayınlamayan biri olarak tanınıyor olsa da bu denli önemli -üstelik bir iddia üzerine giriştiği ve başardığı- bir çalışmanın sonucunu yayınlayıp takdirleri toplamak istemez miydi? Kırım Harbi sürerken Rusların haberleşmesini takip eden ve şifrelerini kıran İngiliz istihbaratının sessiz kalma ricasını yerine getirmiş olabilir mi, acaba?

Playfair şifresi:

Özgün kriptografi arayışlarının çok yaygın olduğu Victoria İngiltere'sinde, on dokuzuncu yüzyılın ikinci yarısında, Charles Babbage, Sir Charles Wheatstone, Baron Lyon Playfair gibi bilim adamları da bu akımın dışında kal(a)mamışlar. Charles Babbage -her ne kadar yayınlamasa da- Vigenère şifresini kırmak için çalışırken, Sir Charles Wheatstone ve Baron Lyon Playfair ise harf çiftleri üzerinde uygulanan (ikili) yerine koyma yöntemi olan *Playfair* şifresini geliştirdiler.

Playfair şifresinin esasını alfabenin harflerinin yerleştirildiği 5x5 matris oluşturmaktadır. (5x5=25 *I* ve *J* harfleri tek karakter olarak yerleştirildiğinde 26 harfli İngilizce alfabe kapsanmış olur.)

Düz metin: bu sabah hava sissiz ve berrak olacak

Anahtar: *KASVET*

5x5 matrise önce anahtar kelimeyi, kalan boşluklara diğer harfler yerleştirelim.

K	*A*	*S*	*V*	*E*
T	B	C	D	F
G	H	I/J	L	M
N	O	P	Q	R
U	W	X	Y	Z

Düz metni ikili harf gruplarına ayıralım.

bu sa ba hh av as is si zv eb er ra ko la ca k

Herhangi bir ikili grupta aynı harf kendini tekrarlıyorsa, araya *x* koyalım; en sonda tek harf kalırsa *x* ekleyelim.

bu sa ba h*x* ha va si ss iz ve be rr ak ol ac ak

bu sa ba h*x* ha va si s*x* si zv eb er ra ko la ca k*x*

Tüm harf çiftleri aşağıdaki durumlardan birini karşılar:

1. İki harf aynı satırdaysa; her birinin yerine hemen sağındaki harf yerleştirilir. Satırın en sonundaki harfin sağındaki harf için satırın başındaki harf kullanılır.

Mesela, *sa* çifti, **VS** olur; *va* çifti, **ES** olur; *ve* çifti **EK** olur

2. İki harf aynı sütundaysa; her birinin yerine hemen altındaki harf yerleştirilir. Sütunun en sonundaki harfin altındaki harf için sütunun başındaki harf kullanılır.

Mesela, *ba* çifti, **HB** olur; *si* çifti, **CP** olur; *er* çifti **FZ** olur; *sx* çifti **CS** olur
(Örnekte yok ama *ut* çifti olsaydı, **KG** olarak şifrelenecekti)

3. İki harf aynı satırda veya aynı sütunda değilse; birinci harf için, birinci harfin satırı ile ikinci harfin sütununun kesişimindeki harf kullanılır; ikinci harf içinse, ikinci harfin satırı ile birinci harfin sütununun kesişimindeki harf kullanılır).

Mesela, *hx* çifti, **IW** olur; *kx* çifti **SU** olur.

Bu durumda, düz metnin ayrılmış olduğu harf çiftleri şöyle şifrelenir:

bu sa ba hx ha va si sx si zv eb er ra ko la ca kx

TW VS HB IW OB ES CP CS CP YE AF FZ OE AN HV BS SU

Beşli gruplandığında, **TWVSH BIWOB ESCPC SCPYE AFFZO EANHV BSSUX** olur.

Çok alfabeli yerine koyma yöntemlerinde, düz metinde tekrarlayan kelimelerin olması ve bu kelimelerin tekrarlayan anahtar ile denkleşmesi, şifrelenmiş metinde fark edilmelerine sebep olmakta; dolayısıyla şifrelemeyi zayıflatmakta, kriptanalize imkân vermektedir.

Nihilist şifresi:

19ncu yüzyılın sonlarında çarlık Rusya'sındaki nihistler kullanırlardı bu yöntemi.

Düz metin: saraya saldırın

Anahtar: *KASTAMONU*

5x5 matrise önce anahtar kelimeyi, kalan boşluklara diğer harfler yerleştirelim. (Tekrarlayan harfleri kullanmayalım.)

	1	2	3	4	5
1	*K*	*A*	*S*	*T*	*M*
2	*O*	*N*	*U*	*B*	*C*
3	*D*	*E*	*F*	*G*	*H*
4	*I/J*	*L*	*P*	*Q*	*R*
5	*T*	*V*	*W*	*X*	*Y*

Düz metni matrisi oluşturan hücrelerin koordinatları ile şifreleyelim.
13 12 45 12 55 12 13 12 42 31 41 45 41 22 şifrelenmiş metin.

Ancak bunu çözmek kolay olurdu.

Bir şifre anahtarı daha belirleyelim: *CİDE* 25 41 31 32

Birinci anahtarla şifrelenmiş metni ve bu ikinci anahtarı toplayalım.
13 12 45 12 55 12 13 12 42 31 41 45 41 22
25 41 31 32 25 41 31 32 25 41 31 32 25 41
38 53 76 44 80 53 44 44 67 72 72 77 66 63 şifrelenmiş metin

Nihilist de olsalar bir düzene riayet etmek zorundaydılar.

Vernam şifresi:

Amerikalı mühendis Gilbert Sandford Vernam tarafından 1917 yılında bulunan bu hayli etkin (basit, kolay, hızlı) şifreleme yönteminde, düz metin ve şifre anahtarı önce Baudot koduna çevrilmekte, bilahare XOR işleminden geçirilmektedir. (XOR işlemini Türkçede "ya ya" işlemi, "eşit değil" işlemi olarak tanımlayabiliriz.)

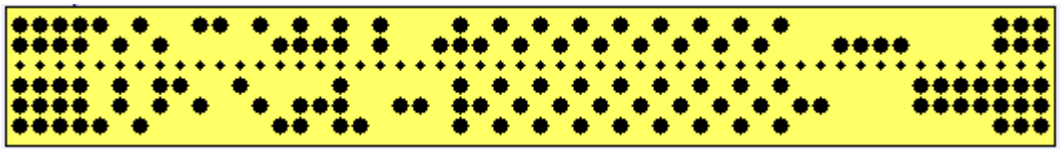
XOR $\oplus$

$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$

Fransız telgraf mühendisi Jean Maurice Émile Baudot tarafından 1870'lerde geliştirilmiş olan kod, teleks makinelerinde (telex, teletype, teleprinter) kullanılır.

Veri iletişiminde kullanılan *baud* birimi Baudot'a saygıdandır.

Baudot kodlamasında her karakter (harf, rakam, işaret) ve komut için delinmiş ya da delinmemiş beş haneden oluşan bir dizin kullanılır.



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z					
“	?	:	$	3	!	&	#	8	4	(	)	.	,	9	0	1	‘	β	5	7	;	2	/	6	“	LF	SP	CR	FIG	LTR
1	**1**	**0**	**1**	**1**	**1**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**1**	**0**	**0**	**0**	**1**	**1**
1	**0**	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**1**	**1**	**1**	**0**	**0**	**0**	**1**	**1**	**1**	**0**	**0**	**1**	**1**	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**1**	**1**
♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦
0	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**1**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**1**	**0**	**1**	**1**	**0**	**0**	**1**	**0**	**0**	**1**
0	**1**	**1**	**1**	**0**	**1**	**1**	**0**	**0**	**1**	**1**	**0**	**1**	**1**	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**1**	**1**	**1**
0	**1**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**1**	**1**	**0**	**1**	**1**	**1**	**0**	**0**	**1**	**0**	**1**	**1**	**1**	**1**	**1**	**0**	**0**	**0**	**1**	**1**

SP Space boşluk
LF Line Feed satır ilerletme
CR Carriage Return satır başı
FIG Rakamlar ve işaretler
LTR Harfler

[0 0 0 0 0] kullanılmaz.

Bu durumda 2^5-1=31 farklı karakter ve/veya komut tanımlanabilir.

Düz metin ve şifre anahtarı ayrı ayrı teleks bandına kodlanarak XOR işleminden geçirildiğinde ortaya şifreli metin çıkar. Benzer şekilde, şifreli metin ile şifre anahtarı XOR işleminden geçirildiğinde düz metin ortaya çıkar.

Düz metin ⊕ Anahtar = Şifreli metin

Şifreli metin ⊕ Anahtar = Düz metin

Düz metin:	A	1 1 0 0 0
Şifre anahtarı:	*K*	1 1 1 1 0
A ⊕ *K*		0 0 1 1 0 : **N**
Şifreli metin:	**N**	0 0 1 1 0
Şifre anahtarı:	*K*	1 1 1 1 0
N ⊕ *K*		1 1 0 0 0 : A

Muhteşem, güzel!.. Değil mi?..

Vernam şifreleme yöntemi, esasında XOR işlemi vasıtasıyla yerine koyma (substitution) uygulayan bir dizi (stream) şifreleme yöntemidir.

Bu denli basit bir yöntemi bu denli muhteşem yapan ne?
Basitliği…

> Tüm bilim dallarında -özellikle matematikte- güzellik basitliktedir.
>
> Mümkün olduğunca basitleştir ama daha fazla değil
>
> Albert Einstein

Peki, böylesi basit bir yöntemi güvenli yapan ne?
Şifre anahtarı olarak tek kullanımlık defter (One Time Pad - OTP)) kullanılması…

Kurallara riayet ederek OTP şifre anahtarı kullanıldığında, Vernam yöntemi çok güvenli bir yöntemdir.

Vernam yönteminin bir başka avantajı ise mesajı göndermeden önce şifrelemek için ayrıca zaman harcamaya gerek bırakmamasıdır; mesaj, akarken şifrelenmektedir.

> 1910'ların Vernam şifresinin temelindeki Baudot kodlamasının gösteriminde 1'ler, 0'lar yerine, delik için (x), boşluk için (.) kullanılıyordu. 1940'larda çözüm için uğraşanlar da aynı formatı kullanıyorlardı. Yani:
>
> | | | | | | | | |
> |---|---|---|---|---|---|---|---|
> | Düz metin: | A | X | X | . | . | . | |
> | Şifre anahtarı: | *K* | X | X | X | X | . | |
> | A ⊕ *K* | | . | . | X | X | . | : **N** |
>
> Vernam şifresinin uygulanmasında ve çözümünde yararlanılan elektromekanik cihazlarda dişli çarklar ve röleler kullanılıyordu. Röle deyip geçmeyin. Strowger ve crossbar santrallerde çalışmış bir telefon mühendisi olarak söyleyebilirim ki rölelerle çok karmaşık harikalar yaratılıyordu o zamanlar.

Tek kullanımlık defter (One Time Pad - OTP) şifre anahtarı:

Düz metinde tekrarlayan kelime olmaması pek olası değil ama ya asla tekrarlamayan bir anahtar kullanılırsa?.. Bu durumda, tekrarları şifreli metinde tespit etmek mümkün olamayacaktır. Sadece bir kez kullanılan, tamamen rastgele karakterlerden meydana gelmiş ve en az düz metin kadar uzun bir anahtar amaca uygun olurdu. Her mesaj için tek kullanımlık ayrı bir anahtar metni içeren sayfalardan oluştuğu için bu yöntem *Tek kullanımlık defter (One Time Pad - OTP)* olarak adlandırılır. Doğru kullanıldığında; yani, anahtar tamamen rastgele karakterlerden oluşmuşsa, en az düz metin uzunluğundaysa, sadece ve sadece bir kez kullanılıyorsa, OTP yöntemi ile şifrelenmiş mesajın şifresini kırmak mümkün değildir. Enformasyon teorisinin büyük ismi Claude Shannon, OTP yöntemi ile şifrelemenin çözülemez olduğunu ispatlamıştır.

Kurallar:
(1) anahtar, şifrelemede ve şifreyi çözmede bir kez kullanılmalı; asla tekrarlanmamalı. (Bu yüzden tek kullanımlık…)
(2) anahtar, en az düz metin kadar uzun olmalı.
(3) anahtar, rastgele karakterlerden oluşmalı. (Herhangi bir karakter, bir başkasını kullanarak tahmin edilememeli.)

> OTP şifreleme yöntemini kuvvetli yapan özelliği olan rastgele karakterlerden oluşması kuralı (sonradan tümgeneral olan) yüzbaşı Joseph Oswald Mauborgne tarafından

> önerilmiştir. Güzel sanatlar eğitimi alan Joseph Mauborgne, muhabere subayı olarak görev yaptığı sürede kripto, radyo ve radarla ilgili birçok öncü çalışmada yer almış; bu arada güzel sanatlara ilgisini sürdürmüş, resim sergilerine ilaveten keman yapımcılığında da ün kazanmıştır. Nereden, nereye… Kriptoloji tarihi böyle örneklerle doludur. Kriptoloi, bilim olduğu kadar sanattır da…

Birinci kural bir bakıma ikinciyi ima ediyor. Anahtar, düz metin kadar uzun değilse tekrarlamak zorunda kalınır ki bu da birinci kuralın ihlali demektir.

> Soğuk Savaş döneminin yıllar boyu süren VENONA kod adlı kriptanaliz projesinde Amerikalılar ve İngilizlerin nihayetinde başarı elde etmesinin nedeni bazı Rus kripto operatörlerinin bu kuralı ihlal etmeleridir. Ellerinde tek kullanımlık defter kalmadığı için eskileri kullanmışlar!..

OTP şifreleme yöntemini güçlü kılan kurallar aynı zamanda pratikliğini azaltmakta, kullanımını zorlaştırmaktadır.

Anahtar asla tekrarlanmamalı, her mesaj tek bir anahtar ile şifrelenmeli. Şifreleme ve şifre çözmeişleminden sonra anahtar mutlaka imha edilmeli. Bu durumda görülüyor ki, anahtarın hafızada kalma veya ağ üzerinde bir yerde tutulma ihtimali olan ağ ve bilgisayar ortamları OTP için güvenli değildir. Doğrusu, adından anlaşılacağı üzere, defter (pad) kullanmak ve sonra o sayfayı yırtarak imha etmek hala en güvenli yöntemdir.

> Soğuk Savaş döneminin yıllar boyu süren VENONA kod adlı kriptanaliz projesinde Amerikalılar ve İngilizlerin başarıyı elde etmesinin nedeni, bazı Rus kripto operatörlerinin bu kuralı ihlal etmeleridir. Ellerinde tek kullanımlık defter kalmadığı için eskileri kullanmışlar!..

En az düz metin kadar uzun ve mutlak rastgele (random) karakterlerden oluşan bir anahtar üretmek oldukça zordur; dolayısıyla pratik değildir. Bu sebeple, genellikle yarı-rastgele (pseudo-random) üreteçler kullanılır ki bu durum daha baştan yöntemin güvenliğini zayıflatır.

> Burada önemli olan şudur: “pseudo” ne kadar “pseudo”?..

Her mesaj için tek kullanımlık bir çift anahtar üretmek, bu anahtarları gönderen ve alan taraflara güvenli şekilde ulaştırmak ve kullandıktan sonra güvenle imha etmek oldukça zor, hatta gizli haberleşmenin pratiğine aykırı bir durumdur.

> İdaresi zor olan her şey gibi OTP de gerektiği şekilde kullanılmadığında, kurallardan taviz verildiğinde, hata yapıldığında beklenenden çok daha zayıf hale gelir ve ciddi güvenlik zaafına yol açar.

. . . . . .

Yerine koyma (substitution) yönteminde olduğu gibi, yerini değiştirme (transformation) yönteminde de farklı uygulamalar geliştirilmiştir. Birkaç örnek vermek gerekirse:

Parmaklık (Rail Fence) şifresi:

Düz metin: bugün hava güzel olacak

b						a						e						a			
	u				h		v				Z		l				c		k		
		g		n				a		u				o		a					
			u						g						l						

Anahtar olarak satırlardaki harfleri soldan sağ yazdığımızda,
şifrelenmiş metin, **BAEAU HVZLC KGNAU OAUGL** olur.

Yol (Route) şifresi:

Düz metin: bugün hava güzel olacak Yukarıdan aşağıya ve soldan sağa yazalım.

b	n	a	e	a
u	h	g	l	c
g	a	u	o	a
u	v	z	l	k

Anahtar olarak sol alttan başlayarak saatin tersi yönde spiral şeklinde yazdığımızda,
şifrelenmiş metin, **UVZLK ACAEA NBUGA UOLGH** olur.

ADFGVX şifresi:

Birinci Dünya savaşında kullanılan ADFGVX veya ADFGX şifresi ise, yerine koyma (substitution) ve yerini değiştirme (transposition) yöntemlerini birlikte kullanması bakımından ilginçtir. (A D F G V X harfleri, telgraf operatörlerinin hata yapmasını en aza indirmek için seçilmiş, Morse alfabesinde birbirinden kolayca ayrıştırılabilen karakterlerdir.)

ADFGVX şifresi, 26 harf ve 10 rakamdan oluşan karakter setinin 6x6 matris içerisine rastgele yerleştirilmesiyle kurulur. (Rakamlar kullanılmadığında ADFGX yeterli olur.) Bu rastgele matris, şifrenin anahtarıdır. Mesajı alanın şifreyi çözebilmesi için bu matris anahtara sahip olması gerekir.

	A	**D**	**F**	**G**	**V**	**X**
A	r	1	j	7	w	d
D	l	y	a	T	g	o
F	p	6	b	Z	v	5
G	f	u	m	0	s	i
V	3	c	2	X	k	9
X	8	h	q	N	e	4

Açık metindeki *p* harfi, şifreli metinde **FA**; *m* harfi, **GF**; *5* rakamı **FX** olur.

Mesela, "bugün saat 1230da" düz metni **FFGDDVGDXG GVDFDFDG ADVFVAGGAXDF** olarak şifrelenir. Beş harfli gruplandığında **FFGDD VGDXG GVDFD FDGAD VFVAG GAXDF** şeklinde yazılır.

Oldukça karışık, değil mi? Aslında değil; çünkü buraya kadar yapılan sadece basit bir yerine koyma (substitution) işlemiydi; çözümü de o denli kolaydır.

Peki, biraz daha zorlaştırmak için, bunun üzerine bir de yerini değiştirme yöntemi uygulayalım. Mesela, yerini değiştirme (transposition) anahtarı da *SERKAN* olsun. Önce yerine koyma yöntemi ile şifrelenmiş mesajdaki harf çiftlerini bu yerini değiştirme anahtarının altına soldan sağa yazalım.

S	*E*	*R*	*K*	*A*	*N*
F	**F**	**G**	**D**	**D**	**V**
G	**D**	**X**	**G**	**G**	**V**
D	**F**	**D**	**F**	**D**	**G**
A	**D**	**V**	**F**	**V**	**A**
G	**G**	**A**	**X**	**D**	**F**

Yerini değiştirme anahtarındaki harfler alfabetik sırada olacak şekilde tabloyu yeniden düzenleyelim.

A	*E*	*K*	*N*	*R*	*S*
D	**F**	**D**	**V**	**G**	**F**
G	**D**	**G**	**V**	**X**	**G**
D	**F**	**F**	**G**	**D**	**D**
V	**D**	**F**	**A**	**V**	**A**
D	**G**	**X**	**F**	**A**	**G**

ve şifreli mesajın harflerini bu kez yukarıdan aşağıya sıralayarak yazalım.

DGDVD FDFDG DGFFX VVGAF GXDVA FGDAG

Yerine koyma ve yerini değiştirme yöntemlerinin birlikte kullanıldığı, oldukça kuvvetli bir şifre olan ADFGVX şifresinin kırılması günümüz teknolojisi ile birkaç saniye alsa da, yaygın kullanılmakta olduğu yirminci yüzyılın başında bu şifreyi kırmak çok zordu.

O dönemde yerine koyma (substitution) ile yerini değiştirme (transposition) karışımı ADFGVX ve çifte transposition ÜBCHI yöntemleri sıklıkla kullanılıyordu. Fransız ve İngiliz kriptanalistler -önceleri küçümsedikleri ama başarılı çözümlerini gördükten sonra saygı duyarak aralarına aldıkları- Amerikalı meslektaşlarının da yardımıyla, Alman genelkurmayı ile cephedeki komutanlar arasında teati edilen şifreli mesajları

çözmeye çalışıyorlardı. Çok zordu ama yine de kurallara uymayan operatörlerin hataları sayesinde oldukça çok miktarda ve önemli mesajı çözebiliyorlardı.

Kafkaslardaki petrol yataklarını korumak, daha doğrusu Türklere bırakmamak için Suriye'deki general Von Kressenstein'ın Tiflis'e tayin emri kriptosunu çözen Müttefikler bu sayede Almanlar ile Türkler arasındaki sürtüşmenin farkına varıp politikalarını buna göre oluşturmuşlardır.

°°° Kriptanaliz

Kriptografinin (gizyazım) gizli yazı ilmi olmasına karşılık, kriptanaliz (gizçözüm) gizli yazıyı çözme ilmidir. Kriptanaliz de -kriptografi gibi- matematiktir ama yanı sıra dilbilimdir, önsezidir ve biraz da şanstır.

Şifrelemede özensiz ve dikkatsiz davranılırsa, düz metinde kullanılan kelimeler veya seçilen anahtarlardaki zaaflar çözüme yardımcı olabilir. Mesela, dikkatli gözlerden kaçmamıştır, daha öncesözü edilen Vigenère şifrelemesi örneğinde eğer şifre anahtarında *A* harfi varsa, düz metindeki harf değişmiyor. (Benzer şekilde, düz metinde a harfi varsa, anahtardaki harf aynen şifrelenmiş metne geçiyor.)

Diyelim ki düz metinde *saat* kelimesi var.

S	*E*	*R*	*T*
s	a	a	t
Q	**E**	**R**	**B**

İşte, anahtarın iki harfi kendini gösteriyor: *E* ve *R*.

Peki, ya anahtar *ARABA*, düz metin ise "sabah beşte hücum" olsaydı?

A	*R*	*A*	*B*	*A*	*A*	*R*	*A*	*B*	*A*	*A*	*R*	*A*	*B*	*A*
s	a	b	a	h	b	e	s	t	e	H	u	c	u	m
S	**R**	**B**	**B**	**H**	**B**	**V**	**S**	**U**	**E**	**H**	**L**	**U**	**V**	**M**
S		B		H	B		S		E	H		C		M

Mesajın ne hakkında olabileceğini tahmin eden Türkçeye hakim biri, altı çizili harflere bakarak mesajın düz metnini ortaya çıkarabilir: *s*abah beşte hücum *(Muhtemel Metin)*

En güvenilir şifreleme yöntemi olduğu kabul edilen tek kullanımlık defter (One Time Pad - OTP) dahi gerektiği gibi kullanılmadığında kriptanalizi mümkün olabilir.

Kural: düz metin kadar uzun, rastgele bir anahtarı sadece bir kez kullan.

düz metin1 ⊕ anahtar1 = şifreli metin1

düz metin2 ⊕ anahtar2 = şifreli metin2

düz metin3 ⊕ anahtar3 = şifreli metin3

… … …

Kriptanalistler çaresiz kaldıklarında şanstan medet umarlar; en çok da şifreleyen tarafın hata yapmasından. Aynı anahtarın tekrarlanması, birden fazla mesajda kullanılması en sık rastlanan ve beklenen hatadır. Bu tekrarlara "derinlik" (depth) denir.

İki ayrı gönderide aynı anahtarın kullanılması halinde;

düz metin1 ⊕ anahtar = şifreli metin1

düz metin2 ⊕ anahtar = şifreli metin2

(düz metin1 ⊕ düz metin2) ⊕ (anahtar ⊕ anahtar) = şifreli metin1 ⊕ şifreli metin2

Kendisiyle XOR işlemi yapıldığında anahtar ortadan kalkar (sıfırlanır).

düz metin1 ⊕ düz metin2 = şifreli metin1 ⊕ şifreli metin2

Kısaltarak yazıldığında; dm1 ⊕ dm2 = sm1 ⊕ sm2

Diyelim ki herhangi bir şekilde birinci düz metni ele geçirmiş olalım.

dm1 ⊕ (dm1 ⊕ dm2) = dm1 ⊕ (sm1 ⊕ sm2)

(dm1 ⊕ dm1) ⊕ dm2 = dm1 ⊕ (sm1 ⊕ sm2)

dm2 = dm1 ⊕ (sm1 ⊕ sm2)

Şifreli metinler ve birinci düz metin elimizde olduğuna göre ikinci düz metni kolayca elde edebiliriz.

düz metin1	KASA (ele geçirildi)	düz metin2	ATES (bilinmiyor)
anahtar	PQNL		PQNL
1 1 1 1 0 1 1 0 0 0 1 0 1 0 0 1 1 0 0 0		1 1 0 0 0 0 0 0 0 1 1 0 0 0 0 1 0 1 0 0	
0 1 1 0 1 1 1 1 0 1 0 0 1 1 0 0 1 0 0 1		0 1 1 0 1 1 1 1 0 1 0 0 1 1 0 0 1 0 0 1	
1 0 0 1 1 0 0 1 0 1 1 0 0 1 0 1 0 0 0 1		1 0 1 0 1 1 1 1 0 0 1 0 1 1 0 1 1 1 0 1	
şifreli metin1	BHDZ	şifreli metin2	YUFQ

dm2 = dm1 ⊕ (sm1 ⊕ sm2)

1 0 0 1 1 0 0 1 0 1 1 0 0 1 0 1 0 0 0 1	sm1
1 0 1 0 1 1 1 1 0 0 1 0 1 1 0 1 1 1 0 1	sm2
0 0 1 1 0 1 1 0 0 1 0 0 1 0 0 0 1 1 0 0	(sm1 ⊕ sm2)
1 1 1 1 0 1 1 0 0 0 1 0 1 0 0 1 1 0 0 0	dm1
1 1 0 0 0 0 0 0 0 1 1 0 0 0 0 1 0 1 0 0	
ATES	dm2

ikinci düz metni bulduk: ATES

Birinci düz metin ile ikincisi arasındaki farkı biliniyorsa; bu da işe yarar.

düz metin1 ⊕ düz metin2 = şifreli metin1 ⊕ şifreli metin2

fark = şifreli metin1 ⊕ şifreli metin2

düz metin1	KASA	düz metin2	KAYA (bilinmiyor)
anahtar	PQNL		PQNL
1 1 1 1 0 1 1 0 0 0 1 0 1 0 0 1 1 0 0 0		1 1 1 1 0 1 1 0 0 0 1 0 1 0 1 1 1 0 0 0	
0 1 1 0 1 1 1 1 0 1 0 0 1 1 0 0 1 0 0 1		0 1 1 0 1 1 1 1 0 1 0 0 1 1 0 0 1 0 0 1	
1 0 0 1 1 0 0 1 0 1 1 0 0 1 0 1 0 0 0 1		1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 1 0 0 0 1	
şifreli metin1	BHDZ	şifreli metin2	BHBZ

fark = sm1 ⊕ sm2

BHDZ	1 0 0 1 1 0 0 1 0 1 1 0 0 1 0 1 0 0 0 1
BHBZ	1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 1 0 0 0 1
. . T .	0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0

Üçüncü karakterin farklı olduğunu ve farkın T olduğunu bulduk. Baudot kodlamasında farkı T olan harflerin S ve Y olduğunu bulmak için pratik bir matristen yararlanabiliriz. Elimizde şifreli iki metin var. Düz metinde üçüncü harfin S veya Y olabileceğini de biliyoruz. Bundan sonrası tahmin, tekrarlayan karakterleri gözleme, dile hakimiyet ve biraz şans…

Kriptolojinin ana dalları kriptografi ve steganografinin bilinen geçmişi iki bin beş yüz, üç bin sene öncesine uzanırken -son zamanlara kadar bilinen tarihiyle- kriptanaliz nispeten kısa bir zaman diliminin eseridir. Çok uzun zamandan beri kullanılagelen steganografide, saklı mesajı açığa çıkarmak için saklamanın ne şekilde yapıldığını bilmek gerekir. Benzer şekilde, kriptografi ile şifrelenmiş mesajı açığa çıkarmak için de şifre anahtarına sahip olmak gerekir. Şifre anahtarına sahip olmayan biri ise -muhtelif yöntemlerin yanı sıra- kriptanaliz sayesinde şifreyi çözebilir.

Bu amaçla kullanılan yöntemlerin -yumuşak bir okşayıştan falakaya- ne kadar çok ve çeşitli olduğunu söylemeye gerek yok. Bunların içerisinde bizim falakaya benzeyen lastik hortum yöntemi kripto jargonunda *rubber hose cryptanalysis* diye bilinir ki hayli etkilidir. Başka yöntemler de vardır: rüşvet, şantaj, hırsızlık, ağızdan laf almak, bilgisayara sızmak, vesaire…

Bilgi gizlemek amacıyla şifrelenmiş mesajların haricinde, çivi yazısını, hiyeroglifleri veya Orhun yazıtlarını çözmek için de ileri derece kriptanaliz becerisi gerekir. Bu yüzdendir ki herhangi bir dilde hazırlanmış şifreli bir metnin şifresinin çözülmesi için matematikçilerin, istatistikçilerin yanı sıra dilbilimcilere de ihtiyaç duyulmaktadır. İkinci Dünya Savaşı'nda birçok şifreyi çözerek savaşın kaderini önemli derecede etkileyen, İngiltere'nin kriptanaliz merkezi Bletchley Park'ta istihbarat uzmanları tercümanlar ve matematikçilerle birlikte çapraz bulmaca, satranç ve briç ustaları da görev yapmıştır. ENIGMA, ULTRA, VENONA gibi, savaş yıllarında ve savaştan sonra açığa çıkarılan birçok sır kriptanalistlerin başarılı çalışmalarının sonucudur.

En ufak zekâ kırıntısı içermeyen, kirli sakallı etnik terörist saçmalıklarından bıkan, benim gibi yetmişlerin, seksenlerin o muhteşem Soğuk Savaş entrikalarını özleyenler için bahsi geçen kod adları ilginç araştırma konuları olabilir. İçinde biraz da kurgu olsun isteyen Arthur Conan Doyle veya Jules Verne veya Edgar Allan Poe ile başlayabilir.

Kriptanalizin icat edilmesi ve geliştirilmesi sayesinde bilimsel yöntemler, özellikle matematik ve biraz dilbilim vasıtasıyla gizli mesajların anlaşılması mümkün olmuştur. Gelişmiş algoritmalar, güçlü ve hızlı işlemciler sayesinde yerine koyma ve/veya yerini değiştirme yöntemleriyle şifrelenmiş metinleri çözmek oldukça kolay hale gelmiştir günümüzde. Diğer yöntemler için de benzer durum söz konusudur. Nihayetinde, bulunan veya geliştirilen her kriptografik yöntem için etkili kriptanaliz yöntemleri araştırılır ve bir gün mutlaka bulunur. Başarılı her kriptanaliz yönteminin geliştirilmesinin hemen ardından o yöntemin etkili olamayacağı kriptografi yöntemleri geliştirilir. Ve bu, böyle sürer, gider…

Kriptografi ile kriptanaliz arasındaki yarış keşke hep böyle eğlenceli olsa ama değil…
-- Kolay?.. --- Hiç değil.

İşin esası matematiktir; seven için eğlenceli olabilir.

Matematik, dilbilim, yetenek, çok çalışma ve şans kadar -hatta daha önemli- başka etkenler de vardır kriptanalizin başarısında: şifreleyenin hata yapması; yani kurallara harfiyen uymaması, yeterince zaman ayırmaması, özensizliği, umursamazlığı, kendine aşırı güveni, kuvvetli olduğunu zannettiği ama aslında işe yaramayan algoritma kullanması, vesaire, vesaire…

Malum, kuşatma altındaki kaleyi koruyan taraf, saldıran tarafa göre daha dezavantajlı durumdadır. Kaleyi koruyanlar, akla gelen, gelmeyen her deliği tıkamak, her yeri korumak durumundadırlar. Halbuki saldıran taraf tek bir zayıf nokta, tek bir delik bulsa, kâfi.

Kriptograflar ile kriptanalistler arasında 17. yüzyılda başlayan mücadelenin yoğun sürdüğü 18. yüzyılda dile getirildiği gibi, “Kriptanalistler kazandıkları payeyi kötü şifrelere ve şifreleme yöntemini layıkıyla uygulamayanlara borçludurlar.” (Şifre anahtarlarını gerektiği gibi korumayanları da eklemeliyiz buna.)

Kriptografide şu altın kural asla akıldan çıkarılmamalı, asla:

Kurallara harfiyen riayet etmeden şifreleyeceksen hiç şifreleme daha iyi.

İşin gerçeği, hata yapanlar o kadar çoktur ki kriptanalistler uzun vadede daima galip gelirler kriptograflara karşı. NSA teoremi denen bir altın kural daha:

Kriptanaliz mutlaka galip gelir.

Nehrin kıyısında yeterince beklersen düşmanlarının cesetlerinin önünden akıp geçtiğini görürsün diyen atasözünde olduğu gibi, bu da benim teoremim:

Yeterince beklendiğinde tüm sırlar açığa çıkar.
(Termodinamiğin ikinci kanunuyla alakası olsa gerek.)

°° Araplar

Günümüzde kriptografi (şifreleme) ve kriptanaliz (şifre çözme) yüksek işlem kapasiteli bilgisayarlar ve karmaşık algoritmalar vasıtasıyla yapılıyor olsa da kriptolojinin varmış olduğu seviye aslında iki bin beş yüz yılı aşkın düşünce, çalışma ve birikimin sonucudur.

Arapların yarım milenyum boyunca kriptoloji üzerinde sahip olduğu hakimiyet ve üstünlük zamanla, özellikle Hıristiyan keşişler vasıtasıyla önce kıta Avrupa'sına, bilahare okyanus ötesine, Amerika'ya geçmiştir.

> Şifre kelimesi, Arapça *sıfır* kelimesinden türemiştir. (Fra., Alm. *chiffre*, İta., İsp. *cifra*, İng. *cipher*, Hol. *cijfer*, Pol. *szyfr*) Arapların da Sanskritçeden aldıkları sanılmaktadır. Dahası, Batı'da sıfır kavramı olmadığı için sayı sisteminde sıfıra karşılık bir işaret yoktu. Sıfır, Araplardan Avrupa'ya geçtiğinde pek de kolay anlaşılamamıştı. Bu yüzden, biri anlaşılmaz laf ettiğinde, "Sıfır gibi konuşma" derlermiş. İşte o gün bu gündür, anlaşılmaz olanla sıfır (Batı'nın tabiriyle şifre) özdeş olmuş.

Araplar, özellikle Abbasi hanedanlığı döneminde (750–1258), kriptolojide zamanın ötesine geçmiş, önemli buluşlar yapmışlardır. Kuran ayetlerinin ve hadislerin sahihliğinin tespiti amacıyla çok kişi, uzun yıllar boyunca ifadelerin anlamları, lisanın incelikleri, yazın hataları, kelimelerin ve harflerin dizilişleri, kullanım sıklıkları gibi birçok ayrıntı ile ilgilenmişlerdi. Bu çalışmalar, sahip oldukları ileri seviyede matematik bilgi ve becerisi ile birleşince, o çağda yaygın kullanılan (yerine koyma) kriptografi yöntemiyle şifrelenmiş metinlerin çözülmesi mümkün hale gelmiştir. Tabii ki dönemin ticaret erbabı olan Arapların birçok dile hakim olmalarının katkısı da küçümsenemez.

> Şimdilerde oyun gibi gelen ebced hesabı ve tarih düşme gibi işlemler o zamanlar ciddi işti ve kriptolojinin temel taşlarını döşemede yardımcı olmuştu.

Son zamanlara kadar, kriptanalizin on beşinci yüzyılda Avrupa'da doğduğu bilinirdi. Gerçi, Arapların çok daha önceleri yapmış oldukları çalışmaların bu doğuma yardımcı olduğuna dair emareler vardı ama kesin kanıt yoktu elde. Ancak, İstanbul Süleymaniye Kütüphanesi'nde bulunan, ünlü Arap filozof ve bilim adamı El-Kindi (801-873) tarafından kaleme alınmış bir risale, kriptanalizin temellerini oluşturan ve bugün dahi uygulanmakta olan tekniklerden söz etmektedir. Mesela, yerine koyma (substitution) ve yerini değiştirme (transposition) şifreleme teknikleri ve bunların birlikte kullanıldığı kompozit şifrelemeden, kriptanalizde istatistiki yöntemlerden ve muhtemel kelime tahmininden söz etmiştir. Öyle ki, dokuzuncu yüzyılda yazılmış olan bu risalede, bugün dahi kriptanalizin en temel yöntemi olarak kullanılmakta olan *sıklık (frekans) analizi* çok açık bir ifadeyle anlatılmaktadır.

Şifrelenmiş bir mesajın şifresini çözmek için El-Kindi der ki:

1. Mesajın düz metninin yazılmış olduğunu tahmin ettiğiniz lisanda yeterince uzun, mesela bir sayfa düzyazı alın ve bu lisanda kullanılan harflerin sıklığını (*frequency*) belirleyin.

2. Şifreli mesajda kullanılmış olan harflerin (veya işaretlerin) sıklığını belirleyin.

3. Şifreli mesajda en sık rastlanan harfler (veya işaretler) ile mesajın yazıldığı lisanda en sık rastlanan harfleri eşleştirin.

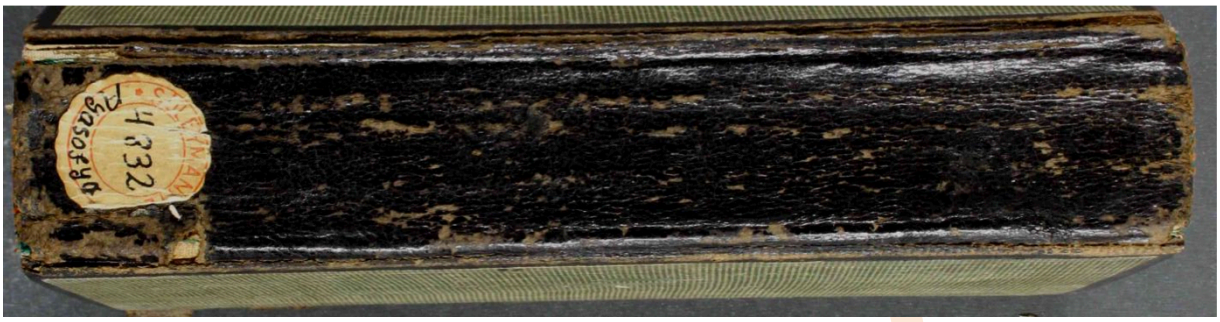
4. Düz metnin yazılmış olduğu lisandaki harf çiftleri, üçlüleri, hitap ve selamlama ifadeleri ve kafiyelerden yararlanın.

5. Anlamlı kelime parçacıkları ortaya çıktığında, *muhtemel kelimeyi* tahmin edin ve mesajın bütünlüğü ile uyumluluğunu test edin.

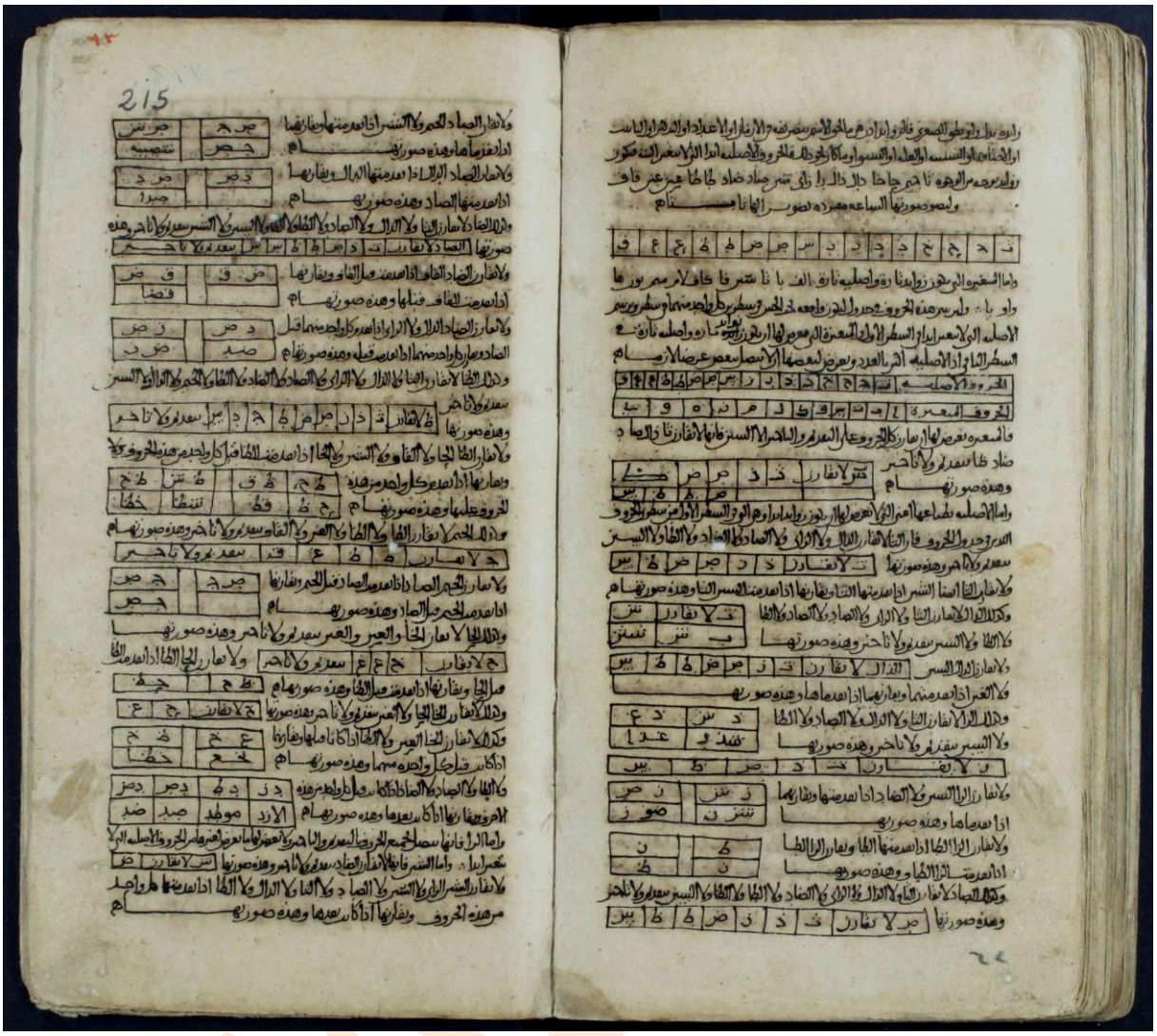
Kriptolojinin bilinen tarihinde belirtildiği gibi, kriptanalizin temelleri on beşinci yüzyılda değil, altı yüz sene önce, dokuzuncu yüzyılda Arap filozof ve bilim adamı El-Kindi tarafından atılmıştır. El Kindi'nin sıklık (frekans) analizi yöntemi o denli sağlam ve bir o kadar pratiktir ki kriptanalizin elifbasını oluşturmuş, yüzyıllar boyu kullanılagelmiştir.

> Arap bilim adamı ve düşünürü Ebu Yusuf Yakub ibn İshak El-Kindi (801-873) yetmiş yıllık ömründe çok sayıda ve farklı konularda kaleme almış olduğu iki yüz yetmişten fazla kitap ve risale bulunmaktadır çeşitli kütüphanelerde. Kriptanalizin temellerini atan risalesinden başka felsefe, mantık, matematik, geometri, eczacılık, kimya, astronomi, optik, armoni ve daha birçok konuda eserler veren El-Kindi'nin yaşadığı zamanın ne denli ilerisinde olduğunu anlatmaya sadece şu bile kâfidir: El-Kindi, elementlerin kimyasal yöntemlerle değiştirilemeyeceğini söylüyor, değersiz madenlerden altın elde etmeyi amaçlayan simya saçmalığını reddediyordu. (Simya ki daha yüzyıllar boyu Avrupa bilimini(!) esir alacaktı.)
>
> El-Kindi'nin 1987'de İstanbul Süleymaniye Kütüphanesi'nde ortaya çıkarılan risalesinin adı: *Risale fi istihraç el muamma* (İng. *A treatise on deciphering of cryptographic messages*); yani, gizin açığa çıkarılması hakkında risale. Gerek bu risalede, gerek dönemin Arap bilim adamlarının eserlerinde kriptolojinin temel kavramları Arapça kelimelerle ifade edilmektedir -ki bu durum, daha önce değinilen, kavramların dildeki yeri ve bilim dilinin gelişmesi mevzuuna bir başka örnektir. Bir zamanlar kriptoloji ve matematik kavramlarını -dolayısıyla bilim dilini- geliştirmiş olan Araplar şimdi ise aynı kavramları Batı dillerinden dönüştürülmüş haliyle öğreniyorlar kendi üniversitelerinde.

İstanbul Süleymaniye Kütüphanesi’nde 4832 numarayla kayıtlı El-Kindi’nin kitabından sayfalar:



Risale fi istihraç el muamma



°° Evrim

Kriptoloji, zaman içerisinde evrim geçirmiştir, geçirmektedir, geçirecektir. Bu sürekli evrimi belirli dönemlere ayıracak olursak; birinci dönemde, kâğıt kalemle yapılan yerine koyma veya yerini değiştirme uygulamaları; ikinci dönemde ise elektromekanik cihazlar vasıtasıyla gerçekleştirilen uygulamalar söz konusuydu. Matematik ve bilgisayar bilimleri üçüncü döneme damga vurmuş ve kriptolojiyi bir başka boyuta taşımıştır.

Kriptolojinin temelinde matematik vardır. İleri bilgi işlem teknolojileri ile birlikte matematikteki çarpıcı gelişmeler sayesinde kriptoloji günümüzde çok farklı şekilde uygulanmaktadır. Her ne kadar yerine koyma ve yerini değiştirme yöntemleri ve modulo aritmetik temel olarak var olsa da yeterli olmamaktadır. Büyük bloklar, çok büyük asal sayılar, çok çok uzun şifreler, ters çevrilemeyen fonksiyonlar, vesaire…

> Her şey artık bulutta. Buluttaki uygulamadan yararlanmak için bilginizi buluta gönderiyorsunuz, uygulamayı kullanıyor ve işlenmiş bilgiyi geri alıyorsunuz. Peki, buluttaki uygulamanın bilginizin ne olduğunu tam olarak bilmeden çalışmasın ve bilginizi işlemesini; hem gönderdiğiniz ham bilginin hem de geri aldığınız işlenmiş bilginin başkaları tarafından görülmemesini nasıl sağlarsınız; nasıl emin olursunuz? Mesela diyelim ki buluttaki çarpım işlemcisini kullanarak elinizdeki sayılarının çarpımını bulmak istiyorsunuz. Bu sayıları buluta gönderiyorsunuz ve çarpım işlemcisi onların ne olduklarını bilmeden çarpma işlemini yapıp sonucu buluyor ama bulduğu sonucun ne olduğunu o da bilmiyor. Tüm bu sayılar yolda gidip gelirken araya giren kimse onların ne olduklarını anlamıyor. İlginç, değil mi?..

Kriptografi, kriptanaliz, steganografi ve steganaliz yöntemleri artık gelişkin algoritmalar ve bunları destekleyen güçlü işlemciler ve diğer donanım ve yazılım vasıtasıyla gerçekleştirilmektedir. Bir zamanlar kriptanalistlere kök söktüren şifreli metinler şimdilerde herkesin ulaşabileceği, basit donanım ve yazılım kullanarak saniyeler mertebesinde çözülebiliyor.

> Elli sene evvel uzaya insan gönderen bilgisayarlar şimdinin cep telefonları ile dahi kıyaslanamayacak basitlikte ve hantaldı. Daha otuz sene önce kullanmakta olduğum, zamanın teknolojisine sahip bir sabit disk ünitesi 300 MegaByte kapasiteliydi ama neredeyse bir çamaşır makinesi kadar yer kaplıyordu ve birkaç kiloWatt güç harcıyordu. Şimdi 300 MegaByte'ın yüzüne bile bakmıyor kimse. Şimdilerde on bin misli kapasiteli 3 TeraByte disk ünitesi avuç içi kadar yer kaplıyor ve 10 Watt'ın altında güç harcıyor; fiyatı da el yakmıyor.
>
> Peki, bunun kriptolojiyle alakası ne diyeceksiniz. Kriptolojiyi en ileri seviyede uygulayan kurumlar mutlaka en gelişkin -hatta süper- bilgisayarları kullanıyor olsalar dahi yine de işlem ve hafıza kapasiteleri "sayı"larla ifade ediliyordu. Şimdi ise, bu tür kurumların (mesela NSA) kullanmakta olduğu günümüzün ileri teknoloji bilgisayarlarının miktarı "dönüm"lerle -"acre"larla- ifade edilmektedir. Varın siz tahmin edin ne denli devasa işlem ve hafıza kapasitesine sahip olduklarını...

Kriptolojinin iki bileşeni olan kriptografi ve kriptanaliz birbirini besleyerek evrimin gerçekleşmesini sağladılar. Şöyle ki: yeni bir ihtiyaç ortaya çıktığında, uygun olduğu düşünülen bir kriptografik yöntem geliştirilir; bilahare bu kriptografik yönteme karşı

bilinen kriptanaliz yöntemleriyle saldırarak açıkları bulunmaya çalışılır. Bulunan açıkları kapatmak, zaafları gidermek için kriptografik yöntem revize edilir, geliştirilir. İteratif bir evrim söz konusu ama iterasyonu bir yerde sonlandırıp yöntemi kullanmak gerekiyor. Belirli bir güvenlik ve güvenilirlik seviyesine ulaşıldığında o kriptografik yöntem kullanılır ve ümit edilir ki bir başkası yepyeni bir kriptanaliz yöntemiyle şifreyi çözmesin. Bu durumda kriptografik yöntem yeniden revize edilir (tabii, edilebilirse). Bu revize etmeler kriptografik yöntemin evrilmesini ve nihayetinde gelişmesini sağlar (tabii ki bir yere kadar).

> Peki ya siz değil de bir başkası o kriptografik yöntemde bir açık tespit eder ve bunu size söylemezse?..
>
> İyisi mi, dışarıdan izlemektense evrimin içerisinde yer almalı, onun parçası olmalı.

Geleneksel kriptografide hiç kimse, hiçbir zaman emin olamaz yöntemin tamamen güvenli ve güvenilir olduğundan.

Modern zamanlarda kriptoloji bir başka boyuta ulaşmış, algoritmanın "güzelliği"nin yanı sıra hesaplamanın zorluğu da önem kazanmıştır. Çözüme ulaşabilmek için artık ne denli hızlı ve büyük işlem gücüne ve bununla ilintili olarak, ne kadar uzun süreye ihtiyaç olduğu öne çıkmaktadır. Bu yaklaşımda, kriptanalizin yapılabilirliğinin, şifrenin kırılabilirliğinin sadece bir zaman meselesi olduğu baştan kabul edilmektedir.

°° Şebeke Bütünlüğü

Haberleşmenin bir *şebeke* (*ağ, network*) üzerinde yürütüldüğü göz önüne alındığında, haberleşmenin gizliliği kadar önemli başka meselelerin de halledilmesi gereği ortaya çıkmaktadır. Bunlar: *gizlilik* (*confidentiality*), *sahihlik* (*authentication*), *inkâr edilemezlik*, *(non-repudiation*), *bütünlük* (*integrity*) olarak sıralanabilir. (Aralarında önem sırası yoktur; haberleşmenin sağlıklı yürütülmesi bakımından her biri diğeri kadar önemlidir.)

Gizlilik (Confidentiality): Ağ üzerinde dolaşan bilginin gizli kalması, muhatapları haricinde kimsenin bu bilgiye ulaşamaması temin edilmeli. Kriptolojinin mesajı gizlemeyle, şifrelemeyle ilgili işlevi olan kriptografi işte bu gizliliği temin etmeye yaramaktadır.

> Medeni birçok ülkede olduğu gibi, ülkemizde de **haberleşme gizliliği anayasal güvence altındadır**. **Herkes, haberleşme hürriyetine sahiptir ve haberleşmenin gizliliği esastır**.
>
> Bilginin aktarılması veya depolanması durumunda gizliliği sağlayacak, bilgiyi koruyacak, yetkisiz ellere geçmesini engelleyecek tedbirlerin başında şifrelemek, yani kriptografiden yararlanmak gelir. (Tabii, steganografi veya silahlı muhafız gibi yöntemler de vardır ama en kullanışlı ve yaygın olanı kriptografidir.)
>
> Kriptolojide çok kullanılan benzetmeyle; Alice ile Bob, aralarındaki mektuplaşmayı başkasının görmesini, duymasını istemezler. Mektuplar Eve tarafından ele geçirilse bile okunamamalı.

Sahihlik (Authenticity): Kimlik doğruluğudur kastedilen. Birbirleriyle haberleşen taraflar mesajı gönderen ve alanın gerçekten göndermesi ve alması gereken kişiler olduklarından emin olmalılar. İmza, işte bunu temin eder.

> Alice ile Bob, mektupların doğru kişiden geldiğinden ve yine doğru kişiye gönderildiğinden emin olmak isterler. Eve, kendini Alice gibi göstererek Bob'u kandıramamalı (veya Bob gibi göstererek Alice'i).

İnkâr edilemezlik (Non-repudiation): Gönderilen mesajın daha sonra inkâr edilememesinin temini gerekir. İmza, bu amaca hizmet eder.

> Alice, mektubunda Bob'a bir söz vermişse daha sonra inkâr edememeli.

Bütünlük (Integrity): Gönderilen mesajın bütünlüğü bozulmamalı. Mesajın özetinin (hash) alınması ve muhataba gönderilmesi bütünlüğün sağlanmasına yardımcı olur.

> Bob bir şiir göndermişse Alice'e, hecesinin bile değişmesi vezni bozar.

Modern kriptoloji -gizliliğin yanı sıra- bu meselelerin en uygun (etkin, kolay, çabuk) şekilde halledilebileceği yöntemleri geliştirmekle uğraşmaktadır.

°° Dizi mi Blok mu?

Elli yıl öncesine kadar şifreleme genellikle bir dizi bilgi üzerinde yapılıyordu. Her bir karakter (harf, rakam, Byte, bit, vs.) sırayla ele alınıyor ve değiştiriliyordu. Bu yüzden bu tür şifreleme sistemleri *dizi şifreleme* (*stream cipher*) olarak adlandırılır. Ancak, bilgisayarların kullanılmaya başlamasıyla bu yöntem hantal ve uzun zaman alır oldu. Düz metindeki karakterleri tek tek ele almak yerine büyük bir blok halinde şifrelemek eskiden yapılamazken, gelişen bilgi işlem teknolojisi sayesinde kolaylıkla yapılır oldu. Günümüz kriptografisi daha ziyade *blok şifreleme* (*block cipher*) üzerine gelişmiştir.

Blok şifrelemede düz metnin belirli uzunluktaki bir bölümü blok halinde değiştirilebilir, tüm blok ters çevrilebilir, bloklar birbiriyle yer değiştirebilir veya bir işlemden geçirilebilir. Böylece, *karıştırma* ve *dağıtma* işlemleri çok daha kısa süre zarfında gerçekleştirilmiş ve gerekli *karışıklık* (*confusion*) ile *dağınıklık* (*diffusion*) elde edilmiş olur.

> Karışıklık ve dağınıklık niçin gerekli diye merak edenlerin Shannon'a başvurmalarını öneririm. Kendisi, "bilgi kuramı - information theory"nin piri olmanın yanı sıra kriptolojinin de piridir. Normal...

Karıştırma (*confusion*), şifrelenmiş metin ile anahtar (key) arasındaki ilişkinin anlaşılmasını engellerken; *dağıtma* (*diffusion*), şifrelenmiş metin ile düz metin arasındaki ilişkinin anlaşılmasını engeller.

Blok şifreleme tekniği temelde bir *simetrik* şifreleme tekniğidir. S-box denilen *yerine koyma* (*substitution*) işleminin yapıldığı işlemci kutucuklarında *karıştırma* işlemi gerçekleştirilir. P-box denilen *değiştirme* (*permutation*) kutucuklarında ise *dağıtma* işlemi gerçekleştirilir. S-box ve P-box işlemlerinden elde edilen ara sonuçlar şifreleme

algoritmasında belirtildiği şekilde ve sayıda tekrarlanarak sonuç elde edilir. Söz konusu algoritma ve kutucuklarda gerçekleştirilen işlemler tersine çalıştırılabildiği için, şifreli metin de benzer bir süreçten geçirilerek düz metine ulaşılabilir.

> Blok şifrelemedeki *değiştirme* (*permutation*) işleminin klasik kriptografideki *yerini değiştirme* (*transposition*) işlemine karşılık geldiği; dolayısıyla, *yerine koyma* (*substitution*) ve *yerini değiştirme* (*transposition*) işlemlerinin birlikte uygulandığı söylenebilir.

Blok şifreleme farklı şekillerde yapılabilir; kimi yöntemin güvenlik zaafı varken kimi yöntemin uygulanması uzun zaman almaktadır. Uygulamanın özelliğine göre uygun yöntem kullanılmaktadır.

> Blok şifrelemenin matematiği bu derlemenin sınırlarını aşar; ancak yine de en basit haliyle birkaç örnek vermekte yarar var.
>
> Diyelim ki düz metin: patriotlar gelsin
>
> Anahtar: *GUMUSHANELILESTIREMEDIKLERIMIZDEN MIYDINIZ*
>
> *GUM SHANELI T R D K Y Z*

p	a	t	r		G	U	M	S	
i	o	t	l		H	A	N	E	
a	r	g	e		L	I	T	R	
l	s	i	n		D	K	Y	Z	

> Düz metin bloğu ile şifre anahtarı bloğunu mod 26 (modulo 26) toplayalım.

16	1	20	18		7	21	13	19		23	22	7	11
9	15	20	12		8	1	14	5		17	16	8	17
1	18	7	5		12	9	20	18		13	1	1	23
12	19	9	14		4	11	25	26		16	4	8	14

W	V	G	K
Q	P	H	Q
M	A	A	W
P	D	H	N

> Buraya kadar düz metin bloğu ile şifre anahtar bloğunu modulo 26 aritmetik ile toplayarak *yerine koyma* (*substitution*) uyguladık.
>
> (Harflerle uğraştığımız için bu örnek daha kolay anlaşılıyor. 10001101 gibi bitlerle uğraşsaydık, *ya-ya* (*XOR*) işlemini tercih ederdik.)

Şimdi de satırlarda *yerini değiştirme* (*transposition*) uygulayalım.
Sütunları *1 3 4 2* şeklinde sıralayalım.

W	V	G	K		W	G	K	V
Q	P	H	Q		Q	H	Q	P
M	A	A	W		M	A	W	A
P	D	H	N		P	H	N	D

Satırları önce soldan sağa ve sonra yukarıdan aşağıya yazalım.

Şifrelenmiş metin: **WGKV QHQP MAWA PHND**

Çok karmaşık gibi görünse de, *yerine koyma* (*substitution*) bölümü aslında klasik şifrelemedeki çok alfabeli (polyalphabetic) yerine koyma şifrelemesinden farklı değil. Demek ki blok şifreleme mutlaka kuvvetli şifreleme anlamına gelmiyor. Özen gösterilmezse, blok şifreleme, dizi şifrelemeden farksız olur.

Mesela, şöyle olsaydı:

p	a	t	r		3	3	3	3		S	D	W	U
i	o	t	l		3	3	3	3		L	R	W	O
a	r	g	e		3	3	3	3		D	U	J	H
l	s	i	n		3	3	3	3		O	V	L	Q

Şifrelenmiş metin: **SDWU LRWO DUJH OVLQ** İşte, en basit Sezar şifresi…

Yukarıdaki örneklerin aksine, iyi tasarlanmış blok şifre algoritmalarının S- ve P-kutucukları, arzu edilen *karıştırma* (*confusion*) ve *dağıtma* (*diffusion*) işlevini sağlamalı ve -gerek şifrelerken gerekse şifreyi çözerken- kabul edilebilir işlemci kapasitesi kullanmalı ve tabii ki hızlı çalışmalı.

Cep telefonuyla konuşurken, söylediğinizin karşı tarafa üç saat sonra ulaşmasını, telefonun yirmi kilo ağırlığında ve koltuk büyüklüğünde olmasını istemezsiniz.

Günümüzün şifreleme algoritması Advanced Encryption Standard (AES), bir zamanlar çok yaygın olan ancak şimdilerde pek kullanılmayan Digital Encryption Standard (DES) ve çok eski günlerden Hill şifresi, blok şifrenin çok bilinen örnekleridir.

°° Simetrik mi, Asimetrik mi?

Şifreleme sistemleri genelde *simetrik* ve *asimetrik* olarak sınıflandırılabilir.

Simetrik sistemlerde mesaj, bir şifre anahtarı ve kripto algoritması vasıtasıyla şifrelenir; yine aynı anahtarı kullanarak ancak algoritmayı bu kez ters çalıştırarak şifre çözülür.

Mesela, mesaj eğer Sezar şifresi kullanarak kaydırma anahtarı=2 ile şifrelenmişse, şifreli mesajdaki harfler geriye doğru iki kaydırılarak şifre çözülür.

Daha karmaşık algoritmalar ve şifre anahtarları için de durum aynıdır. Aynı algoritmaya sahip olan gönderici ve alıcı, aynı anahtarı kullanarak şifreli mesaj gönderip alabilirler. Tabii ki araya giren bir başkası da aynı algoritma ve anahtarı kullanarak şifreli mesajı çözebilir veya yanıltıcı mesaj gönderebilir. Şifreleme işlemi $\mathbf{C=f_K(P)}$ şeklinde; şifrenin çözülmesi ise $\mathbf{P=f_K^{-1}(C)}$ şeklinde ifade edilebilir. Görüldüğü gibi, aynı **K** anahtarı hem şifreleme hem de şifreyi çözmek için geçerlidir. Şifrelemede kullanılan $\mathbf{f_K}$ fonksiyonunun tersi şifreyi kırmada kullanılır. Bu yüzden, bu tür şifreleme "simetrik" olarak tanımlanmaktadır.

Simetrik sistemlerde her iki tarafta da aynı algoritmanın ve anahtarın olması koşulu sistemi güvenli kılar. Ancak şifre anahtarlarının dağıtılmasının yönetimi oldukça zordur. Mesajı gönderen, onu şifre anahtarı ile şifreledikten sonra alıcıya gönderiyor. Alıcının şifreyi çözebilmesi için şifre anahtarını da ona göndermesi gerekiyor; ancak, bu şifre anahtarı gizli olduğu için çok güvenli bir yöntemle alıcıya ulaştırılmalı. Aynı mesaj için hem gönderenin hem de alanın elinde aynı anahtar bulunmalı ve dahası, bu anahtar başkasının eline geçmemeli. Aynı anahtarın çok sayıda mesajda kullanılmaması (mümkünse her mesajda ayrı anahtar kullanılması) ve anahtarın tamamen rastgele karakterlerden meydana gelmesi gibi gerekler de göz önüne alındığında simetrik sistemin yönetilmesi çok zorlaşmaktadır.

Tek kullanımlık (OTP) şifre anahtarı -eğer doğru şekilde üretilmişse ve doğru şekilde kullanılırsa- en güvenli şifreleme yöntemidir. Ancak mesele, her mesaj için sadece bir kez kullanılan bu anahtarlar nasıl üretilecek ve nasıl dağıtılacak mesajı gönderene ve alana?

Bir haberleşme ağında **n** adet kullanıcı arasında **(n-1)n/2** iletişim kanalı vardır.

n=2	kanal=1	n=3	kanal=3
n=4	kanal=6	n=5	kanal=10
n=50	kanal=1225	n=100	kanal=4950
n=1000	kanal=499500	n=1 milyon	kanal=yaklaşık 500 milyar

100 kullanıcılı bir şebekede 4950 tane, birbirine benzemeyen şifre anahtarı oluşturulmalı ve güvenli bir şekilde ulaştırılmalı kullanıcılara. Bin kullanıcı olması halinde yaklaşık beş yüz bin güvenli anahtar üretmeli ve güvenli şekilde aktarılmalı.
Mümkün mü? Evet.
Pratik mi? Hayır.
Yönetilebilir mi? Hayır.
Güvenli mi? Hayır.

İkinci Dünya Savaşı'nın akabinde, Soğuk Savaş döneminde şifreli mesaj trafiğindeki artış kriptolojide (steganografi, kriptografi ve kriptanaliz dahil) önemli sıçramalara yol açtı. Birçok yeni algoritma geliştirildi ama hepsi simetrik sistemde olduğu için şifre anahtarlarının yönetimi, yani anahtarların üretimi, dağıtımı, korunması, imhası, kullanım kurallarının belirlenmesi ve bu kurallara riayet edildiğinin temini ve benzer birçok husus neredeyse içinden çıkılmaz derecede zorlaştı. Öte yandan, radar ağlarının

ve benzeri dinleme merkezlerinin bilgisayarları ile komuta merkezleri arasındaki yoğun sayısal bilgi akışının güvenli şekilde sağlanması ihtiyacı kriptografiyi bilgisayar şebekesinin ayrılmaz bir unsuru haline getirdi. Dolayısıyla, şifre anahtarlarının güvenli dağıtımı konusu acil bir sorun haline geldi. 1960 - 70'lerde tüm kriptologların hayaliydi bu soruna çözüm bulmak.

MIT mezunu matematikçi Whitfield Diffie, Stanford'da doktora yapmaktayken, yine Stanford'da profesör, elektrik mühendisi Martin Hellman ve onun öğrencisi Ralph Merkle ile birlikte anahtar dağıtımı meselesine çözüm arıyorlardı. 1975 sonuna doğru Diffie bir çözüm buldu. 1976'da Hellman ile birlikte yayınladıkları makale, *New Directions in Cryptography*, büyük ses getirdi camiada. *Diffi-Hellman Key Exchange* (anahtar alışverişi) olarak kriptoloji literatürüne geçen bu yöntem, bilahare 2002'de Merkle'in de adının eklenmesiyle *Diffi-Hellman-Merkle Key Exchang*e olarak anılır. Bu makale -simetrik sistemde olduğu gibi- mesaj gönderen ile alan arasında tek bir şifre anahtarını paylaşmaya gerek kalmadan şifreli mesaj gönderilebilen asimetrik sistemin mümkün olduğunu söylüyordu.

Stanford'dan Diffie, Hellman ve Merkle, *tek yönlü fonksiyon* vasıtasıyla anahtar dağıtımı meselesine çözüm bulunabileceğini gösteriyordu ama pratik bir çözüm sunmuyordu. Pratik çözüm, bir sene sonra MIT'den geldi. Ronald Rivest, Adi Shamir adlı bilgisayarcılar ve Leonard Adleman adlı matematikçi, bir yıl süren çalışmanın sonunda asimetrik şifrelemeyi mümkün kılan tek yönlü bir fonksiyon geliştirdiler. Mesajı gönderen kişi, alıcının kendisinin belirlemiş ve açık kanallardan herkese iletmiş olduğu anahtarı kullanarak oluşturulmuş olan tek yönlü fonksiyonu kullanarak mesajı şifreliyor ve alıcıya gönderiyor. Tek yönlü fonksiyon, adı üzerinde, tersine döndürülemez; bu yüzden, başka birinin -hatta gönderenin bile- bu şifreli mesajı açıp okuması mümkün değil. Sadece alıcı kendi belirlemiş olduğu tekyönlü fonksiyonu tersine döndürebildiği için aldığı mesajın şifresini çözebilir.

> Basit bir örnekle açıklayayım: Asma kilit, tek yönlü fonksiyona güzel bir örnektir. Elle basma-çekme işlemi sadece tek yönde çalışıyor; iki yönde değil. Elle basıldığında kilitlenir ama elle çekildiğinde açılmaz. Kilidi açmak için tamamen farklı bir şey, anahtar kullanmalı (çekiçle kırılabilir veya tabancayla ateş edilebilir); ama elle çekerek açmak mümkün değildir.
>
> Diyelim ki ben, arkadaşlarımın bana gönderecekleri hediyeleri kimsenin görmesini istemiyorum. Bunun için arkadaşlarıma üzerinde -tabii ki açık- asma kilitler olan kutular veriyorum. Asma kilitler çok sayıda ama hepsi tek bir anahtarla açılabiliyor. O anahtar ise bende duruyor. Herhangi bir arkadaşım bana hediye göndereceği zaman, hediyesini bu kutuya koyuyor, asma kilidi kapatıyor. (Artık kendisi dahi açamaz o kutuyu.) Kutuyu, kilitli halde bana gönderiyor. Yolda kötü niyetli biri varsa, -kilidi kırmadıkça- açamaz kutuyu. Kutu bana ulaşınca, elimdeki anahtarla kolayca açıyor ve hediyemi alıyorum. Başka bir arkadaşım bana hediye gönderecekse o da aynı yöntemi uyguluyor. Onun gönderdiği kutu bana ulaştığında da yine aynı anahtarla açıyorum kutuyu.
>
> Yüzlerce yıldır kullanılmakta olan asma kilidin matematik eşdeğerini bulmak ancak 1970'lerin ortalarında mümkün oldu ve böylece, bu basit koruma yöntemi kriptografinin en temel sorununa çözüm getirdi.

> İmkânsız gibi görünen çözümü bulmak için -çoğu zaman olduğu gibi- bilinen, alışılmış paradigmanın dışına çıkmak gerekir. O zamana dek kullanılan simetrik kriptoda gönderen belirlerdi şifreyi; halbuki, asimetrik kriptoda -asma kilit örneğinde olduğu gibi- mesajı gönderen değil, alan belirliyor şifreyi.

Açık Anahtar Kriptografi (*Public Key Cryptography*) yöntemi böylece bulunmuş ve pratik hale getirilmiş oldu. Artık şifreli mesaj gönderen ve alan taraflar arasında şifrenin çözülmesini sağlayan ortak anahtarın aktarılması gerekmemektedir.

Açık Anahtar Kriptografi yönteminde, şifrelemek ve şifreyi çözmek için farklı anahtarlar kullanıldığından, asimetrik bir sistem söz konusudur. Bunun karşıtı olan simetrik sistemde, yani *Gizli Anahtar Kriptografi* (*Secret Key Cryptography* veya *Private Key Cryptography*) yönteminde ise şifrelemek ve şifreyi çözmek için aynı anahtar kullanılmaktadır. Dolayısıyla, şifreli mesaj gönderen ile alan arasında şifre anahtarı aktarımı gerekmektedir (ki ne denli zor, karmaşık ve güvensiz olduğu daha önce belirtilmişti).

Mucizevi çözüm gibi görünen asimetrik Açık Anahtar Kriptografi yöntemi, simetrik Gizli Anahtar Kriptografi yönteminin yerini alabildi mi? Hayır. Çünkü her ikisinin de yeri ayrı; her ikisinin de olumlu ve olumsuz yönleri var. En önemlisi, Gizli Anahtar Kriptografi ile aynı güvenlik seviyesini elde edebilmek için Açık Anahtar Kriptografide çok daha uzun şifre anahtarları kullanmak gerekir ki bu durum işlem süresini, dolayısıyla şifreyi çözme süresini uzatmaktadır. Ayrıca, tek yönlü fonksiyonlar bir yönde "kolay"ken diğer yönde "imkânsız" değiller; sadece "çok zor"lar. Bilgi işleme teknolojilerindeki hızlı ilerleme sayesinde bugün çok zor olan yarın kolay olabilir.

> İngiltere'nin kriptoloji üssü olan devlet haberleşme merkezinde de (Government Communications Headquarters - GCHQ) anahtar aktarma meselesi üzerinde çalışanlar vardı, tabii ki. GCHQ'nun yan kuruluşu Haberleşme-Elektronik Güvenlik Grubu'nda (Communications-Electronics Security Group - CESG) çalışan ve anahtar aktarımı meselesine çözüm arandığından haberdar olan James Ellis çok önceleri okumuş olduğu bir makaleyi hatırladı. Amerikan Bell Laboratuarlarının bir yayınında telefon görüşmelerinin dinlenmesinin engellenmesi amacıyla ilginç bir yöntem öneriliyordu: Alıcı, eğer telefon hattına kendi yarattığı gürültüyü yüklerse, hattı dinleyen konuşmayı anlayamaz ama alıcının kendisi o gürültüyü sinyalden ayırarak konuşmayı anlayabilir. İşte bundan esinlenen Ellis, kriptografinin en önemli meselesi olan anahtar dağıtımı meselesinin çözümünün mümkün olduğunu 1969'da gösterdi. Bu durumda şifrelemeyi gönderen değil, alan taraf yapıyordu. (İmkânsız görünen meselelerin çözümü için alışılmış paradigmanın dışına çıkmak gerektiğinin güzel bir örneğidir bu.)
>
> James Ellis çözümü bulmuştu ama nasıl gerçekleştirilebileceğini bulamamıştı; ancak var olduğundan emindi, çünkü teorik kanıtı vardı. Mesele artık bunun olup olamayacağı değil, ne şekilde olacağına indirgenmişti. Doğrusu, saman yığınında iğne aranıyordu. Umutsuz gibi görünse de umut vardı, çünkü iğnenin var olduğu biliniyordu. Mesele, iğnenin bulunmasıydı sadece.
>
> Çözüm 1973'te geldi. Üniversiteden henüz mezun olmuş matematikçi Clifford Cocks adlı bir matematikçi katılmıştı GCHQ kadrosuna. Yeni gelen birinin yüksek gizlilik dereceli şifre programlarında çalışması için zaman gerektiğinden, bir süre Ellis'in

meselesi ile ilgilenmesini istedi amiri. Yirmi üç yaşındaki Cocks çok kısa sürede buldu çözümü. Bulduğunun ne denli önemli olduğunun farkında değildi; hatta pek umursamamıştı bile. "Bana bir problem verdiler, ben de çözdüm; hepsi bu," diyordu. Çözümü gören amiri derhal GCHQ üst yönetimini haberdar etti ve her şey kalın bir gizlilik perdesi ile örtüldü. Daha sonra bu çözümü kendisi gibi GCHQ kadrosuna yeni katılmış olan çocukluk arkadaşı, matematikçi Malcolm Williamson ile paylaştı. Williamson çözümü yanlışlamak için çok uğraştı ama tüm çabasına rağmen çözüm gayet sağlam şekilde oradaydı.

James Ellis, Clifford Cocks ve Malcolm Williamson tarafından geliştirilen asimetrik kriptografi 1975'te GCHQ bünyesinde biliniyordu; ancak, İngilizler bu gelişmeyi çok gizli olarak sınıflandırdıkları için kriptoloji camiası haberdar olmadı, ta ki 1997'de gün ışığına çıkana dek. Sonunda, Amerikalı mucitler çok meşhur ve zengin oldular ama İngiliz mucitler birer plaket ile yetinmek durumunda kaldılar. James Ellis plaketini alacak kadar yaşayamadı; üç hafta önce öldü.

°° RSA

Asimetrik kriptonun en yaygın, bilinen algoritmalarından biri MIT'den Ronald Rivest, Adi Shamir ve Leonard Adleman tarafından geliştirilmiş olan algoritmadır.

Esasen iki bilgisayarcı, Rivest ve Shamir algoritmayı geliştirmişler, matematikçi Adleman'ın kontrol etmesini istemişlerdir. Çalışmalarını üçünün ismiyle yayınlamaları önerisine Adleman karşı çıkmıştır, buluştaki kendi katkısını azımsadığından. Diğerlerinin ısrarı üzerine, sıralamada kendi adını en sona koymaları kaydıyla kabul etmiştir. Bu yüzden, ARS değil, RSA olarak adlandırılmıştır bu buluş.

Asimetrik şifrelemenin esası, bir yönde "kolay" diğer yönde "çok zor" tek yönlü fonksiyonlardır. Mesela, y=x çok kolay bir fonksiyondur; x'in her değeri için y'nin değerini kolayca bulabileceğimiz gibi, y'nin her değeri için de x'in değerini aynı kolaylıkla bulabiliriz. (x'in karşılığı olan y değerini bulmak kriptografi, yani şifreleme işlemidir; y'nin karşılığı olan x değerini bulmak ise kriptanaliz, yani şifreyi çözmektir.) Alfabenin üç harf kaydırılmasıyla oluşturulan Sezar şifresi y=x+3 için kolaylık söz konusudur. Ancak $y=3x^3+x^2+x+2$ için aynı şeyi söyleyemeyiz. Çözümü zor polinomlar kriptolojinin ilgi alanı olmuştur, hep. Benzer şekilde, büyük asal sayılar da ilgi alanındadır kriptolojinin; çünkü onların çarpımını bulmak kolaydır ama bu çarpımı faktörize etmek ve o asal sayıları bulmak o denli kolay değildir. İşte RSA algoritması bu esasa dayanmaktadır.

Çok basit bir örnek vermek gerekirse, mesela benim doğum günüm (ayın on altıncı günü) şifrelenecek sır olsun.

P=16 Düz metin "Plain text"

Arkadaşım Ali'ye bu sırrımı açacağım. Bu amaçla aramızda bir asimetrik şifreleme sistemi oluşturmak istiyoruz.

Ali iki asal sayı seçer: mesela **p**=3 ve **q**=11
(makul seviyede bir kripto sisteminde bu asal sayılar çok çok büyük olur.)

n=**pq** **n**=3x11=33 **n**=33

z=(**p**-1)(**q**-1)=2x10=20 **z**=20

Ali, bir başka asal sayı **k** daha seçer; öyle ki **z**'yi tam bölemesin. (5 olmaz.) mesela **k**=7

Ali "açık anahtar - public key" olarak **n** ve **k** değerlerini bana gönderir ve isterse başkalarına da yayınlar.

Ali'nin bir de kimseyle paylaşmayacağı bir "gizli anahtar - secret key" belirlemesi gerekir.

kj=1 (mod **z**) olacak şekilde 7**j**=1 (mod 20) 7**j**=21 (mod **z** : modulo **z**)

j=3 Ali'nin gizli anahtarı

Artık **p**, **q** ve **z**'yi unutabiliriz (silebiliriz); kimsenin bilmesi gerekmiyor.

Ben, doğum günümü Ali'ye göndermek için onun açık anahtarı ile şifrelerim.

P^k=E (mod **n**) 16^7=268435456 (mod 33)=25=**E** Şifrelenmiş "Encrypted text"

Ali'ye göndereceğim şifrelenmiş mesaj, **E**=25 olur.

Aramızdaki şifrelemeyi bilmeyenler benim Ali'ye 25 gönderdiğimi görür; dolayısıyla, benim doğum günümün ayın 25'i olduğunu zanneder.

Peki bu 25'i alan Ali düz metine ulaşmak için nasıl çözecek şifreyi?

Ali, bu amaçla kendi gizli anahtarını "secret key" kullanır.

E^j=P (mod **n**) 25^3=15625 (mod 33)=16=**P** Düz metin Doğru!

Ali, kendisinin açık anahtarı ile şifrelenerek gönderilen şifreli mesajı (25) kendi gizli anahtarı ile çözerek düz metini (16) buluyor.

Peki, Ali'nin "açık anahtarına - public key" sahip olanlar bunu yapabilirler mi? Hayır.

(Ali'ye göndereceğim mesajı onun açık anahtarıyla şifreledikten sonra ben dahi çözemem.)

E^k=P (mod n) 25^7=6103515625 (mod 33)=31 Yanlış!

Görüldüğü gibi, bilmeyen tarafından tahmin edilemeyecek bir matematiksel bağlantı söz konusu. Her şey iki asal sayı, **p** ve **q** ile başlıyor. Bunlardan **n** ve **z** elde ediliyor. **z**'den **k** ve **j** elde ediliyor. Nihayetinde **k** ve **j** her ikisi de **n** ile bağlantılı. Bir başkası biraz gayret, biraz bilgisayar gücü ile her ikisini de bulabilir ve şifreyi kırabilir. Ama **n**'nin çok büyük asal sayıların çarpımından meydana gelmesi halinde bunu yapmak hayli zordur.

Peki, büyük asal sayılar ne kadar büyük?

25 Ocak 2013 itibariyle en büyük asal sayı: 2^57885161-1 yani $2^{57885161}$ -1 (on yedi milyon dört yüz yirmi beş bin yüz yetmiş haneli bir sayı).

Büyük asal sayıları bulma ve test etme yöntemleri var; mesele, bilgisayar zamanı... Bazı uygulamalarda binlerce kişisel bilgisayarın işlem kapasitesi -boş zamanlarında- bu amaçla kullanılmakta. Bugün, yarın, her an yeni bir büyük asal sayı bulunabilir. Ne var ki pratik uygulamalarda bu denli büyük asal sayılardan ziyade iki yüz, dört yüz haneli asal sayılar kullanılmaktadır.

°° Herkes İçin Kripto

Erişmiş olduğu muazzam teknolojik gelişmişlik düzeyine ilaveten kriptoloji çok önemli bir sıçrayış daha yapmıştır. Bir zamanlar sadece askerlerin, diplomatların, casusların, matematikçilerin ve bir avuç meraklısının gündeminde ve tekelinde olan kriptoloji, günümüzde herkesin kullanımına amade bir kolaylık haline gelmiştir. Milyonlarca kişi, kriptoloji uygulamalarını kullanmakta, kriptolojiyle iç içe yaşamaktadır her an; e-posta gönderirken, bankacılık işlemleri yaparken, kredi kartı kullanırken, televizyon izlerken, cep telefonuyla konuşurken...

> Cep telefonumuzu açtığımızda şifre gireriz ve bizim girdiğimiz şifreden üretilen bir başka şifre ile şifrelenir konuşmalarımız. Bu sayede, cep telefonumuz ile baz istasyonu arasında açıktan giden konuşmamızı araya giren birinin dinlemesi, anlaması imkânsız hale gelir. Benzer şekilde, e-posta hesabımıza ulaşırken kullanıcı adı ve şifre kullanıyoruz, başkaları okumasın diye yazdıklarımızı. Arabamızın kapısını açmak için uzaktan kumandanın düğmesine bastığımızda sadece bizim arabamızın kapısı açılıyor, başkasınınki değil. Banka kartımız ve dört haneli şifremizle her türlü banka işlemini güvenle yapıyoruz sokaktaki bankamatik makinesinde. Dahası, doğalgaz kullanıyor, televizyonda film izliyor, loto oynuyor, kredi kartıyla alışveriş yapıyor, resmi işlerimizi hallediyoruz.

Kurumsal veya ticari kripto uygulamalarının yanı sıra kişiler de özel haberleşmelerini kırılması çok zor kuvvetli kripto gizliliği içerisinde yapabilme imkâna sahipler artık.

> İngilizce *Public Key Cryptography* tabirinin Türkçeye *Açık Anahtar Kriptografi* diye tercüme edilmesi -daha önce değinmiş olduğumuz- kavramların dile olan etkisine bir başka örnek teşkil etmektedir. İngilizce tabirlerde kastedilen public, umumi kriptografidir; yani, halka açık, halk tarafından kullanılan umumi kriptografi. İşin ruhu şudur: kriptografi artık umuma açık hale gelmiştir. Public Key Cryptography ifadesinde matematiksel güzelliğin yanı sıra felsefi anlam da vardır.

Kişilerin kuvvetli kripto kullanmalarına imkân sağlayan en önemli adım, *PGP* diye adlandırılan yöntemin -devletlerin tüm engelleme çabalarına rağmen- yaygın kullanılıyor olmasıdır. Gizli Anahtar ve Açık Anahtar yöntemlerinin birlikte kullanıldığı bir karma sistem olan PGP yönteminde mesajın kendisi -simetrik- Gizli Anahtar Kriptografi yöntemiyle şifrelenirken, simetrik şifrelemenin anahtarı karşı tarafa -asimetrik- Açık Anahtar Kriptografi yöntemiyle aktarılmaktadır. Böylece, mesajın şifrelenmesinde nispeten kuvvetli olan simetrik kriptografi kullanarak mesajın gizliliği en üst düzeyde korunurken, anahtarın aktarılmasında ise asimetrik kriptografi kullanarak anahtar aktarımı sorununa çözüm getirilmiş oluyor.

> PGP, her ne kadar Türkçemize *Oldukça İyi Mahremiyet* olarak çevrilebilse de aslında gayet iyi gizlilik sağlamaktadır.
>
> Bir ülkede bireyin özgürlüğüne ne derece kıymet verildiğini anlamak için o ülkede umuma açık *PGP* veya benzeri kuvvetli kripto uygulamalarına izin verilip verilmediğine bakmakta yarar vardır. Hapse girme pahasına, Açık Anahtar kodunu telefon kulübelerinden tüm dünyaya yayan ve ileri derecede güvenli kripto uygulamalarının sadece devletin değil vatandaşların da kullanma hakkı olduğu

bilincinin yerleşmesine öncülük yapan Phil Zimmermann'ı saygıyla yad etmeden geçemeyiz.

°° Nasrettin Hoca'nın Türbesi ve Yılan Yağı

Güvenlik, bir yönetim meselesidir, esasında.

Güvenliği gizlilikle değil akıllı yönetimle sağlamak daha doğru bir yaklaşımdır. Akıllı yönetim, güvenliğin yanı sıra kaynakların optimum kullanımını da dikkate alır. Kaynaklar ve amaç dikkate alınmadan kurulan güvenlik sistemi kısa süre sonra atıl kalmaya mahkumdur.

Bir bakın, etrafta ne kadar çok manyetik detektör kapı var, çalışmayan veya her geçende öten ama kimsenin umursamadığı. Ne kadar çok ve karmaşık şifreler belirlememiz isteniyor ama kısa sürede kafamız karışıp hepsini en kolay hatırlayabileceğimiz -ve tabii başkalarının da kolayca bulabileceği- basitliğe indirgemek zorunda kalıyoruz.

Herhangi bir güvenlik sistemi, ne derece gizli, ne kadar ileri teknoloji içeriyor, ne kadar çok koruyucu önleme sahip, ne denli karmaşık olursa olsun, eğer iyi yönetilemiyorsa güvenli değildir, kesinlikle. Sadece göz boyar, o kadar.

Çok güvenli(ymiş) gibi görünen o kadar çok *Nasrettin Hoca'nın Türbesi* var ki sağlam kapıların, eli silahlı korumaların ardında...

Birçok güvenlik sistemi, özellikle kriptografi böylesi göz boyamaya çok müsaittir; çünkü tasarım ve uygulama genellikle gizlilik içerisinde yürütülür. Oysa, bu gizlilik çok yanıltıcıdır; olumsuz sonuçlara sebep olabilir. Güvenliğin akıllı yönetim yerine gizlilikle sağlandığı sistemler gerçekte en zayıf olanlardır; gizlilik kalkanı ardına sığınarak zaaflarının açığa çıkmasını engellemek isterler; daha doğrusu, engelleyebildiklerini zannederler.

1883'de Hollandalı dilbilimci Auguste Kerckhoffs von Nieuwenhof tarafından kaleme alınan *La Cryptographie Militaire* adlı kitapta belirtildiği ve bilahare Kerckhoffs prensibi olarak bilindiği üzere, bir kriptografik sistemin güvenilirliği kripto algoritmasının gizliliğine değil, şifre anahtarının gizliliğine bağlıdır.

Daha önce de belirtmiştim; kuvvetli olduğu zannedilen ama aslında işe yaramayan algoritmalar kriptanalistlerin en büyük yardımcılarıdır. Kriptografi tarihi, güvenli olduğunu iddia eden, kerameti kendinden menkul binlerce kriptografik algoritma ile doludur. Halbuki bu algoritmalar, herhangi bir kriptografik zaaf içerip içermediklerinin anlaşılması için, en ince ayrıntılarına kadar incelenmelidir. Zira, algoritmayı geliştirenin farkına varamadığı bir zaaf düşman tarafından fark edilebilir ve düşman bunu belli etmeden uzun süre bu algoritma ile şifrelenmiş mesajları okuyabilir. Mesajı şifreleyerek gönderen bunu bilemez dahi.

İlgi duyanlar için ekte hikâye edilen Enigma örneğinde olduğu gibi, ne denli gizlenirse gizlensin, algoritmanın açığa çıkma ihtimali vardır her zaman.

Öğrenme ve beceri kazanma süreçlerinin bilinen evreleridir; (1) bilinçsiz beceriksizlik, (2) bilinçli beceriksizlik, (3) bilinçli beceriklilik, (4) bilinçsiz beceriklilik. Bilinçsiz beceriksizlik evresinde kişi beceriksizdir, ancak beceriksizliğinin bilincinde değildir. Bu evre çok tehlikelidir, çünkü bilinçli olmadığı için kişi becerikli olduğunu zannediyor olabilir. İkinci evreye geçildiğinde tehlike tamamen kalkmasa da azalır, en azından yönetilebilir olur. En güvenli ve uygulayan için keyif verici evre üçüncüsüdür. Kişi, neyi, niçin ve nasıl yaptığını bilerek yapar işini. Dördüncü evrede kişi artık meseleyi aşmıştır. Yaptığı işi çok iyi yapar. O kadar iyi ki, düşünmeye -ve dikkat etmeye- dahi gerek duymaz. Bu denli aşırı özgüven ister istemez hataya yol açabilir. Kriptografi gibi hataların geri bildirimi olmayan (*) bir alanda hataya yer olmasa gerekir. Bu yüzden, bu konuda ciddi çalışma yapmaya niyetlenenlerin ikinci evreden başlamaları ve üçüncü evrenin ötesine geçmemeleri -bir başka ifadeyle, bilinçsiz evrelerden uzak durmaları- doğru olur.

> (*) Bir kriptografik sistemdeki hatayı bulan genellikle geri bildirmek yerine bundan faydalanmayı tercih eder.

Kriptografik algoritmalar konunun uzmanlarınca ayrıntılı incelenmeli (peer review), defalarca denenmeli, varsa zaafları açığa çıkarılmalı ve ancak güvenliği kanıtlandıktan sonra kullanılmalı. Herhangi bir kriptografik algoritmanın güvenliği test edilirken algoritmanın biliniyor olduğu baştan varsayılmalı.

Ne yazık ki kripto algoritmaları geliştirenlerin birçoğu gizlilik perdesi ardına sığınarak algoritma hakkında bilgi vermezler. Vermek istemezler; çünkü, yapmış oldukları veya yapmış olabilecekleri hataların, dolayısıyla algoritmanın işe yaramazlığının ortaya çıkmasını istemezler. Bu durum, bir zamanlar Amerika'da madrabazların panayırlarda, pazar yerlerinde sattıkları ve her derde deva olduğunu iddia ettikleri ancak içeriğini kesinlikle gizli tuttukları, *Yılan Yağı* (*Snake Oil*) denilen iksiri akla getirdiği için, kerameti kendinden menkul böylesi gizli algoritmalara *Yılan Yağı* denir.

> Kriptografik algoritma geliştirdiğini iddia eden bir kimse veya kurum eğer algoritmayı açıklamıyor, gizli tutuyor, "peer review"dan sakınıyorsa en temel kuralı ihlal ediyor, Yılan Yağı satıyor demektir. Bu ciddi ihlal genellikle "gizli" ve "milli" perdesi ardına saklanır. Artık matematik ne kadar milli ise?.. (İster istemez akla şu McCarthy dönemindeki, "Atomla ilgili sırları nasıl oluyor da veriyorlar fizikçilere?" sorusu geliyor.) Biri çıkıp, "Milli matematik nedir?" diye sorana dek bu çok kârlı Yılan Yağı ticareti sürecek gibi görünüyor. Hâlâ milli kriptoda ısrar edenlere tavsiyem: Alice, Bob, Carol'dan başlayabilirler.
>
> Şifreleme algoritması DES ve onun türevi Triple DES kırıldığı için yeni bir algoritma arayışına giren -ancak algoritmanın "milli" ve "gizli" olması gerektiğinden bihaber- ABD hükümeti uluslararası bir yarışma sonucunda, Belçikalı iki kriptoloğun geliştirmiş olduğu (ve kendi isimlerinin birleşimi ile adlandırdıkları) Rijndael algoritmasını seçmiş ve onu Gelişmiş Şifreleme Standardı (Advanced Encryption Standard –AES) adıyla kullanmaktadır. Hem ABD hükümetinin uygulamalarında hem de tüm dünyada birçok uygulamada AES tercih edilmektedir. Bu algoritma, seçim sürecinde ve daha sonra yüzlerce uzman tarafından incelenmiş, defalarca test edilmiş ve bu sayede bazı açıkları ortaya çıkarılıp düzeltilmiş olduğu için -şimdilik- herkesin güvenini

kazanmıştır. (Belki de biri çıkıp ABD hükümetine ve tüm dünyaya yanlış yaptıklarını söylemeli...)

Kriptografiyle uğraşan devlet kurumları veya başka ilgili kuruluşlar, güvenliği artırıcı bir önlem olarak kriptografik algoritmayı gizli tutmayı tercih edebilirler. Amaç, karşı tarafa uğraşacağı bir zorluk basamağı, bir engel daha çıkarmaktır. Algoritmayı gizli tutmakla kriptanaliz sürecinin daha zor hale geleceği zannedilir.

Olabilir. Güvenliğin ancak gizlilikle sağlanabileceğine inananların tercihidir; öte yandan karar verici yöneticilerin kulağına hoş gelir. İyi niyetli bir yaklaşımdır; ancak, unutmamak gerekir ki felakete giden birçok yol iyi niyet taşlarıyla döşenmiştir.

Gizliliği öne çıkaran kurumlar genellikle sahip oldukları imkânların ve yeteneklerin bilinmesini arzu etmezler. Bu, salt güvenlik açısından bakıldığında, doğru bir yaklaşımdır. Bazı kurumlar ise imkânsızlıklarının ve beceriksizliklerinin ortaya çıkmaması için gizliliği tercih ederler. Yine salt güvenlik açısından bakıldığında ise bu yanlış bir yaklaşımdır. Demek ki salt güvenlik açısından bakıldığında yanlışlar doğruları götürmekte, elde karar vermeyi kolaylaştıracak bir şey kalmamakta. Öyleyse, salt güvenlikten ziyade pratik, akılcı ve bilimsel yaklaşım öne çıkmalı.

Her ne sebeple olursa olsun, algoritmanın incelemeye açık olmadığı, gizli tutulduğu kriptografik yöntemlere kuşkuyla yaklaşmakta yarar vardır. Bilmeyerek -çoğu kez maalesef bilerek- Nasrettin Hoca'nın Türbesini veya Yılan Yağını özgün çözüm olarak sunan; üstelik, hamaset ve hamiyetle süsleyerek bu kandırmacayı sürdüren ve kendilerine inanan kişi veya kurumların ciddi zarar görmesine sebep olanlara karşı ihtiyatlı olmakta yarar vardır.

° Elektronik Harp (EH)

Bilginin iletilmesinde ve muhafazasında, kimi zaman üretilmesinde elektronik yöntemlerin kullanıldığı ortamlarda bilgi harbinin yürütülmesinde de yine elektronikten yararlanmaktan daha tabii ne olabilir? Elektromanyetik spektrumu etkin şekilde kullanabilmek, öte yandan düşmanın kullanmasını engellemek amacıyla yürütülen mücadele Elektronik Harbin (EW) esasını teşkil eder.

Elektronik Harp - EH (EW) faaliyeti, haberleşme için kullanılan radyo frekans bandından mikrodalga radar frekanslarına veya milimetrik dalga boyundan kızılötesi (infrared) hatta morötesi (ultraviyole) banda kadar çok geniş bir spektrumda yürütülür. Genel olarak elektromanyetik spektrumdan yararlanmak amacıyla yürütülen Elektronik Destek Tedbirleri - EDT (ESM) ve düşmanın yararlanmasını engellemeye yönelik Elektronik Karşı Tedbirler - EKT (ECM) şeklinde sınıflandırılabilir. Tabii, hemen her mücadelede olduğu gibi, engellemenin etkinliğini azaltmaya yönelik Elektronik Karşı Karşı Tedbirler - EKKT (ECCM) de vardır.

EKKKT de var mı diye sormayın.

Bugüne dek geleneksel harpte bir destek unsuru, kuvvet çarpanı olarak kullanılan elektronik harp, günümüzde elektromanyetik spektrumun savaş ortamı haline gelmiş olması sebebiyle bir harp unsuru olmuştur.

Esasında bilginin, daha doğrusu malumatın aktarılması demek olan *haberleşme*, bilgi harbinin en önemli konusudur. Öte yandan haberleşme, elektromanyetik ortamın yaygın kullanım alanı bulduğu uygulamaların başında gelir; dolayısıyla, elektronik harbin -birincil olmasa da- önde gelen hedefini oluşturmaktadır. Haberleşmeye yönelik elektronik harbin hedefleri kendi içerisinde çok çeşitli olabilir; mesela, haberleşme yayınının algılanması, yayın yapılan yerin tespiti, yayının muhatabı tarafından anlaşılmasını engellemek amacıyla karıştırılması veya muhatabın yanıltılması ve tabii ki bunlara karşı tedbirlerin uygulanması *haberleşme elektronik harbinin* bilinen uygulamalarıdır.

Elektronik harbin önemli bir uygulaması ise radar ile alakalıdır. Uçağı, gemiyi veya başka bir objeyi algılamaya yarayan radar sinyallerini bozmak, karıştırmak, engellemek elektronik harbin en temel uygulamalarıdır. Mesela uçak söz konu olduğunda, uçağın hızını veya mesafesini radarın yanlış algılamasını sağlamak o radarın kumanda ettiği hava savunma silahının etkinliğini büyük ölçüde azaltacak ve böylece uçağın zarar görmeden görevini yerine getirmesine yardımcı olacaktır. Misal: elektronik harp ile teçhiz edilmeden muharebe ortamına giden on uçaktan üçü sağ salim eve dönerken, elektronik harp ile teçhiz edilmiş on uçaktan yedisi eve döner. Bu bakımdan elektronik harp önemli bir kuvvet çarpanı olarak değerlendirilmektedir. Uçağın veya füzenin yaydığı kızılötesi veya morötesi ışınımı algılayan cihazları yanıltmak da bir başka elektronik harp uygulaması olarak öne çıkmaktadır.

> Yukarıdaki radar veya ışınım örneklerinde *bilgi* nerede, bilgi harbiyle alakası ne diye merak edenlere; bu uygulamalar, bilginin temel hali olan *veri* veya *malumat* üzerine odaklanmaktadır.
>
> Tabii şu da mümkündür: nihayetinde, radar veya haberleşme anteni sisteme giriş sağlayan bir kapıdır; bu kapıdan girip sistemin bilgi ağına, dolayısıyla bilginin işlendiği veya depolandığı yere ulaşarak bilgiyi manipüle etmek de bir bilgi harbi - elektronik harp uygulaması olabilir.

Ayrıca, tüm bu uygulamalara karşı geliştirilmiş olan tedbirler de elektronik harbin kapsamındadır. Mesela, elektronik harpçiler radarı yanıltmaya çalışırken radarcılar da yanılmamaya çalışırlar. Elektronik harpçiler, radarcıların tekniklerini, taktiklerini öğrenip bunlara karşı teknikler, taktikler geliştirirken radarcılar da bunları bertaraf edecek başka teknikler ve taktikler geliştirirler. Bu oyun böyle sürer, gider…

° Ağ Merkezli Harp

Ağ Merkezli Harp (*Network Centric Warfare*), bilginin üretildiği, saklandığı ve aktarıldığı bilgisayarların, çevre birimlerinin ve iletişim cihazlarının meydana getirdiği ağ (*şebeke, network*) üzerinde yürütülen; bilgiyi ele geçirme, bilgiye müdahale etme ve bilgiyi muhafaza etme mücadelesidir.

Haberleşme ve bilgi işlem teknolojilerinin günümüzde ulaşmış olduğu seviye, harpte kullanılan her unsurun, her birliğin, bataryanın, tankın, uçağın, hatta her bir askerin komuta kontrol ve iletişim ağında bir kesişme noktası (düğüm - node) olmasını mümkün kılmaktadır. Elektronik harbin bu komuta kontrol ve iletişim ağını hedef alması çok

doğaldır. Bu ağı ele geçiren düşmanın komuta kontrol sistemini yanıltabilir, işlevsiz hale getirebilir, hatta kendine zarar vermesini sağlayabilir.

Komuta kontrol ve iletişim şebekeleri askeri amaçların yanı sıra sivil amaçla da çok yaygın kullanılmaktadır. Bankalar, finans kurumları, sağlık kuruluşları, demiryolları, metrolar, trafik ışıkları, hava trafik kontrol sistemleri, barajlar, elektrik santralleri, gaz, su, elektrik iletim ve dağıtım şebekeleri, telefon şebekeleri ve daha birçok kritik işlev günümüzde bilgisayar ağları vasıtasıyla iletişim sağlamakta, bilgi alış verişinde bulunmakta ve yönetilmektedir. Hemen her endüstriyel tesis bir endüstriyel kontrol sistemi (Industrial Control System - ICS) vasıtasıyla yönetilmekte; bu amaçla muhtelif PLC, SCADA, DCS sistemleri kullanılmaktadır. Bu bilgisayar şebekelerinin ve kumanda merkezlerinin ele geçirilmesinin ne denli hayati sonuçlar doğuracağı aşikârdır: çöken bankacılık sistemi, havada çarpışan uçaklar, raydan çıkan trenler, açılan baraj kapakları, bozulan santraller, uzun süre giderilemeyen elektrik, su, gaz kesintileri, çalışmayan telefonlar, patlayan kimyasal reaktörler, çevreye yayılan zehirli gazlar, kargaşa, panik ve nihayetinde siyasi istikrasızlık…

> Stuxnet bilgisayar solucanı siber savaşın ne derece etkin olduğuna güzel ve güncel bir örnek teşkil etmektedir.
>
> [Nükleer yakıt veya bomba yapımında gerekli olan uranyum izotopu U235'i nükleer tepkimede yararı olmayan U238'den ayırabilmek için yüksek hızlı santrifüjler kullanılır. Bu ayırma işlemi *zenginleştirme* diye adlandırılır.] İran'ın nükleer yakıt hazırlama tesisi Natanz'da uranyumu zenginleştirmek amacıyla çalıştırılan binlerce santrifüjü denetleyen Uluslararası Atom Enerjisi Ajansı (IAEA) yetkililerinin dikkatini 2010 yılının başında bir şey çekti: santrifüjler, olması gerekenden çok daha fazla oranda arızalanıyordu. Daha sonra, bilgi güvenliği ile ilgili bir Belarus firması bu anormal arıza oranının sebebini açığa çıkardı. Stuxnet adı verilen bilgisayar solucanı yerel alan ağında (LAN) bir bilgisayara muhtemelen USB vasıtasıyla bulaştırıldıktan sonra Windows işletim sistemi ortamında bilgisayarlar arasında yayılıyor ve bu sayede SCADA sistemlerinde çok yaygın kullanılmakta olan Siemens Simatic STEP 7 ve WinCC yazılımları vasıtasıyla PLC'leri ve onların kumanda ettiği cihazları kontrol altına alıyordu. Stuxnet vasıtasıyla bir taraftan santrifüjlerin hızı aniden çok artırılıp yine aniden düşürülürken öte yandan kumanda merkezine sanki doğru hızda çalışıyorlarmış bilgisi gönderiliyor ve böylece kumanda merkezindeki operatörlerin bu anormal durumu algılaması engelleniyordu. Hızı aniden artırılıp aniden düşürülen santrifüjler kısa sürede arızalanıyor, devre dışı kalıyorlardı. Sonuçta, uranyum zenginleştirme işlemi ciddi ölçüde sekteye uğruyordu.

Askeri veya endüstriyel amaçlı ağ merkezli harbin başarılı uygulamalarında, saldırılan tarafın saldırıdan -iş işten geçene kadar- haberdar olmaması, saldırının vahametini misliyle artırmaktadır.

> Ağ merkezli harp saldırı unsurlarının komuta, kontrol, haberleşme, bilgi şebekesine gizlice girdiği, yayıldığı, yerleştiği, kendini gizlediği ve zamanı geldiğinde zarar verdiği düşünüldüğünde bu harp türünü kansere benzetmek yanlış olmaz. Öyleyse; kanserden korkma, geç kalmaktan kork.

Endüstriyel kontrol sistemlerinin (ICS) önceliği farklı olduğundan, endüstriyel kontrol sistemlerine yönelik ağ merkezli harp, istihbarat veya askeri amaçlı ağ merkezli harbe nazaran farklılık gösterir. Endüstriyel kontrol sistemlerinin öncelik sırası erişilebilirlik-bütünlük-gizlilik (Availability-Integrity-Confidentiality - AIC) olarak tanımlanır; halbuki, askeri ve güvenlik amaçlı ağ sistemlerinin önceliği gizlilik-bütünlük-erişilebilirlik (Confidentiality-Integrity-Availability - CIA) şeklinde sıralanmaktadır. Bu sebeple, endüstriyel kontrol sistemlerine yönelik ağ merkezli harp teknikleri veya bu sistemleri korumak için alınan tedbirler -askeri sistemlerden farklı- endüstriyel kontrol sistemlerinin önceliklerini, tasarım ve uygulama özelliklerini göz önüne almalıdır.

° İstihbarat

Bilgi operasyonlarının temelinde bilgiyi elde etmek, yani istihbar etmek, yani *istihbarat* vardır. İstihbarat daha ziyade malumat, enformasyon (*information*) üzerinde yürütülse de kimi zaman bilgi (*knowledge*) üzerinde de yürütüldüğü durumlar da söz konusu olur. Batı dillerindeki entelejans (*intelligence*) ise, bilgi toplamanın ötesinde, daha ziyade istihbar edilen enformasyonun değerlendirilmesi, yorumlanması ve faydalı sonuçlara varılmasına odaklanmaktadır.

Daha önce de ifade edildiği gibi, bilgi harbinin en ilkel ama temel hali bilgiyi ele geçirmek ve eldeki bilgiyi muhafaza etmek olsa da, ele geçirmenin ve muhafaza etmenin ötesinde, bilgiyi yönetmek, değerlendirmek, kullanmak çok daha etkili sonuçlar veren bir eylem olarak öne çıkmaktadır.

> Farklı kültürlerin kavramları farklı algılayışının bir örneğini *istihbarat* kelimesinde görebiliriz. Kelime, *istihbar etmek*, yani haber (Ar. *haber*) toplamaktan gelir. Batı dillerinde haber toplamanın karşılığı tabii ki vardır ama *istihbarat* kavramı söz konusu olduğunda *intelligence* daha doğru bir ifadedir ki *zekâ*, *kavrama*, *anlama* demektir.
>
> Haber, malumat toplama anlamında istihbarat söz konusu olduğunda batı dillerinde *enformasyon* tabiri kullanılır. (İng. information, Fra. information, İsp. información, İta. informazioni) Söz konusu olan değerlendirme, yorumlama anlamında istihbarat ise *entelejans* kullanılır. (İng. intelligence, Fra. intelligence, İsp. inteligencia, İta. intelligenza) Almancada da benzer bir durum söz konusu: enformasyon, malumat anlamında istihbarat söz konusu olduğunda *Information* kullanılırken, askeri veya sivil istihbarat söz konusu olduğunda gizleme, saklama, koruma, savunma anlamında *Abschirmdienst* veya *Abwehrdienst* tercih edilmektedir.
>
> Kelimelerdeki bu farklılık, ister istemez, kavramların geliştirilmesine ve uygulanmasına da yansımaktadır. Tarihsel süreçte kavramı sadece haber alma ile sınırlayan, karar verici "beyin"e bilgi aktaran "göz ve kulak" olarak kabul eden kültürlerde *istihbarat* tercih edilirken, "beyin"in parçası olarak kabul eden kültürlerde *entelejans* (*intelligence*) tercih edilmektedir.
>
> Bilgi harbi çerçevesinde istihbarat, önceleri sadece askeri amaçla dikkate alınıyor ve bu sebeple *askeri istihbarat* aslında *askeri haber alma* olarak değerlendiriliyordu. Halbuki, modern bilgi çağında askeri bilgi ortamının dışında ve ötesinde küresel bilgi ortamı söz olduğunda, askeri istihbarat artık haber almanın ötesinde anlam üstlenmek durumundadır. "Military intelligence, the great oxymoron" esprisi modern harp için

artık geçerli değildir. İşte bu değişiklik, sadece askeri istihbarat veya genel anlamda istihbaratın değil, topyekun bilgi harbinin omurgasını oluşturmaktadır.

Bu bağlamda, *espionage* kelimesinin Türkçemize geçişi de ilginç: *espiyonaj* dendiğinde saygı uyandırırken, *ispiyonculuk* dendiğinde aşağılama içermektedir. Ben yine de *istihbarat* (*haber alma*), *espiyonaj* ve *entelejans* (*intelligence*) terimlerinin etimolojisini uzmanına bırakıp Türkçemizdeki yaygın haliyle *istihbarat* terimini kullanacağım metin içerisinde.

Gerek açık, gerekse kapalı kaynaklara yönelik istihbarat faaliyetinde çeşitli yöntemler bir arada veya tek başına kullanılabilir; istihbarat, insan vasıtasıyla veya teknik yöntemlerle elde edilebilir.

Oldukça karmaşık olan istihbarat süreci genellikle, (1) planlama (ve yönlendirme), (2) toplama, (3) işleme (tasnif, değerlendirme ve yorum), (4) dağıtım (ve uygulama) gibi evrelerden oluşan bir *istihsal döngüsü* şeklinde işler. Toplanan *malumat* (*information*), istihbarat istihsal döngüsü sayesinde faydalı *bilgiye* (*intelligence*) dönüşür.

Gerek açık, gerekse kapalı kaynaklara yönelik istihbarat faaliyetinde çeşitli yöntemler bir arada veya tek başına kullanılabilir:

-- Açık kaynak istihbaratı (Open Source Intelligence - OSINT) hem insan, hem de teknik vasıtalarla yapılabilir.

-- Kapalı kaynaklara yönelik (gizli) istihbarat
    -- İnsan kullanarak yürütülen istihbarat (Human Intelligence - HUMINT)
    -- Teknik yöntemlerle yürütülen istihbarat (Technical Intelligence - TECHINT)
        -- Görüntü (Imagery) istihbaratı (IMINT)
        -- Sinyal (Signal) istihbaratı (SIGINT)
            -- Haberleşme (Communication) istihbaratı (COMINT)
            -- Elektronik istihbarat (ELINT)
        -- Network istihbaratı (NETINT)
        -- Ölçüm ve iz sinyal (Measurements and Signals) istihbaratı (MASINT)

Açık kaynak istihbaratı (OSINT), tanımından da anlaşılacağı üzere, radyo, televizyon, gazete, dergi, kitap, resmi bildiri, basın toplantısı, internet, kısa dalga telsiz, benzeri açık kaynaklardan veya henüz yayınlanmamış araştırma notları, teknik raporlar (grey literature) elde edilen istihbarattır. Açık kaynak istihbaratı, insan vasıtasıyla ve/veya teknik yöntemlerle elde edilebilir; ancak, teknik yöntemlerin ileriliğinden ziyade istihbarat toplayan veya değerlendirenin sezgi ve algı yeteneği öne çıkar.

Gizli, kapalı kaynaklardan elde edilen istihbarat *(espiyonaj)* için çeşitli yöntemler kullanılır ki bunların başında yine insan vasıtasıyla yürütülen HUMINT gelir. Yanı sıra, günümüzde teknolojinin ulaşmış olduğu seviyede, istihbarat istihsal döngüsünün hemen her evresinde teknik yöntemlerden de yararlanılmaktadır. Bunların önde gelenleri: gözetleme radarları veya uydulardan elde edilen görüntü üzerinde yürütülen IMINT; haberleşme (COMINT) ve elektronik sinyaller (ELINT) üzerinde yürütülen SIGINT

[yabancı enstrümantasyon istihbaratı (Foreign Instrumentation - FISINT) ve telemetri istihbaratı (TELINT) de bunun parçasıdır]; bilgisayar şebekesi üzerinde yürütülen NETINT; parametrik ölçüm ve iz sinyalleri üzerinde yürütülen MASINT olarak sıralanabilir.

° Propaganda ve Psikolojik Harp

Bilgiyi yönetmek kadar bilgiyi manipüle etmek de bilgi harbinin önde gelen amaçları arasındadır.

> Bilgiyi yönetmek ile manipüle etmek arasındaki çizgi pek belirgin değildir. Olamaz da; çünkü yönetmek bir bakıma manipüle etmektir. Mesela, kendisini izleyen radarın yayınını alıp, uçağın hızını farklı algılayacak şekilde değiştirerek radara gönderen elektronik harp sistemi aslında bilgiyi manipüle etmektedir. Benzer şekilde, araya girerek şifreli mesajı alan ve değiştirerek alıcıya ulaştıran aradaki şahıs da (*Man-in-the-Middle*) manipülasyon yapmaktadır.

Bilgi üzerinde manipülasyon farklı seviyelerde (veri, malumat, bilgi) yapılabilir; ancak, esas amaç algıda yanılgı sağlamaktır. Amaç algıda yanıltma olduğunda psikolojik harp ve onun bir vasıtası olarak propaganda öne çıkmaktadır. Bilginin daha ziyade içerik bakımından manipüle edilmesi söz konusudur burada.

> Görsel veya elektromanyetik veya sayısal veya bir başka türlü yanıltma amacıyla kullanılan kamuflaj veya sahte modeller (decoy) değil sözü edilen. Bunlar da mutlaka algıda yanılmaya sebep olurlar ama söz konusu psikolojik harp ve propaganda olduğunda amaç, bireyin zihinsel algılama, anlama ve karar alma mekanizmasını etkilemektir.

NE YAPMALI?

> Albert Einstein, "Üçüncü dünya harbin nasıl olacağını bilmiyorum ama eminim ki dördüncüsü taşla, sopayla olacak," demiş.
>
> Birinci Dünya Harbi kimyacıların, İkinci Dünya Harbi fizikçilerin savaşıydı; ancak, Üçüncü Dünya Harbinin matematikçilerin savaşı olacağı görüşünü ileri sürer Simon Singh, *The Code Book* adlı kitabında. Katılıyorum. Bilgi harbinin en önemli enstrümanı olan matematik, geleceğin savaş teknolojisinin temelini oluşturacak, kesinlikle. Savaş dilini bırakıp barış diliyle konuştuğumuzda yine aynı kesinlikle söyleyebilirim ki matematik, geleceğin barış içerisinde yaşam teknolojisinin temelini oluşturacak ve sürekliliğini sağlayacak.

Bu yeni yaşam ortamında hayatta kalabilmek, varlık sürdürebilmek için -öğreniminden ziyade- matematik eğitimi öne çıkarılmalı ve tabii ki uygulama imkânları yaratılmalı.

Niçin öğrenimden ziyade eğitime önem verilmeli? Çünkü, kısa değil ama orta ve uzun vadede toplumda matematik bilincinin artırılması öğretimle değil, eğitimle mümkündür, ancak.

Sporu alın mesela: Sporla barışık, onu bir yaşam tarzı olarak benimsemiş bir toplum hentbol sahasının ölçüleri veya futbolda ofsayt kurallarını öğretmekle yaratılamaz; yürüterek, yüzdürerek, top oynatarak, sırıkla atlatarak yaratılır.

Öğrenimin ötesinde eğitimin örneği olarak, Prof. Ali Nesin'in büyük özveriyle hayata geçirdiği Matematik Köyü projesini önemsiyor, övgüyle selamlıyorum. Keşke böylesi projeleri çoğaltabilsek; öncülerini desteklesek, hatta el üstünde tutabilsek. Geçen asrın izcileri gibi matematik dostu gençlere ihtiyacımız var bu asırda. (Matematik dostu gençlerin meslek olarak matematiği seçmeleri gerekmiyor; doktor, tüccar, avukat, hakim, siyasetçi, asker, kadastrocu, şekerlemeci, ev hanımı veya veteriner olabilirler.)

İzninizle, lisede okuduğum matematik kitaplarının kapağındaki SMSG harflerini hatırlayarak kapatacağım bu konuyu: Başlarda bir yerde değindiğim Sputnik meselesi, dönemin ABD yetkililerini ciddi tedbirler almaya yöneltti. Anladılar ki kendi iyi Almanları ile Rusların daha iyi Almanları arasındaki farkı ortadan kaldırmanın tek yolu işleri iyi Almanlara gerek kalmayacak şekilde kendilerinin yapabilmelerinden geçiyor. Ancak, dönemin lise matematik eğitimi bunu mümkün kılacak nitelikte değildi. Okul Matematiği Çalışma Grubu (SMSG) adıyla oluşturulan kuruluşun önderliğinde yeniden tasarlanan matematik eğitimi ve yazılan kitaplar Amerika'nın son yarım asırda bilim ve teknoloji alanında gerçekleştirdiği atılımın itici gücü olmuştur.

Yine de sanılmasın ki Amerika bu konuda liderdir ve bunu sürdürebilecektir. Aksine… Amerika, SMSG programını 1977'de terk etmiş ve her Amerika seyahatimde benim için vazgeçilmez bir eğlence yaratmıştır. Şöyle: Diyelim ki bir süpermarkette alışveriş yaptım ve kasaya 7 dolar 20 sent ödemem gerekti. Kasiyere bir 20 dolarlık banknot ile iki tane 1 dolar ve iki tane 10 sent uzatırım. Hatta, küçük bir kopya verir, para üstü olarak bir 10 dolarlık, bir de 5 dolarlık banknot vermesini söylerim. İşte o an o kasadaki kuyruk kilitlenir; kasiyer panikler, ne yapacağını bilemez olur, süpervizörünü çağırır. İşin içinden çıkamazlar. Sonunda, verdiğim bozuklukları iade eder ve 20 dolarlık banknotun üstünü verirler; 12 dolar 80 sent. Bu bakımdan, iddia ediyorum ki bizdeki ortalama matematik seviyesi Amerika'nın şimdiki haline nazaran çok daha ileridedir. Yapmamız gereken, SMSG benzeri programlarla sistemik olarak daha da ileri götürmektir.

Bilimin gelişmesine öncü olmakla yükümlü kurumların ve üniversitelerin değerli kaynaklarını asli görevlerinden ziyade ticari boyutu öne çıkan faaliyetlere yönlendirmeleri bir talihsizliktir. Tahsis edilmiş arazileri vergi avantajından yararlanmak isteyen şirketlere yüksek bedelle kiralamanın ötesine geçmelidir bilim.

Temel bilimlerin göz ardı edildiği, değer verilmediği ortamda matematiğin öne çıkarılmasını talep etmek anlamlı gelmeyebilir belki ama içinde bulunduğumuz yüzyılda güçlü olmanın, hatta ayakta kalabilmenin ön koşuludur bu.

Matematik köylerinin benzeri fizik köyleri, kimya köyleri, bilgisayar bilimleri köyleri olmalı.

Toplumun bekası için beden ve zihin sağlığının yanı sıra ahlaki değerler kadar, hukuk kadar, estetik kadar matematik de önem arz eder.

Matematiğin yanı sıra, bilginin iletildiği, işlendiği, muhafaza edildiği -elektrik, haberleşme, yazılım gibi- diğer disiplinlerde de eğitim ve uygulamayı yaygınlaştırmak, matematiğin zihinlerde yaratacağı sağduyu sayesinde bilgi harbi, bilgi güvenliği ve genel güvenlik meselelerinde daha sağlıklı, gerçekçi çözümler geliştirmek gerekir.

Çözüm, uzun vadeli düşünülmeli; uzun erimli politika geliştirilmeli ve günün koşullarına uyarlanarak ısrarla yürütülmeli. Mutlaka popülerlikten uzak durarak… Ve yine mutlaka paradigmanın dışına çıkarak… Bunun için, çerçevenin dışına çıkan beyinleri desteklemeli, çıkabileceklerin önünü açmalıyız.

İlkokuldan itibaren çocuklar, 2'nin 2'ye eşit olduğunu kabul etmemeli; ıspatlamalı.

a'nın a'ya eşit olduğunu bir önkabul olarak almayan, bunu ıspatlayan beyinlere ihtiyaç vardır. Hatta, "Niçin?" ve dahası, "Ya değilse?.." diye soran beyinlere…

Bilgi ortamında üstünlük elde etmek, bu ortamdaki varlık seviyesini yükseltmekle mümkün olabilir ancak. Bunun yolu, "ne" veya "nasıl" sorularının ötesinde "niçin" ve "ya değilse" sorularını sormaktan geçer.

Geçen yüzyılda, ülkenin ve toplumun güçlü olmasının ve bütünlüğünün bekasının yolu bu soruların sorulmamasından geçiyordu. Bu yüzyıl çok farklı olacak. Bu soruları sormayı içselleştiremeyen toplumlar, diğerlerinin dümen suyunda kalacak ve sonunda kaybedecekler. İnanın.

Bu sayfa bilhassa boş bırakılmıştır.

BİRİNCİ BÖLÜME EK

- . -

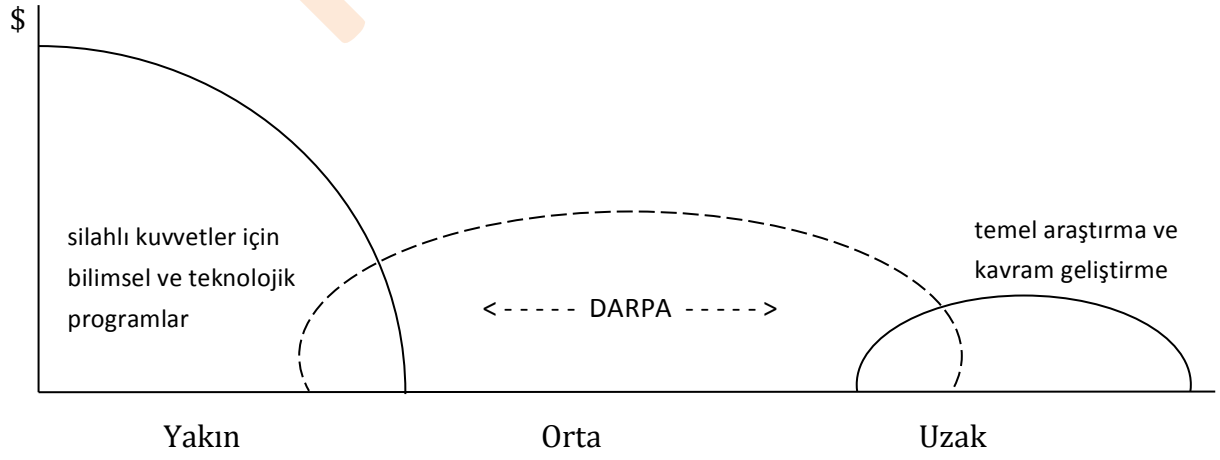
TRAVMATİK SIÇRAMA

Eisenhower'ın başkanlık döneminde yaşanan Sputnik sürprizi Amerikalıları ciddi düşünmeye ve tedbir almaya yöneltmişti. Okullardaki temel bilimler ve özellikle matematik eğitimindeki iyileştirmenin yanı sıra kurumsal yapılar oluşturdular. Sputnik sürprizi -daha doğrusu şoku- görünen o ki Amerikalılar üzerinde hayli travmatik bir etki yaratmış. Ancak, bu travma, bir çöküşe değil, aksine oldukça etkili teknolojik sıçrayışa sebep olmuş ve bu sıçrayış, Amerika'nın bugünkü teknolojik ve askeri üstünlüğünün itici gücü olmuştur.

> Amerika'nın bugünkü teknolojik üstünlüğünü sadece bu travmatik sıçrayışa bağlamak, temel ve uygulamalı bilimlerdeki altyapısını görmezden gelmek doğru olmaz. Temel bilimleri göz ardı ederek sıçramaya kalkışırsanız olduğunuz yere düşersiniz. (Her zaman söylerim; balıkların pullarını inceleyen biyologlara kıymet verilmeyen bir ülkede denizaltı yapılamaz.)

Amerika'nın teknolojik sıçrayışının öncülerinden biri olan Savunma İleri Araştırma Ajansı (Defense Advanced Research Agency - DARPA) , Başkan Eisenhower'ın talimatıyla 1958'de kurulmuştu. Stratejik plan dokümanında ve internet sitesinde ajansın misyonu ve sloganı, Amerika'yı teknolojik sürprizlerden korumak ve düşman için teknolojik sürprizler yaratmak olarak belirtilmektedir.

Güncel ve yakın geleceğin meseleleri öncelik taşımakta, dolayısıyla ulusal araştırma bütçesinin büyük kısmı silahlı kuvvetlerin güncel ve yakın gelecekteki ihtiyaçlarını karşılamaya yönelik bilimsel ve teknolojik araştırma için harcanmaktadır.



Daha ziyade temel bilimler ve kavram geliştirme ile ilgili araştırmalar öncelikli görülmediklerinden yeterli desteği bulamazlar. Genellikle olmayan meselelerle ilgili bu araştırmalar çoğunlukla radikal yöntemler ve çözümler içerirler. Kısıtlı bütçe ve imkânlara sahip olan uzak zaman araştırmalarının olası sonuçları kimi durumda yakın zaman meselelerine çözüm olabilir. İşte bu boşluğu kapamak, iki farklı amaca yönelik çalışmalar arasında ilişki kurmak, yakın zamanın meselelerine çözüm olabilecek temel bilim araştırmalarına destek sağlamak amacıyla kurulmuştur DARPA. Yarım asrı aşkın bir sürede bir dolu bilimsel ve teknolojik gelişmeye kaynak sağlayan ve öncülük yapan bu kuruluşun yönlendirdiği ve yönettiği araştırma projelerinde ABD silahlı kuvvetlerinin ihtiyaçlarına yönelik değerli çözümler ortaya çıkmıştır.

> DARPA bugün, 2013 mali yılı için birkaç milyar ABD doları bütçesiyle yüzlerce proje yönetmektedir. Projeler kamu kurumları, özel şirketler veya üniversiteler tarafından yürütülmekte; DARPA sadece program yönetimini üstlenmektedir. Burada ilginç olan: bu denli muazzam bütçe ve ileri teknoloji içeren çok sayıda projenin sadece birkaç yüz kişilik kadroyla yönetiliyor olmasıdır ki bunların yarıdan azı 4-5 yıllık sözleşmelerle görev yapan teknik proje yöneticileridir. Bu denli yalın organizasyon ile bu derece karmaşık projelerin yönetiliyor ve başarılı sonuçların elde ediliyor olması takdire değer.

DARPA tarafından yürütülen ileri teknoloji projeler içerisinde bilgi harbi ile ilgili olanlar da var, mutlaka. Diş-kuyruk oranının (Tooth-to-Tail Ratio) azaltılmasına yönelik, muhakeme yetisi olan bilişsel bilgiişlem (cognitive computing) teknolojileri ile ilgili araştırmalar bu bağlamda öne çıkmaktadır.

Günümüz askeri unsurları -birlik, uçak, tank, asker düzeyinde- oldukça yoğun bilgiişlem teknolojisi kullanmaktadır. Büyük ya da küçük, hemen her operasyon bilgi sistemleriyle ilişki içerisinde, bu teknolojiyi kullanarak yürütülmektedir. Bunun bedeli, operasyonu yürüten vurucu unsurların (diş - tooth) taşıması gereken destekleyici bilgiişlem yüküdür (kuyruk - tail). Tabii ki bu yükün (kuyruğun) iş yapan unsura (dişe) oranını en aza indirmek arzu edilmektedir. Bu amaçla, bilgi teknolojileri donanımı mümkün olduğunca ve hatta ötesinde küçültülmeli, işlem hızı artırılmalı ve yazılım geliştirilmeli.

Bilgi harbine yönelik araştırmalar, matematiğin yanı sıra bilgi teknolojileri ile ilgili şu üç konuda yoğunlaşmaktadır: yüksek verimli bilgiişlem, bilişsel bilgiişlem (cognitive computing), dil işleme.

Yüksek verimli bilgiişlem teknolojisi, çok yüksek miktarda işlemi çok yüksek hızda yapabilme imkânı sağlamaktadır. Bilişsel bilgiişlem sayesinde ne yaptığını bilen bilgi sistemleri karar verebilmekte; daha önemlisi, öğrenebilmekte ve bu sayede komutana kararlarında yardımcı olmaktalar.

> Günümüz akıllı telefonlarındaki kişisel yardımcının benzeri.

Dil işleme yetisi sayesinde gerçek zamanlı tercüme ve yabancı ortamlarda kolayca iletişim kurma imkânı sağlanmaktadır.

ENİGMA

Milattan önce beşinci yüzyılda askeri amaçla kriptografiden yararlanan Ispartalıların icadı olan Scytale belki de şifreleme cihazlarının ilk örneklerinden biriydi. Sonraki yüzyıllar içerisinde -çoğu dönen diskler şeklinde- çeşitli aletler geliştirildi. Alberti diski, Jefferson diski, Wheatstone diski bunlara örnektir.

On dokuzuncu yüzyılın sonları, yirminci yüzyılın başlarında ve özellikle Birinci Dünya Harbi'nde şifreli mesaj kullanılması çok yaygınlaşmıştı. Bu denli çok şifreli mesaj gönderiliyor olması ister istemez tekrarlara, özensizliklere yol açıyordu. O dönemlerde yaygın kullanılan şifreleme yöntemleri böylesi tekrarlara, özensizliklere karşı hassastı. Hem bu yoğun trafikle baş edebilmek, hem de insan hatasını en aza indirmek amacıyla mekanik aletlerden medet umuldu ama bunlar da yeterli olmadı. Devir elektrik devriydi; hemen her yerde elektrik kullanılması modadan öte bir mecburiyet gibiydi. Tabii ki kriptografi de bundan nasibini alacaktı; aldı da. 1900'lerin başında şifre disklerini kullanan elektromekanik cihazlar yapılmaya başladı. Bunların arasında, gerçekten -adı gibi- muamma olan Enigma en kullanışlı olanıydı; defalarca şifresi kırılmış olmasına rağmen, uzun zaman boyunca, İkinci Dünya Harbinin sonuna, hatta çok daha sonralara dek kullanıldı.

19ncu yüzyılda Rusya ve Almanya arasında bölüşülmüş olan Polonya, Birinci Dünya Harbi'nin sonunda cumhuriyet olarak tekrar bağımsızlığına kavuşmuştu. Dönemin Avrupa'sında süregiden istikrarsızlığın farkında olan -Almanya ile Rusya arasına sıkışmış- Polonya, yakında tekrar Almanların veya Rusların saldırısına uğrayacağı endişesini taşıyor ve bu yüzden onların telsiz haberleşmelerini izliyor, kaydediyor ve şifrelerini çözmeye çalışıyordu. Devir, telsiz haberleşmesi devriydi. Özellikle askeri amaçlı olmak üzere, çoğu haberleşme telsiz vasıtasıyla yapılıyordu. Bu yüzden, askeri mesajlar nispeten kolay takip edilebiliyor, ele geçirilebiliyordu.

> Polonya-Sovyet Harbi'nde Polonya'nın başarısının bir sebebi belki de telsizden ziyade telli haberleşiyor olmalarıydı.

1919 yılında kurulan, Polonya genelkurmayına bağlı Şifre Bölümü (*Sekcja Szyfrów*), Sovyetlerle harpte Polonya'nın galibiyetine önemli katkı sağlamıştı. Bu katkıda ünlü matematikçilerin payı büyüktü. 1931 yılında ise çalışma alanı daha da genişletilen Şifre Bürosu (*Biuro Szyfrów*) kuruldu. Büro, askeri haberleşmeyi ele geçirmenin ve şifreli mesajları çözmenin ötesinde kriptoloji alanında da çalışmalar yapıyordu.

Polonya genelkurmayı 1929 yılında önemli bir adım atmış, önceleri Prusya idaresinde olan ve çokça Almanca konuşulan bir bölgedeki Poznań Üniversitesi'nden (Universytet Poznański) seçilmiş yirmi iki matematik öğrencisini kriptoloji kursundan geçirmişti. Bu kursu başarıyla tamamlayan sekiz öğrenci Almanların şifrelerinin kırılmasında Polonya genelkurmayının Poznań bürosuna yardımcı oldular. İşte kriptolojiye -ve tabii ki matematiğe- vermiş olduğu bu önem sayesinde Polonya genelkurmayı ve Biuro Szyfrów, bilahare Enigma kriptanalizinde önemli başarıların beşiği oldu. Kriptoloji kursunu tamamlayan matematikçiler arasından Varşova'daki merkeze alınan, Marian Rejewski, Jerzy Różycki ve Henryk Zygalski bu başarının öncüleri oldular.

> Polonya otoritelerinin bu yaklaşımı takdiri şayan olsa gerek. Sivil bilim adamlarının dehasını ve birikimini askeri amaçlar için çekinmeden kullanmak pek olağan bir durum değildi o zamanlar.
>
> Şifre Bürosu'nun özellikle Poznań Üniversitesi'ni tercih etmiş olması da dikkati şayandır. -- Poznań Üniversitesi, o dönemde Polonya'nın en iyi üniversitesi miydi? Hayır. -- Matematik bölümü mü çok kuvvetliydi? Hayır. -- Büro'nun şefi Poznań'lı mıydı? Hayır? -- Poznań'ın havası, suyu zihnini mi açıyordu kriptanalistlerin? Hayır. Peki neydi bu tercihin sebebi? Çünkü, Poznań bölgesindeki üniversitenin öğrencileri çok iyi Almanca konuşuyorlardı; Almancaya hakimdiler. İşte, iyi sonuç veren akıllıca bir seçim daha…

Almanların yeni ve kırılması o dönem için neredeyse imkânsız bir şifreleme sistemi kullanmaya başladıklarını fark etti Polonyalılar. Esasında çok alfabeli yerine koyma (polyalphabetic substitution) yönteminin kullanıldığı bu şifreleme sisteminin omurgasını kriptoloji tarihinde efsane sayılan Enigma şifreleme makinesi oluşturuyordu.

Elektromekanik bir şifreleme makinesi olan Enigma, 1918 yılında, Alman elektrik mühendisi Dr. Ing. Arthur Scherbius tarafından ticari mesajların şifrelenmesi amacıyla icat edilmişti. Bu icadın askeri faydası olabileceğine ihtimal vermeyen Alman askeri yetkililer pek ilgi göstermediler Enigma'ya. (Scherbius, icadının askeri amaçlarla kullanıldığını ve bu sayede elde ettiği ünü göremeden 1929 yılında öldü, maalesef.)

> Amerikan askeri otoriteleri de ilk gördüklerinde Wright kardeşlerin uçağının hiçbir askeri faydası olmayacağına hükmetmişlerdi. Gerçi, bilim tarihi böyle öngörülerle doludur. Mesela, uçağın icadından sadece birkaç sene önce, havadan ağır cisimlerin uçamayacağı, dolayısıyla uçak gibi bir hava taşıtının olamayacağını söyleyen Lord Kelvin -ki kendisi fizikte artık icat edilecek bir şey kalmadığı öngörüsünde de bulunmuştur. Mesela, atomun parçalanmasının işe yarar bir enerji kaynağı olamayacağını söyleyen Sir Rutherford -ki kendisi fizikten başka bilim olmadığını iddia ettiği halde kimya dalında Nobel ödülü almıştır. Mesela, kara deliklerin olamayacağını gösteren Albert Einstein –ki kara deliklerin varlığı onun uzay-zaman modeli ile açıklanmaktadır.

Birçok yanlış öngörü sahibinin aksine, Alman askeri otoriteleri kısa sürede hatalarını anladılar ve Enigma'ya hakkettiği değeri verdiler. 1926 yılında Enigma'nın geliştirilmiş bir modelini deniz kuvvetlerinde kullanmaya başladılar. 1928'de kara kuvvetleri ve askeri istihbarat Abwehr dahil birçok askeri ve sivil kurum kullanıyordu Enigma'yı. Enigma'nın değiştirilebilen üç adet şifre diskine (rotor, Alm. Walze, Walzen) ilaveten bir yansıtıcı disk (Alm. Umkehrwalze) bulunuyordu bu geliştirilmiş modelde. 1930'da altı çift fişli bağlantı içeren fiş paneli (Alm. Steckerbrett) ekleyerek şifrenin kırılmasını çok daha zorlaştırdılar. Sonraları, beş veya sekiz adet disk içerisinden üç veya dört tane kullanmaya başladılar ki bu daha da zorlaştırdı şifrenin kırılmasını.

Enigma'nın kullanılması Almanlara kriptolojik olarak büyük üstünlük sağlamıştı. Alman haberleşmesini izleyen Polonyalılar, Fransızlar, İngilizler bir süreliğine çaresiz kaldılar bu üstünlük karşısında.

1928 yılında Varşova'daki Alman elçiliği, Polonya gümrüğüne yanlışlıkla gelmiş olan bir telsiz cihazının hafta sonu fazla mesai yaparak derhal Almanya'ya iade edilmesini talep ettiğinde şüphelenen gümrük memurları durumu askeri yetkilere bildirdiler. O hafta sonu çok hızlı ve etkin çabayla gümrükteki cihaz ayrıntılı incelemeye alındı ve görüldü ki telsiz olduğu deklere edilen cihaz aslında bir şifreleme makinesiydi. Cihaz, tekrar kutulanarak Almanya'ya iade edildi. Bu vesileyle, Almanların yeni bir şifreleme cihazı geliştirmiş olduğunu anlamış oldu Polonyalılar. Bir süre sonra bu cihazın benzeri satın alınarak Polonya'ya getirtildi; ancak bu cihaz ticari Enigma olduğu için askeri şifrelerin çözümünde pek yararlı olmadı. Yine de Polonyalılar Enigma'nın çalışma prensibi hakkında fikir sahibi oldular, kopyalarını yaparak üzerinde çalışmaya başladılar, olası permutasyonları bulabilmek için matematik modeller geliştirdiler.

Matematik modellerin doğruluğunu anlayabilmek için bilinen bir düz metin ile aynı metnin şifrelenmiş halini ele geçirmeleri gerekiyordu ama bu imkânı bulamamışlardı bir türlü. İşte tam bu çaresizlik anında, hiç beklemedikleri bir ipucu yetişti imdada: Fransız istihbaratının elde etmiş olduğu ve üzerinde çalışmaları için Polonyalılara verdiği Enigma belgeleri (kullanma kılavuzları, kullanılmış anahtarlar, şifreli metinler, düz metinler) Polonya Şifre Bürosu'ndaki kriptanalistler için çok değerli armağandı. Ele geçirdikleri belgeleri Fransızlar nasıl kullanacaklarını bilemediklerinden önce İngilizlere teklif etmişlerdi. İngilizlerin efsanevi kriptanaliz merkezi Bletchley Park'taki uzmanlar da bu bilgiyi layıkıyla değerlendirememişlerdi. İngilizler, o zamana dek ellerindeki ticari Enigma üzerinde sadece cihazın nasıl çalıştığını anlamaya yönelik inceleme yapmışlar ve telsiz dinlemesiyle elde ettikleri -Almanlar'ın İtalyanlara vermiş olduğu modifiye edilmiş askeri Enigma ile şifrelenmiş- mesajları çözmeye uğraşmışlardı; ancak, Almanların gerçek Enigma ile şifrelenmiş askeri mesajları üzerinde yeterince çalışmamışlardı. Sonunda, Fransızlar ellerindeki Enigma belgelerini Polonyalılara aktardılar.

> 1932 aralık ayının sonunda, Polonyalılar için paha biçilmez bir Noel hediyesi oldu bu bilgi. Daha sonra, yıllar boyu bu istihbarat akışı devam etti.

Yıllardır sürdürdükleri çalışmaları, geliştirdikleri matematik modelleri ve imal ettikleri Enigma kopyalarını Fransızların verdiği belgelerle birleştiren Polonyalı kriptanalistler, Enigma'nın şifrelerinin kırılmasına yönelik çok önemli bulgulara ulaştılar. Poznań bürosundan Varşova'daki Şifre Bürosu'na transfer olan matematikçiler, Marian Rejewski liderliğinde Jerzy Różycki ve Henryk Zygalski, matematik modeller geliştirmenin yanı sıra, çözüm tabloları ve elektromekanik cihazlar tasarlıyorlardı. Bunların içerisinde Zygalski delikli kartonları yararlı oluyordu ama kullanılması güç ve oldukça zaman alan bir yöntemdi. 1938'de Rejewski tarafından tasarlanan elektromekanik cihaz *Bomba* ise muammanın çözümde çığır açacak nitelikteydi. Bomba'yı kullanarak, Enigma'nın günlük şifre anahtarları birkaç saat içerisinde elde edilebiliyordu ki bu oldukça pratik fayda sağlıyordu Polonyalılara. Artık, ele geçirdikleri şifreli mesajların neredeyse yüzde yetmiş beşini çözebiliyorlardı.

Önceleri, Enigma'nın üç diski (rotor) farklı sırada yerleştiriliyordu. Diskleri (3!) altı farklı şekilde yerleştirmek mümkündü. (I-II-III, I-III-II, II-I-III, II-III-I, III-I-II, III-II-I) Almanlar, 1938 sonunda beş diskten üç tanesini kullanmaya başladılar; artık, diskler (5!/[5-3]!) altmış farklı şekilde yerleştirilebiliyordu. Polonyalılar için uğraşmaları gereken ihtimaller on misli artmıştı. Daha çok Bomba'ya, Enigma modeline, delikli

kartona ve insan gücüne ihtiyaçları olacaktı. Öte yandan 1939'un ortalarında, Polonya'nın işgali neredeyse gün meselesi olmuştu. Bu durum karşısında Polonya genelkurmayı ellerindeki bilgiyi müttefiklerle paylaşmaya karar verdi. Polonya istihbaratının başı, Büro'nun amiri ve üç Poznań matematikçisi Varşova yakınlarında bir yerde Fransız ve İngiliz istihbaratçılarıyla buluştular; ellerindeki Enigma modellerini, Bombaları ve delikli kartonları Fransızlara ve İngilizlere verdiler; kriptanalizi nasıl yaptıklarını izah ettiler, bilgi ve tecrübelerini paylaştılar.

Kriptoloji tarihinde Enigma ne kadar önemliyse, casusluk tarihinde de Hans-Thilo Schmidt o denli önemli rol oynamış, en büyük savaşın gidişatını etkilemiş belki de değiştirmiştir. Alman aristokrat bir aileden gelen Hans-Thilo Shmidt, Birinci Harp'te Alman ordusunda görev yapmıştı; ancak, savaştan sonra Versailles anlaşması gereğince asker sayısı azaltılan orduda kalması uygun bulunmamıştı. Kurduğu sabun imalathanesi, dönemin ekonomik zorlukları karşısında ayakta duramayınca zaruret içerisine düşmüştü. Kardeşi Rudolph, yarbay rütbesiyle askeri muhabere bölümünde önemli bir görevde, Enigma'nın askeri amaçlarla kullanılmasını onaylayanlardan biriydi. Rudolph, kardeşi Thilo'nun işe alınmasına yardımcı oldu, hem de kripto kayıtlarının tutulduğu ofiste. Thilo, burada kullanılmış şifre anahtarları ve şifrelenmiş mesajların imhasından sorumluydu. Bu görevi süresince güvenlik yetkisi (kleransı) izin verdiği için Enigma ile ilgili birçok bilgi ve belgeye ulaşma imkânı buldu.

(Tam bu noktada, "need-to-know" yani, "bilmesi gereken" prensibinin ne denli önemli olduğunun altını defalarca çizmek isterim. Sadece kleransı müsaade ediyor diye Enigma ile ilgili birçok belgeye ulaşma imkânı bulmuş olmasaydı, Thilo'nun verdiği zarar bu kadar büyük olmayacaktı.)

Hans-Thilo Schmidt, ele geçirdiği belgeleri 1932 yılında Almanya'da faaliyet gösteren Fransız istihbaratına aktardı. Fransız istihbaratı bu denli değerli bilgiyi elde ettikleri kaynaklarına -muhtemelen adının baş harfi H'den mülhem- *Aschè* kod adını verdi. Aschè, yıllar boyu Enigma ile ilgili değerli istihbarat aktarmaya devam etti Fransızlara; onlar da Polonyalılara. Ta ki bir başka casusun yakalanmasıyla kimliği açığa çıkana dek. 1943 ilkbaharında tutuklandı; sonbaharda kızı cesedini teşhis etmeye çağrıldı. Ashes to ashes… Küller, küllere… Ne diyelim?..

Kaderin cilvesi: Thilo'nun ağabeyi Rudolph Schmidt, 1931'de yarbay, 1934'te albay oldu. 1937'te Generalmajor (tuğgeneral) olan Rudolph, Wimar'daki 1nci Panzer tümeninin komutanlığına atandı. 1938'de Generalleutnant (tümgeneral) olarak Polonya'nın işgalinde rol aldı. 1939'da 39ncu Panzer kolordusunun (Panzerkorps) komutasına atandı ve bu kolordunun Fransa'daki harekâtını idare etti. 1940'da Demir Haç nişanı ve -Alman ordusundaki karşılığı General olan- General der Panzertruppe (korgeneral) rütbesi ile onurlandırıldı. Moskova Muharebesinde 2nci ordunun komutan vekili olarak görev yaptı ve 1941 sonunda -Hitler'le anlaşmazlığa düştüğü için görevden alınan Heinz Guderian'dan boşalan- 2nci Panzer Ordusu üst komutanlığına atandı ve 1942 başında Generaloberst (orgeneral) rütbesini aldı. Hitler'in gözde generallerinden biri olan Rudolph Schmidt 1943 nisanında Gestapo tarafından tutuklandı. Kardeşinin ihanetinin ortaya çıkmış olması kadar Hitler'in savaşı yönlendirmesini yönelik eleştirilerinin de rolü vardı bu tutuklamada. Divanıharbe çıkarılan ve beraat eden Rudolph, savaşın sonuna kadar askeri göreve getirilmedi. Savaşın bitiminden 1955'e dek savaş esiri olarak Sovyetler tarafından

> tutuldu. Serbest bırakıldıktan iki yıl sonra öldü. Kaderin cilvesi; Almanların savaş kahramanı general ne yazık ki -bilmeden de olsa- savaşı kaybetmelerinde önemli rol oynayan ihanete yol açan kişiydi.

Enigma kriptanalizi ile ilgili bilgi, belge ve ekipmanı Polonyalıların müttefiklere aktarmasından birkaç ay sonra İkinci Dünya Harbi başladı. Poznań matematikçileri ülkeyi terk ettiler, bir süre Fransa'da kaldılar. Bu sırada en gençleri Różycki elim bir deniz kazasında hayatını kaybetti; diğer ikisi İngiltere'ye geçtiler. Ne sebeptendir bilinmez -belki İngiliz kendini beğenmişliği olsa gerek- Enigma'nın gizinin çözülmesi amacıyla İngiltere'de, Bletchley Park'ta süregiden çalışmalara dahil edilmediler. Savaştan sonra Zygalski, İngiltere'de kaldı; Rejewski, Polonya'ya döndü.

Bletchley Park, İkinci Dünya Harbi süresince ve daha sonraları İngilizlerin kriptanaliz çalışmalarını sürdürdüğü merkez olarak kriptanaliz tarihinde çok önemli yer tutar.

İngilizler, sonra Amerikalılar, Enigma şifrelerini çözmek için *Bombe* adını verdikleri elektromekanik cihazlar yaptılar. Savaş boyunca ve daha sonraları *Ultra* kod adıyla yürüttükleri istihbarat faaliyeti ile elde ettikleri şifreli mesajları savaş boyunca ve daha sonraları çözmeyi sürdürdüler. Alman deniz kuvvetlerinin 1942'den itibaren Atlantik'teki U-Boat'larla haberleşmek için kullandığı, dört adet şifre diski içeren M4 modelinin şifresini, Polonyalıların Bomba'sına nazaran daha gelişmiş olan Bombe sayesinde İngilizler yirmi dakikada çözülebiliyordu.

> Kriptoloji tarihinin önemli muamması Enigma ile ilgili bilinmeyenler açığa çıkmışken, Bomba'nın adının ardındaki muamma hâlâ çözülememiştir. Bir iddiaya göre, çalışırken saatli bomba gibi ses çıkardığı için; bir başkasına göre, çözümü bulduğunda bomba gibi ses çıkarıyormuş; bir başkası, *kriptoloji bombası* anlamında Lehçe *bomba kryptologiczna* denildiği için; bir başkası, *bomba* aynı zamanda *muhteşem* anlamına geldiği için… Benim tercihim; Poznań ekibinin en genci Jerzy Różycki'nin aklına o zamanlar çok revaçta dondurmalı bir tatlı olan *bomba* yerken geldiği hikâyesi. Bomba'nın mucidi Rejewski de akıllarına daha iyi bir şey gelmediği için bu ismi koyduklarını söylemişti. Dahası, Enigma şifrelerinin çözümünü Bletchley Park'ta sürdüren İngilizler bu amaçla yaptıkları benzeri cihaza *Bombe* adını koydular -ki bu, Polonyalıların bomba dedikleri dondurmalı tatlıya Fransızların verdiği addır. Bu yüzden, dondurmalı tatlı hikâyesi daha gerçekmiş geliyor bana.
>
> İşte Polonya askeri otoritelerinin yaptığı sıra dışı bir şey daha: önce *matematikçiler*, sonra *Poznań*, şimdi de kod adı *Bomba*. Halbuki şimdilerde bile kolay kabul görmez askeri projelerde böyle sıra dışı kod adları. Adettendir, *Atılgan*, *Kartal*, *Şafak*, *Fırtına* gibi adlar makbuldür. Winston Churchill de uyarmıştır ilgilileri, operasyonlara kod adı verme hususunda. Kimse mezar taşında *Paslı Teneke* veya *Topal Ördek* veya *Üçkâğıtçılar* operasyonunda öldüğü yazılsın istemez. Aslında çok iddialı kod adları da iyi değildir. Mesela, hezimetle sonuçlanan *Zafer* harekâtı veya kolayca çözülen *Çözülmez* kripto algoritması sonuçta utanç verici olur. Ama kod adı her ne kadar bir dondurmalı tatlı olsa da, Rejewski'nin *Bomba*'sı gerçekten bomba etkisi yaratmıştır kriptoloji tarihinde.

Çok daha gelişkin elektronik bilgisayarlara rağmen Bombe'lerin kullanılması Soğuk Savaş yıllarında da devam etti.

Almanların Enigma'ları kullanması savaşın bitmesiyle hemen sona ermedi; bir on yıl daha azalarak devam etti. Tabii ki artık Doğu Almanlar kullanıyordu Enigma'ları; ancak, muammanın çözülmüş olduğunu bildikleri için kritik askeri haberleşmede değil, polis ve itfaiye telsiz çevrimlerinde kullanıyorlardı, Telsiz haberleşmesini dinleyen Amerikalılar bu cihazları kodlamışlardı; mesela: GCPB00103. (GC, Doğu Alman demekti; P, polis; B, manuel Morse; 001 ve 03 ise çevrim numarası ve çevrim içerisindeki cihaz numarasını belirtiyordu.)

> Peki, Amerikalılar niçin polis veya itfaiye haberleşmesini izliyordu? Çok mu önemliydi Soğuk Savaşta? Bir bakıma, evet. O sıralar Amerikalılar ve İngilizler, bölünmüş Berlin'in Sovyet sektöründeki haberleşmeyi izlemek amacıyla Doğu Berlin'deki telefon kablolarının geçtiği güzergâhın hemen altına bir tünel açıyorlar ve dinleme cihazları yerleştiriyorlardı. Biliyorlardı ki Doğu Almanlar ve Ruslar bunu fark ettiklerinde, açıklamak yerine hiçbir şey olmamış gibi davranıp telefon hatlarından yalan mesajlar gönderip kendilerini aldatacaklardı; o hatlardan akan bilginin hiçbir değeri olmayacaktı. Eğer tüneli fark etmezlerse, bu sefer de o telefon hatlarından akan bilgi altın değerinde olacaktı. (Belki bu yüzden bu projenin adı Altın Operasyonuydu.) Tünelin fark edilip edilmediğini bilmek çok önemliydi. Ama bir sorun vardı: oldukça kontrollü olan askeri haberleşmeyi izleyerek bunu anlamaları mümkün olmayabilirdi. Belki, tünel kazılırken kazara meydana gelebilecek bir çöküntüye müdahale edecek itfaiye ve polisi dinlemek faydalı olabilirdi. Ama atladıkları bir şey vardı: o zamanlar İngiliz istihbaratında çokça bulunan köstebekler... MI6'dan George Blake, tünel henüz planlama aşamasındayken Rusları haberdar etmişti. Sovyetler, tam da korkulduğu gibi, birkaç yıl yalan haberlerle besledi Amerikalıları ve İngilizleri. Tabii, köstebekleri Blake açığa çıkmasın diye bir miktar da doğru haberler koydular araya. 1955'te Blake bir başka göreve transfer edildikten bir süre sonra Ruslar artık rahatça keşfedebilirlerdi tüneli. 1956 nisanında "keşfettiler" ve bunu bir skandal olarak duyurdular dünyaya.

1956'da bir gün ABD başkentinde son bir mesaj Bombe'den geçirildi ve bir devir kapandı. Enigma, Bomba, Bombe ancak 1970'lerin ortalarında açıkça telaffuz edilebilir oldu.

> Savaş 1945'de bittiği, son şifre 1956'da çözüldüğü halde Enigma ile ilgili ilginç hikâye nasıl, daha doğrusu niçin gizli kaldı yetmişlerin ortalarına kadar? Birincisi, hikâyenin kahramanları ve eşleri hayattaydı; anılar çok tazeydi. İkincisi, hayatta olan ve bilinen kriptanalistleri, istihbaratçıları tehlikeye atmak doğru olmazdı. Üçüncüsü, geçmişteki operasyonlarda kimliği gizli istihbarat elemanlarının kimliklerinin açığa çıkması ihtimali vardı. Dördüncüsü -ki yine bana göre en gerçekçi olanı- o tarihe kadar Enigma hâlâ kullanılıyordu. İngilizler savaştan sonra çok sayıda cihaz ele geçirmişlerdi ve bu cihazları savaşı takip eden on beş, yirmi sene içerisinde bağımsızlıklarını ilan eden İngiliz Milletler Topluluğu üyesi devletlere vermişlerdi. Onlar da saf değillerdi; tabii ki biliyorlardı ellerindeki şifre cihazlarını İngilizlerin kırabildiğini. Ama İngilizler değildi sorun; onlar için önemli olan, diğer rakip -düşman- devletlerdi. Nihayetinde elektromekanik cihazlar olan Enigmaların mekanik aksamı otuz sene içerisinde aşınıp sık sık arıza yapmaya başlayınca artık kullanılamaz oldular. Yerine yenileri de imal edilmiyordu. Zaten, yeni teknoloji elektronik cihazlar sürülmüştü piyasaya. 1970'lerin ortalarında kullanımı sona eren Enigma artık gün ışığına çıkabilirdi.

Enigma'nın klavyesinde bir harfe basıldığında onun şifrelenmiş karşılığı olan harfi gösteren lamba yanıyordu. Karşı tarafta aynı şifre anahtarının kullanıldığı cihazda ise klavyede şifrelenmiş harfe basıldığında düz metnin harfini gösteren lamba yanıyordu.

Üç adet, birbirinden farklı şifre diski (Walze) takılabiliyordu. (1942'de kullanıma giren M4 modelinde dört adet disk vardı.) I, II, III, IV, V diye işaretlenmiş olan beş adet diskten herhangi üç (veya dört) tanesi takılabiliyordu. Böylece, üç disk kullanıldığında, diskler 5!/(5-3)!=60 farklı sırada; dört disk kullanıldığında ise 5!=120 farklı sırada yerleştirilebiliyordu.

Şifre disklerinin her birinde A'dan Z'ye 26 harf bulunuyordu. Şifre diskinin iki tarafında her bir harf için kontaklar vardı ve bu kontaklar diskin içerisinde farklı şekilde birbirine bağlanmıştı. Bir başka deyişle, diskin bir tarafında –misal- D kontağından giren akım diğer taraftan -misal- P kontağından çıkıyordu. Klavyedeki tuşlara her basıldığında, en sağdaki disk, bir turun yirmi altıda biri kadar dönüyor, bir sonraki kontağa (bir adım) ilerliyordu. En sağdaki disk bir tur dönünce, yandaki bir çentik vasıtasıyla hareketi ikinci diske taşıyor ve ikinci disk bir adım ilerliyordu. Böylece, 26x26x26=17576 kez tuşlara basıldığında diskler tekrar aynı konuma dönmüş oluyordu. Ancak, mekanik yapısından dolayı ortadaki disk çift adım ilerlediği için gerçekte döngü 26x25x26=16900 adımda tamamlanıyordu. (Döngü 16900 adımda tamamlansa da, makineyi kurgularken, şifre anahtarını oluştururken 17576 ihtimal mümkündü.)

Diskler bir tur attığında, hangi harfin hizasına geldiğinde hareketin bir sonraki diske aktarılacağının ayarlanabildiği halkalar vardı her diskin yanında. Böylece en sağdaki ile ortadaki diskler arasında ve ortadaki ile en soldaki disk arasında bu ayarı yapmak mümkündü. Dolayısıyla, 26x26=676 ihtimal söz konusuydu.

Dönen disklerin en solunda sabit bir yansıtıcı disk (Umkehrwalze) bulunuyordu. Buradaki sabit bağlantılardan dönen elektrik akımı tekrar disklerden geçerek lambaya ulaşıyordu. Yansıtıcının bağlantı şekli sabit olduğu için ihtimali artıran bir etkisi yoktu.

Disklerin haricinde bir de fiş paneli (Steckerbrett) vardı. Harf çiftlerinden oluşan altı veya on çift bağlantı olabiliyordu üzerinde. Bu bağlantılar da olasılığı artırıyordu. Formül: $(26x25)(24x23)(22x21)(20x19)(18x17) \ldots\ldots\ldots\ldots (26-2n+2)(26-2n+1)/2^n n!$

n=6 için $(26x25)(24x23)(22x21)(20x19)(18x17)(16x15)/(64x720) = 100.391.791.500$

26 harf konu olduğunda 13 çift fişli bağlantı, yani en fazla n=13 olabilirdi.

Farklı n değerleri için bir tablo yapıldığında:

n	bağlantı sayısı		n	bağlantı sayısı
0	1		7	1.305.093.289.500
1	325		8	10.767.019.638.375
2	44.850		9	53.835.098.191.875
3	3.453.450		10	150.738.274.937.250
4	164.038.875		11	205.552.193.096.250
5	5.019.589.575		12	102.776.096.548.125
6	100.391.791.500		13	7.905.853.580.625

bağlantı olasılığı mümkün oluyor.

Enigma'larda önceleri altı çift fiş bağlantısı vardı; daha sonra on çift kullanıldı ki bu durumda 150 trilyon 738 milyar 274 milyon 937 bin iki yüz elli olası bağlantı mümkün olmaktadır.

Özet olarak;

-- şifre döngü uzunluğu: 26x25x26 = 16.900 (mesaj uzunluğuna nazaran çok uzun)

-- 3 disk kullanıldığında: 26^3 = 17.576 4 disk kullanıldığında: 26^4 = 456.976 farklı şifre anahtarı kullanılabilir.

-- harf çiftlerinin değişiminde; 6 çift fiş bağlantısı kullanıldığında, 100.391.791.500 (100 milyar); 10 çift kullanıldığında, 150.738.274.937.250 (150 trilyon) ihtimal.

Şifre disklerinin sağladığı olasılık ile altı çiftli fiş panelinin sağladığı olasılıkları birleştirdiğimizde;
60x17.576x676x100.391.791.500=71.567.557.327.506.240.000=$7,15x10^{19}$
71,5 kentilyon!..

> 2003 başında Merkez Bankası yetkilileri, katrilyondan sonra kentilyon (10^{18}), seksilyon (10^{21}), septilyon (10^{24}), oktilyon (10^{27}), nonilyon (10^{30}), desilyon (10^{33}) kullanılacağını açıklamıştı.

Fiş panelindeki fiş sayısı on çift olduğunda ise;
60x17.576x676x150.738.274.937.250=107.458.687.327.250.619.360.000=$1,07x10^{23}$
107 seksilyon ihtimal söz konusu olur ki bu, günümüzün kriptografi ölçütüyle, 77 bit'lik şifre anahtarına karşılık gelir.

> 77 bitlik anahtarlı şifre günümüz bilgisayar teknolojisiyle kolaylıkla kırılabilir ama elektronik bilgisayarların olmadığı dönem için muazzam bir muammaydı (enigma) bu.

Kriptolog ve dilbilimci Kerckhoffs prensibine göre kriptanaliz yapanın algoritmayı, yani makinenin tasarımını ve nasıl çalıştığını bildiği varsayılır; şifreleme sisteminin kuvvetli veya zayıf olması anahtarın bulunabilme ihtimaline bağlıdır, sadece. İhtimal ne kadar küçükse şifreleme yöntemi o denli kuvvetlidir.

Her ne kadar kırılması neredeyse imkânsız olsa da, cihazın tasarımından kaynaklanan zaaflar ve operatörlerin hataları, özensiz davranışları sebebiyle ciddi ölçüde zayıfladığı noktalar olmuştur Enigma'nın. Örneğin: (1) Bir harf şifrelendiğinde asla kendine dönüşmezdi. Dolayısıyla, şifreli metinde mesela BHT üçlü grubu görüldüğünde bunun düz metinde "uhr" (Almanca "saat") olma ihtimali yoktu. (2) En sağdaki disk bir tur döndüğünde ikinci disk bir adım atıyor, ikinci disk bir turunu tamamladığında üçüncü disk bir adım atıyor, dolayısıyla -mesajın uzunluğuna göre- çoğu zaman üçüncü diskin hiç dönmediği oluyordu. (3) Şifre disklerini döndüren mekanizmanın yapısından dolayı, üçüncü diskin ilk adımında ikinci disk iki adım atıyordu; bu durum, şifre döngüsünü 26x26x26=17576'dan 26x25x26=16900'e düşürüyordu. (4) Bazı modellerde, hareketi bir sonraki diske aktaran çentikler iki taneydi ama pozisyonları simetrik (karşılıklı) olduğu için aslında o diskin şifre döngüsünü yarıya düşüyordu. (5) Fiş panelindeki bağlantılar karşılıklıydı; yani A eğer K'ye dönüşüyorsa (bağlanıyorsa), K de A'ya

dönüşüyordu. (6) Mesajların en az 250 karakter uzunluğunda olması gerektiğinden, kısa mesajların arkası genellikle xxxxx ile dolduruluyordu; bu da kriptanalistlerin *bilinen metin* (*known text*) yöntemini uygulamasına imkân veriyordu; çünkü, tekrarlayan harfler çözümü kolaylaştırıyordu. (7) Çok uzun mesajlar ikiye veya üçe bölünerek gönderiliyordu; bu durumda, mesajın başında yer alan mesaj anahtarları genellikle birbirinin aynı seçiliyordu ve bu tekrarlar çözümü kolaylaştırıyordu. (8) Hatayı önlemek için mesajın başındaki mesaj anahtarı peş peşe iki kez gönderiliyordu. Bilinen bu tekrar adeti çözümü kolaylaştırıyordu. Böylesi zaaflar, istihbaratın elde ettiği belgeler ve matematikçilerin yoğun çalışması sonucunda muamma (enigma) çözülebildi.

Matematikçiler daha ziyade permutasyon hesapları ile ilgileniyorlardı; çünkü amaç tüm olası permutasyonları belirleyip bunların içerisinden çözüme en yakın olanları ve mümkünse çözümü bulmaktı. Tabii, en kısa zamanda…

> Sonrası bu derlemenin sınırlarını aştığından, ilgi duyanların araştırma ve çalışmasına bırakıyorum. Tavsiye ederim; çok keyifli…

POSTANEDE DOĞUP PARKTA BÜYÜYEN DEV

İkinci Dünya Harbi kriptografların ve kriptanalistlerin kıyasıya mücadelesinin muhteşem örnekleriyle doludur. Enigma bunların en bilinenidir; onun kadar popüler olmayan ama gerek kriptografik gerekse kriptanalitik bakımdan çok daha ileri seviyede bir başkası ise Alman Lorenz firması tarafından üretilen Lorenz SZ40 veya SZ42 Schlüsselzusatz (anahtar toplama) şifreleme cihazıydı. Almanların üst düzey komuta merkezleri arasında teati edilen mesajları şifrelemede kullanılan Lorenz şifre cihazı Enigma'ya nazaran kırılması çok daha zor bir şifreleme gerçekleştiriyordu. Enigma'nın üç (bazı modellerinde dört) şifre diskine karşın Lorenz'de on iki disk bulunuyordu. Öte yandan, Enigma ile şifrelenen mesaj bilahare Morse kodu kullanarak telsiz telgraf ile gönderilirken, Lorenz ile şifrelenen mesaj teleks vasıtasıyla gönderiliyordu. Dizi şifreleme sayesinde mesaj gönderilirken aynı zamanda şifreleniyor, zamandan kazanılıyordu. Bu yüzden, Enigma için gereken üç operatöre karşın Lorenz sadece bir operatör tarafından kullanılabiliyordu. Her bakımdan hayli üstün özellikleri olan bir cihazdı.

Lorenz şifreleme makinesinde esasında Vernam şifreleme yöntemi uygulanıyordu; dolayısıyla, Vernam şifreleme yönteminin zaafı Lorenz için de geçerliydi. Operatör hatası veya başka nedenle aynı anahtarın birden fazla kullanılması, yani "derinlik" (depth) sayesinde kriptanaliz mümkün olabilirdi.

İngilizlerin efsanevi kriptanaliz merkezi Bletchley Park'taki uzmanlar, telsiz dinlemesine takılan -teleks makinelerinden hızla akan karakterlerden ötürü dinleyenlere müzikvari gelen- sinyallere "balık" (Fish) kod adını vermişlerdi. Lorenz ile şifrelenmiş mesajların çözülmesi ve makinenin nasıl çalıştığının anlaşılması ile ilgili projenin kod adı ise Tunny (tonbalığı) idi. İstihbarat yarbayı John Tiltman, daha önceleri Vernam yöntemi ile aşina olduğundan, Tunny mesajlarının Vernam yöntemiyle, yani XOR toplamasıyla şifrelenmiş

olduğunu belirledi. (Zaten, cihazın Almanca adı da bunu ima ediyordu: anahtar toplama...) Artık beklediği tek bir şey vardı: derinlik... 30 Ağustos 1941 günü beklediğini elde etti.

Atina'daki karargâhtan Viyana'ya mesaj gönderen operatör, karşıdaki operatörün de aynı şifre anahtarını oluşturması için HQIBPEXEZMUG harf dizinini gönderdi ve Viyana'daki operatör hazır olduğunda mesajı yollamaya başladı. İşlem sona erdiğinde Viyana'daki operatörün mesajı iyi alamadığını söylemesi üzerine mesajı tekrar gönderdi; ancak ölümcül hatayı yaptı, aynı şifre anahtarını kullandı ve yine HQIBPEXEZMUG harf dizinini gönderdi karşı tarafa. Bu haberleşmeyi izleyen İngiliz telsiz operatörü tahmin etti bir "derinlik" elde etme ihtimali olduğunu. Atina'daki operatör aynı düz metni aynı şifre anahtarıyla şifrelemiş olsaydı sorun olmayacaktı; ancak -zaman kazanmak için olsa gerek- çok kullanılan bazı kelimeleri kısaltmayı tercih etti. Mesela, mesaj numarasını belirten SPRUCHNUMMER yerine SPRUCHNR yazdı. 3976 karakter uzunluğundaki ilk mesaj, ikinci gönderide 100 karakter daha kısalmıştı. Bunu fark eden İngiliz telsiz dinleme operatörü bir derinlik yakalamış olduğu umuduyla her iki mesajı derhal Bletchley Park'taki uzman kriptanalistlere gönderdi. Evet!.. İşe yarar bir derinlik elde etmişlerdi; dahası,, birbirinin nerdeyse aynı ama bazı kısaltmalardan ötürü biraz farklı iki mesaj söz konusuydu ve kısaltmaların ne olduğunu bildikleri için iki mesaj arasındaki farkı tahmin edebiliyorlardı.

İşte, kriptanalistlerin en önemli yardımcısı olan şans devreye girmiş, işini yapmıştı. Bundan sonrası matematiğin meselesiydi. Tecrübeli kriptanalist Tiltman, mesajın şifresini çözmeyi başardı.

Mesaların şifresini çözmenin ötesinde şifrelemeyi gerçekleştiren mekanizmanın da anlaşılması gerekiyordu. Engin kriptanaliz tecrübesine rağmen matematikteki sınırlarını bilen Tiltman meseleyi matematikçi William Tutte'ye devretti.

> Bletchley Park'a yeni katılmış olan Tutte, o sıra Enigma şifresini çözmeye çalışan Alan Turing tarafından Enigma ekibine kabul edilmediği için Tunny ekibine girmişti. İyi ki…

Şifrelenmiş ve şifresi kırılmış Tunny mesajlarını inceleyen Tutte, tekrarlayan karakterlerden yola çıkarak Lorenz şifreleme cihazının mekanizmasını ortaya çıkardı. Gerçeğini, modelini veya tasarım çizimlerini görmeden bu denli karmaşık bir şifreleme cihazının mekanizmasını sadece matematiksel yöntemlerle ortaya çıkarmak büyük matematik başarısıydı. Hâlâ öyledir... Saygıyla yad etmek gerekir.

> Albert Einstein, bir saatin nasıl çalıştığını anlamak için içini görmeye gerek olmadığın söyler.

Lorenz şifreleme cihazının on iki diski olduğunu, diskler arasındaki ilişkiyi ve diş sayılarını ortaya çıkaran Tutte, bu diskleri Ψ , χ ve μ diye adlandırdı.

Disk	1	2	3	4	5	6	7	8	9	10	11	12
	Ψ_1	Ψ_2	Ψ_3	Ψ_4	Ψ_5	μ_1	μ_2	χ_1	χ_2	χ_3	χ_4	χ_5
Diş sayısı	43	47	51	53	59	37	61	41	31	29	26	23

Tutte'nin tasarımını ortaya çıkardığı cihazı -olası ihtimallerin hepsini değerlendirecek şekilde- mekanik olarak modellemek mümkün değildi. Bletchley Park yönetimi bu projeyi, daha sonra değerlendirmek kaydıyla rafa kaldırdı. Ancak, Tutte ve diğerleri yılmamıştı. İyi ki de… Çünkü, "derinlik içeren mesajlar göndermiş olabileceklerinden şüphelenen Almanlar, bir süre sonra cihazların şifre anahtarlarını ayarlamaya yarayan karakter dizinini mesajın hemen öncesinde göndermekten vazgeçtiler. Bu durumda Bletchley Park'takilerin işi çok zor, hatta imkânsız hale geldi. Tutte'nin modellediği şifre disklerini oluşturmak ve her seferinde bir hane kaydırarak denemek kâğıt kalem veya mekanik yöntemlerle mümkün değildi ama belki başka yollarla mümkün olabilirdi.

Yine de Tiltman, Tutte ve arkadaşlarının başarısı Müttefiklere özellikle Normandiya çıkarmasında çok büyük avantaj sağladı. Alman genelkurmayının çıkarmayı nereden beklediğini, ne gibi tedbirler aldıklarını, çıkarma başladıktan sonra nasıl tepki verdiklerini; nereye, ne kadar kuvvet kaydırdıklarını ve benzeri çok değerli bilgi elde etti Müttefikler.

Tiltman'ın Tunny ekibindeki bir diğer matematikçi Max Newman, Bletchley Park'ta konuşlanmış devlet kodlama ve şifreleme okuluna (Government Code and Cipher School - GC&CS) katılmadan önce programlanabilir hesap makinelerinin teorik temelleri ile ilgileniyordu. Enigma ekibinde görevli Alan Turing de benzer konu ile ilgileniyordu; öyle ki günümüzde hayatımızın parçası haline gelmiş olan programlanabilir hesap makinelerinin -yani bilgisayarların- ilkesel temelini oluşturan Turing Makinesi ve Evrensel Turing Makinesi kavramlarını geliştirmişti.

Alan Turing, Enigma'nın şifresini çözmek amacıyla geliştirilmiş olan elektromekanik Bombe'nin daha etkin bir modelinin yapılabilirliğini tartışmak üzere Posta İdaresi'nde görevli elektrik mühendisi Tommy Flowers'ı davet etti bir gün Bletchley Park'a. Tommy Flowers, Bombe'nin elektromekanik yapısının geliştirilebileceğini söyledi; ancak, Bletchley Park yetkilileri bu konuda fazlasıyla şüpheci olduklarından kabul etmediler. Ne de olsa Bombe ile elde ettikleri sonuçlar -üç veya dört şifre diskine sahip-Enigma ile şifrelenmiş olan mesajların zamanında çözülmesi için yeterli oluyordu.

Tommy Flowers'ın bilgi birikimi ve teknolojiye olan hakimiyetinden etkilenen Alan Turing bir süre sonra onu Max Newman'la tanıştırdı. Bu kez mesele, Tunny şifresini oluşturan makinenin modelinin yapılması ve şifreli mesajın bu makineden geçirerek kısa sürede çözüm elde edilmesiydi. Tutte, bunun nasıl mümkün olabileceğini modellemişti ama işlem kâğıt kalemle yapılıyordu. Almanların şifre disklerini ayarlama anahtarını mesajla birlikte göndermeye son vermesiyle neredeyse imkânsız hale gelmişti. Elektromekanik modellerin yapılması hem çok zordu hem de yapılabilse bile on iki disk arasındaki ilişkiyi deneme yanılma yoluyla bulmak çok uzun zaman alacaktı. Tommy Flowers bu sorunun elektronik yöntemlerle çözülebileceğini söyledi. Bletchley Park yönetimi bu öneriyi de kabul etmedi; çünkü dönemin elektronik bileşeni olan lambaların güvenilirliği hayli düşüktü. Çok sayıda lamba kullanan bir cihaz çalışma süresince çok arıza yapacak ve pratik olarak mesajın geçerli olduğu süre içerisinde çözüm elde edilemeyecekti. Ancak, Flowers bu görüşe katılmıyordu. Ona göre, eğer cihaz bir kez açıldıktan sonra kapatılmazsa, uzun süre çalıştırılırsa lambaların arıza olasılığı gittikçe

azalacak ve cihazın güvenilirliği kabul edilebilir bir seviyede olacaktı. Yine de ikna edemedi Bletchley Park yönetimini. Refüze edilmesine rağmen düşündüğünü hayata geçirmeye kararlı Tommy Flowers, çalışmakta olduğu Posta İdaresi'ne dönünce oradaki direktörünün desteği ve kısıtlı sayıda yardımcı ile ve kendi cebinden ciddi miktarda para harcayarak 1500 lambadan meydana gelen ilk programlanabilir elektronik hesap makinasını (bilgisayar) sadece on bir ay içerisinde tasarladı ve inşa etti. Görünce ikna olan Bletchley Park derhal ikincisini ısmarladı. Flowers, 2400 lambalı ikinci modeli çok daha kısa sürede yaptı. Harp süresince on tane yapıldı bu bilgisayarlardan. Programlanabilir elektronik bilgisayarın dünyada ilk örneği olan bu devasa makinenin adı, dev anlamında, Colossus idi.

İlk elektronik bilgisayar olarak Amerikan imalatı ENIAC bilinir, genellikle. Halbuki ondan yıllar önce, İngiltere'de ve tek bir dahi mühendis tarafından tasarlanarak inşa edilen dev Colossus esasında bilgisayar çağının ilk temsilcisidir. Savaş boyunca toplam on tane imal edilen Colossus'ların hepsi savaşın bitiminde Churchill'in, "en büyük parçası yumruk büyüklüğünü geçmeyecek" talimatıyla parçalandı; tüm tasarım ve imalat dokümanları imha edildi. Üzerindeki gizlilik perdesinin uzun yıllar kalkmaması sebebiyle Colossus projesi karanlıkta kaldı.

> Birinci Dünya Harbi'nde Vernam şifreleme yöntemini bulan Gilbert Vernam, savaştan önce Amerikan Bell telefon şirketinde çalışıyordu; savaştan sonra Posta ve Telgraf şirketinde çalışmaya döndü. İkinci Dünya Harbi'nde -Vernam şifresiyle şifrelenen- Tunny mesajlarını çözen muazzam Colossus'un tasarımcısı ve yapımcısı Tommy Flowers da posta ve telgraf idaresinin mühendisiydi.
>
> Bizim PTT ARLA'mız da bu konuda öncülük yapabilirdi, belki. Ne var ki hemen her konuda olduğu gibi, bu bir irade ve idare meselesidir. Yüzyıllar boyu kütüphanemizde bulunan kriptanaliz risalesinin gün ışığına kavuşmak için 1987'de gelecek yabancıları beklediğini göz önüne alırsak…

ZEKÂ YEŞEREN PARK

Enigma'nın, Lorenz'in şifrelerini çözen, aralarında John Tiltman gibi kriptanalistlerin; Alan Turing, William Tutte, Max Newman gibi matematikçilerin, Tommy Flowers gibi mühendislerin ve adlarını sayamadığımız, hatta bilmediğimiz daha nicelerinin gece, gündüz, canla, başla çalıştıkları Bletchley Park kriptanaliz tarihinde yerini altın harflerle almayı hak eder. İkinci Dünya Harbi sürerken derme çatma barakalarda sessizce ama büyük özveriyle çalışan insanların kendi ülkeleri ve müttefiklerinin zaferine yapmış oldukları katkı en az cephede savaşanlarınki kadar önemliydi.

> Winston Churchill savaştan sonra Bletchley Park'ı ziyaretinde çok şaşırmıştı gördükleri karşısında. Hatta, "Çok saf görünüyorsunuz; gizli bir şey bildiğinize kimse ihtimal vermez," gibi talihsiz bir ifade kaçmıştı ağzından Daha sonra, çalışanların gönlünü alacak şeyler söylemişti ama yine de bu başıbozuk, dağınık görünüşlü topluluğu pek sindirememişti içine. Ayrılırken, arabanın camını indirip Bletchley Park'ın müdürüne, "İşe alırken her taşın altına bakmanı söylemiştim ama beni bu

kadar ciddiye alacağın aklıma gelmemişti." Yine de, bu müthiş ekibin hakkını teslim etmiş, takdirlerini esirgememişti. "Altın yumurtlayan kazlar, hem de gık çıkarmadan" diye anardı onları.

Halen müze olan Bletchley Park malikânesi Londra'nın kuzey-batısında, 80 km mesafededir. Birinci Dünya Harbi sonrası kurulmuş olan devlet kodlama ve şifreleme okulunun (Government Code and Cipher School - GC&CS) İkinci Dünya Harbi öncesi buraya yerleşmesi ve savaşın kazanılmasındaki olağanüstü katkısı ile ünlenmiştir.

Bletchley Park'taki kriptanaliz merkezi GC&CS, savaştan sonra devlet haberleşme merkezi (Government Communications Headquarters) adıyla sürdürdü faaliyetini.

Askeri entelejans, tecrübeli şifre çözücülerin yanı sıra matematikçiler, fizikçiler, matematikçiler, mühendisler, dilbilimciler, bulmaca çözenler, satranç ustaları, çeşitli meslek ve bilim dallarından insanlar toplanmıştı Blethley Park'ta. Onca farklı insanın birlikte çalışmasını sağlayan vatanseverlik, kararlılık, çalışkanlık, fedakârlık, inançlılık gibi özelliklerine ilaveten ortak bir özelliği daha vardı: yüksek zekâ katsayısı.

Böyle nitelikli insanlar, çok tabiidir ki alışılmışın dışında kişilik özellikleri göstermekteydiler; dolayısıyla, bir arada çalışma ortamının sağlanması ve idaresi hayli zordu. Öyle bir ekip ki kimi bütün gün pencereden dışarıyı seyreder, kimileri kriket oynardı.

Daha sonra tuğgeneral olacak, o dönemde yarbay olan John Tiltman, üniformasındaki işaretleri umursamaz, yanlış takardı; özel yapım masası vardı, çünkü ayakta çalışırdı.

Düşman Almanların en zor şifresinin çözümünde önemli rol alan Max Newman, Alman asıllıydı. Babası Herman Alexander Neumann, on beş yaşında Almanya'dan İngiltere'ye göçmüş, orada evlenmiş, çoluğa çocuğa karışmış, 1897'de oğlu Maxwell doğmuştu. Ama Birinci Harp'te enterne edilmesi hayli gurur kırıcı oldu baba Neumann için ve Almanya'ya döndü. Gençliğinde bu ailevi travmayı yaşamış olan, Alman asıllı Max Newman'ın Almanlarla süregiden İkinci Harp'te bu denli kritik bir göreve getirilmesi pragmatik, akılcı yönetimin örneği olsa gerek.

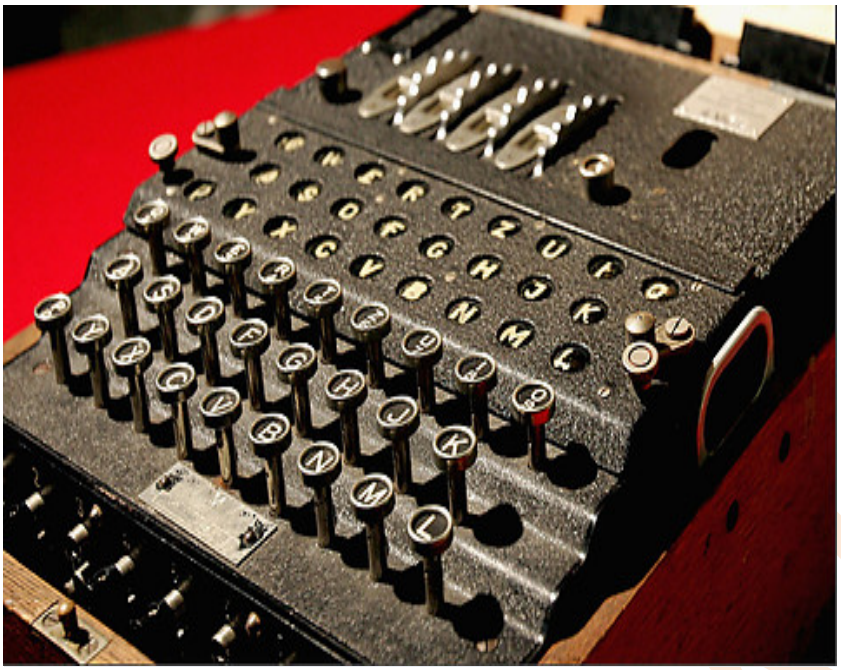
Tommy Flowers savaştan sonra Posta İdaresi'ndeki görevine döndü. Ödül olarak aldığı bir miktar para, Colossus için yapmış olduğu şahsi harcamaları zor karşıladı. Savaştan sonra, sivil amaçlı bir programlanabilir elektronik hesap makinesi (bilgisayar) imal etmek için yapmış olduğu kredi başvurusu reddedildi, çünkü bankalar böyle bir şeyin yapılabileceğine ihtimal vermiyorlardı. Flowers, ne yazık ki gizlilik yemini etmiş olduğu için daha önce on tane yaptığını ve çalıştırdığını söyleyemiyordu.

Alan Turing, savaş bittikten sonra eşcisel tercihinden ötürü ahlaksızlıkla suçlandı, yargılandı, gizlilik kleransı iptal edildi, GCHQ girişi engellendi, Amerika'ya girişine izin verilmedi. Mahkeme, libidosunu azaltan hormon tedavisine hükmetti. Büyük kriptanalist, programlanabilir bilgisayar kavramının öncüsü, matematik dehası artık herkesin kaçındığı biri olmuş, bilimsel çalışmalarını sürdüremez hale gelmişti. Bir sabah yatağında ölü bulundu, yanı başında ısırılmış bir elmayla. Ölüm nedeni siyanür zehirlenmesiydi. Polis, siyanür zerk edilmiş elma ile intihar ettiği sonucuna vardı. (Gerçi, elmayı hiç incelememişlerdi.) Ölümünden yıllar sonra itibarı iade edildi, devlet

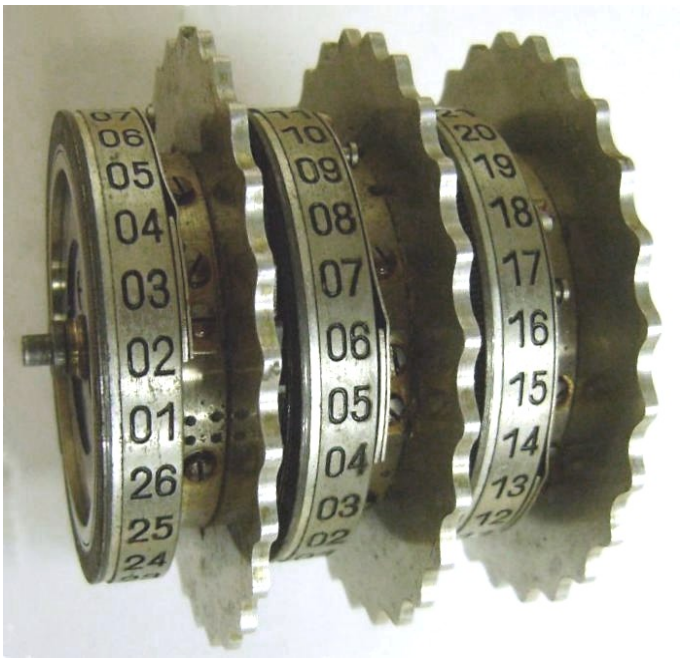
özür diledi, ülkesinde ve başka ülkelerdeki birçok üniversitede adına bölümler açıldı, hatta Bletchey Park'a heykeli dikildi.

> Apple logosu ısırılmış elmanın Turing'e bir gönderme mi olduğu sorulduğunda şirket yetkilileri bunun doğru olmadığını belirtmişlerdir, ısrarla. Ama bir mülakatta Steve Jobs, "Keşke olsaydı," demiştir, saygıyla.

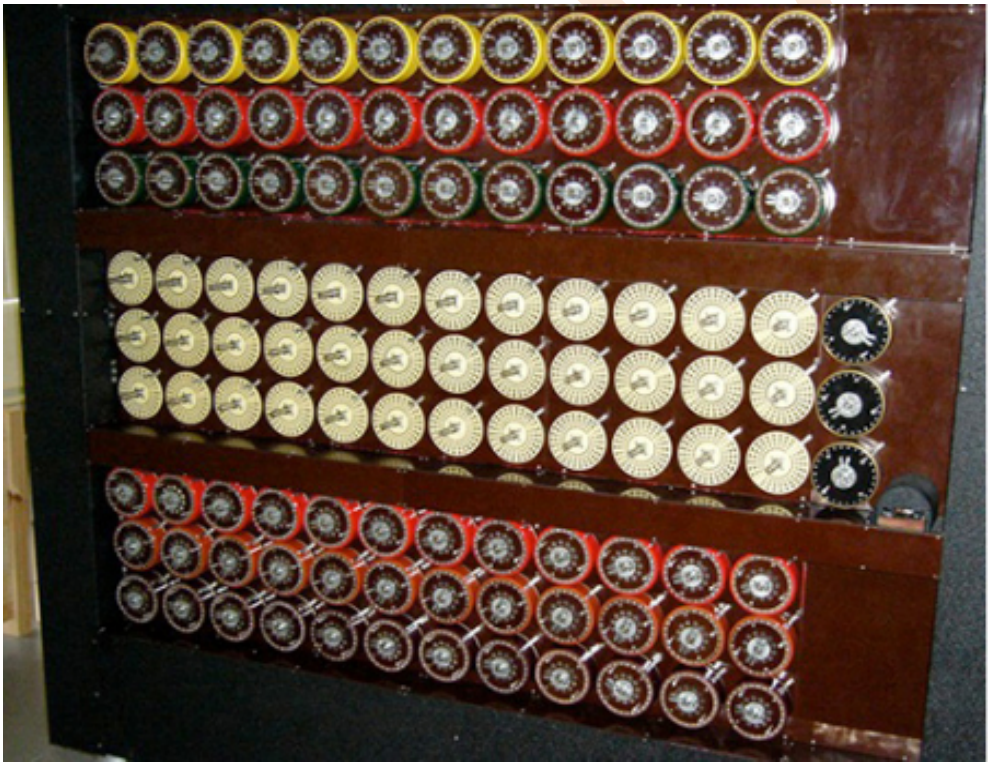
Zeka yeşeren Bletchley Park'ın devamı GCHQ da nevi şahsını münhasır kişilikleri barındırıyordu. (Muhtemelen hala öyledir.) Mesela, fizikçi James Henry Ellis. Takım çalışmalarına katılmayan, kimsenin de kendisiyle çalışmaktan pek haz etmediği bu adamın ne zaman ne yaptığını, ne ile uğraştığını kimse bilmezdi. Eline geçirdiği her konuda, her türlü bilimsel makaleyi okur; gizli veya değil, her şeyi masasının üzerinde bırakırdı. Darmadağınık masası her akşam güvenlik görevlileri tarafından temizlenirdi. Yetenekli biri olduğu bilinmesine rağmen, düzenli çalışmadığı için önemli projelerde yer verilmezdi Ellis'e. Asimetrik kriptografinin çözümünü bulanların ve bilgi iletişiminde çığır açanların önde gelenlerinden biri işte bu James Ellis'dir.



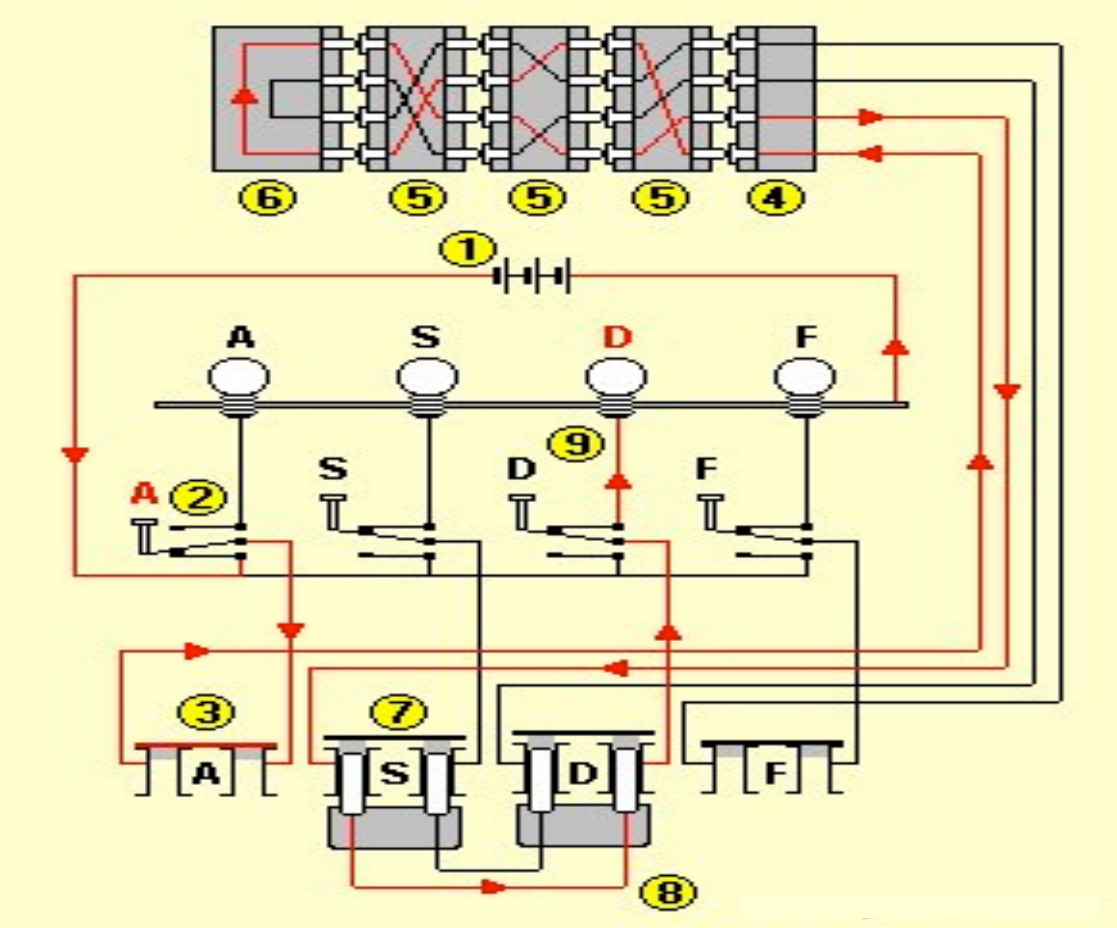
Enigma şifreleme cihazı



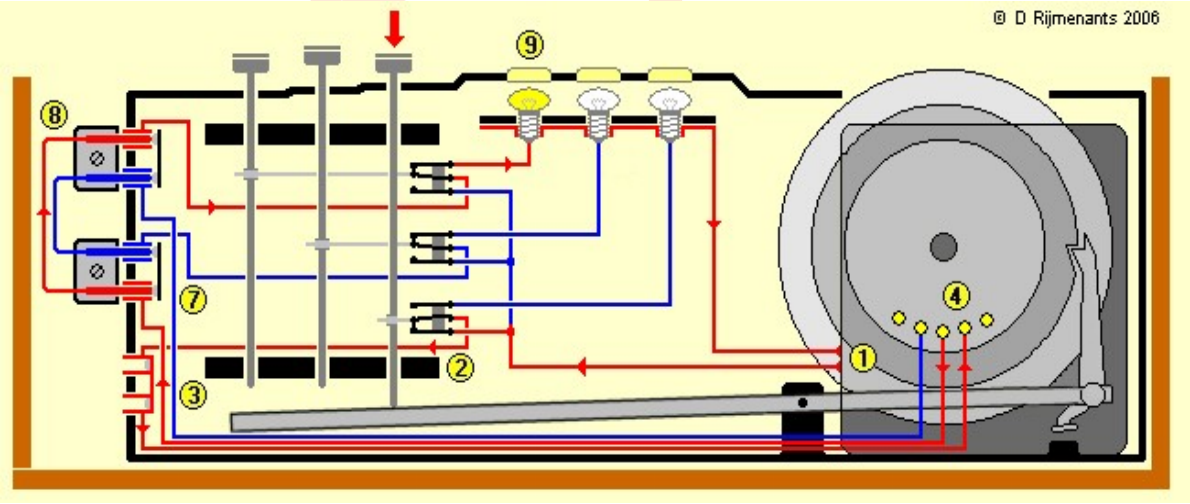
Enigma şifre diskleri (Rotor)



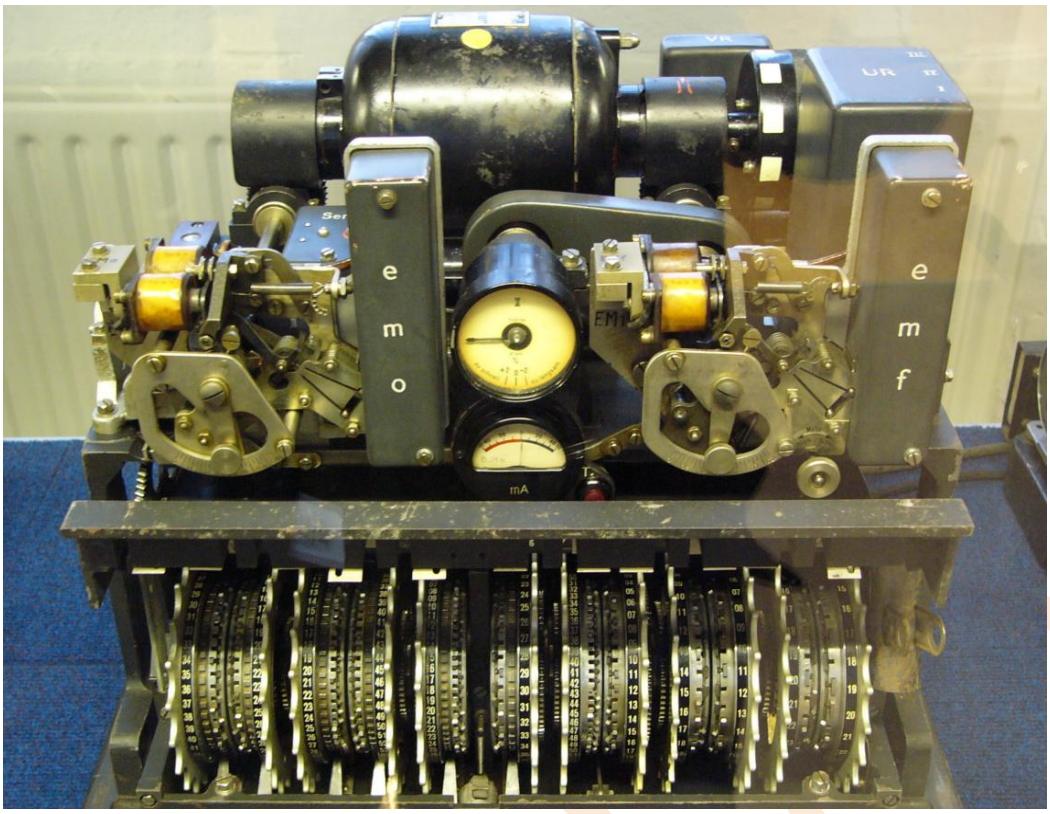
Bombe



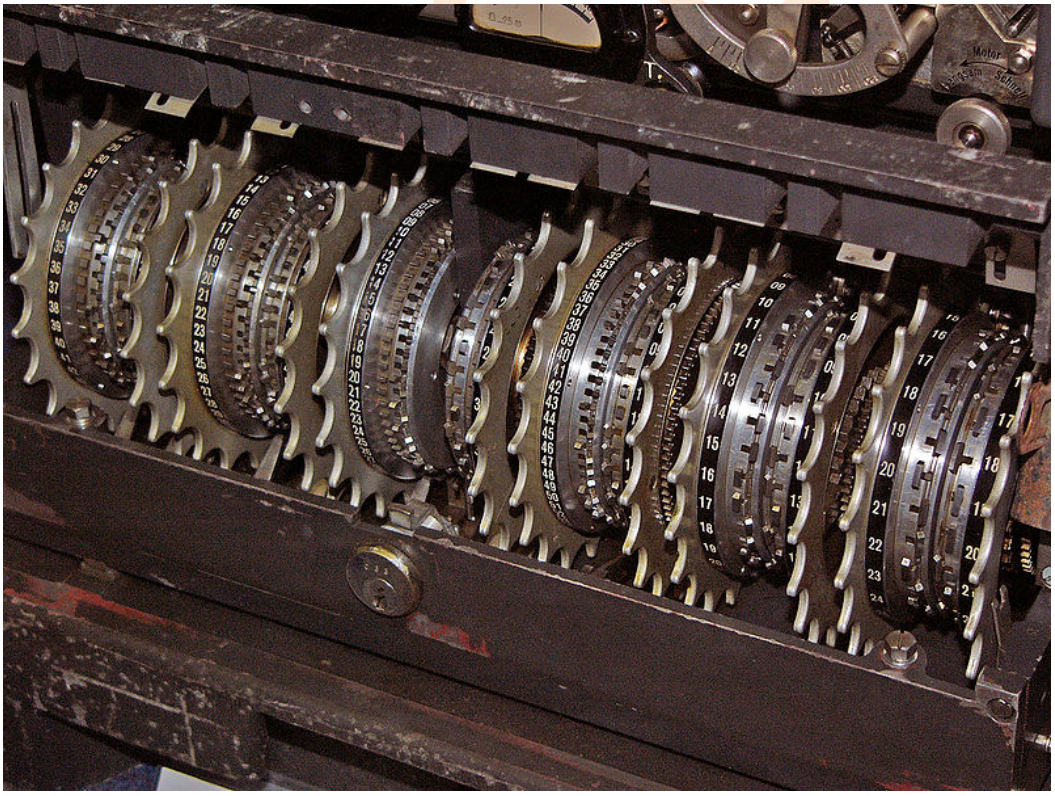
Enigma



Bataryadan (1) gelen akım, klavyenin tuşundan (2) ve fiş panelinden (3) geçtikten sonra en sağdaki giriş diski (4) vasıtasıyla dönen şifre disklerine (5) geçer ve yansıtıcıdan (6) dönüp tekrar disklerden ve fiş panelinden (7) ve fişli bağlantılardan (8) geçerek şifrelenmiş harfin lambasını (9) yakar.



Lorenz şifreleme cihazı

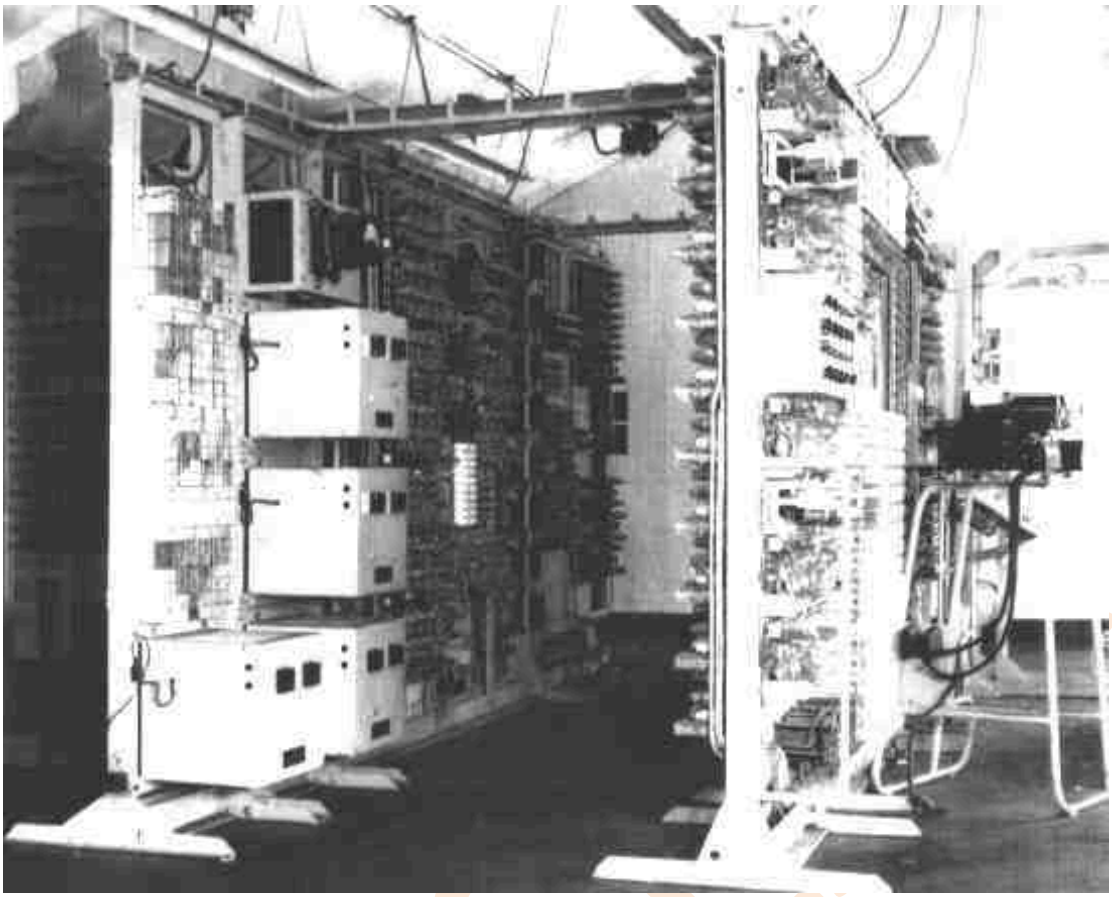


Şifre diskleri (Rotor)

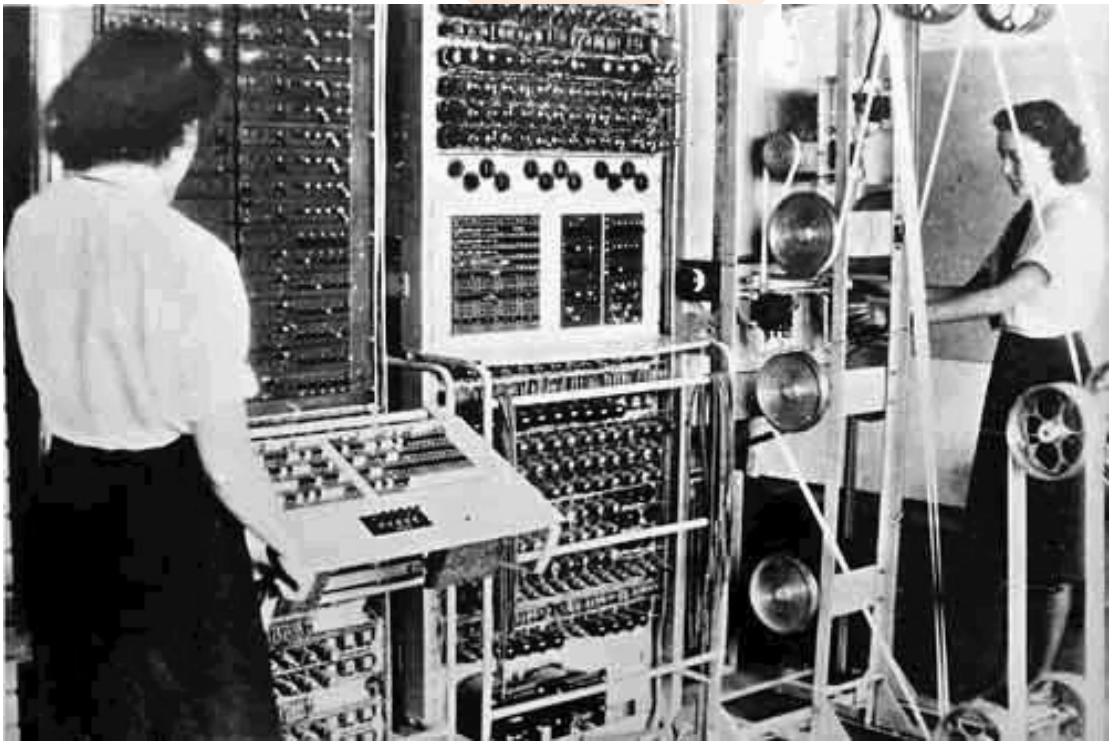
Bletchley Park Ana Bina

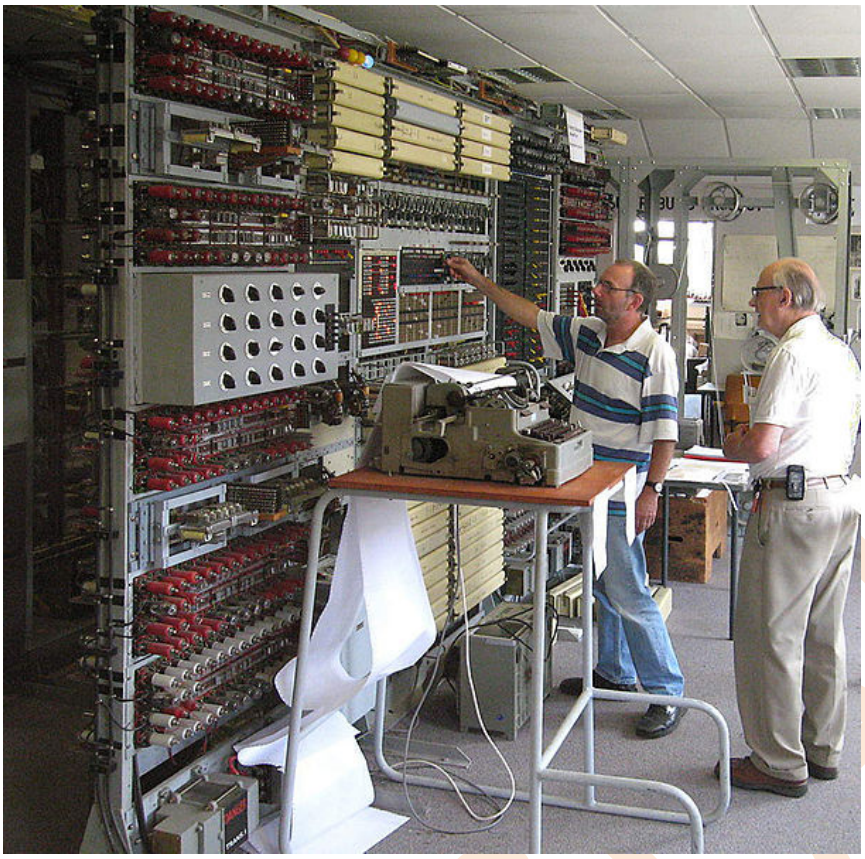
Bletchley Park Baraka 6 ve Baraka 8

Şifre çözücüler

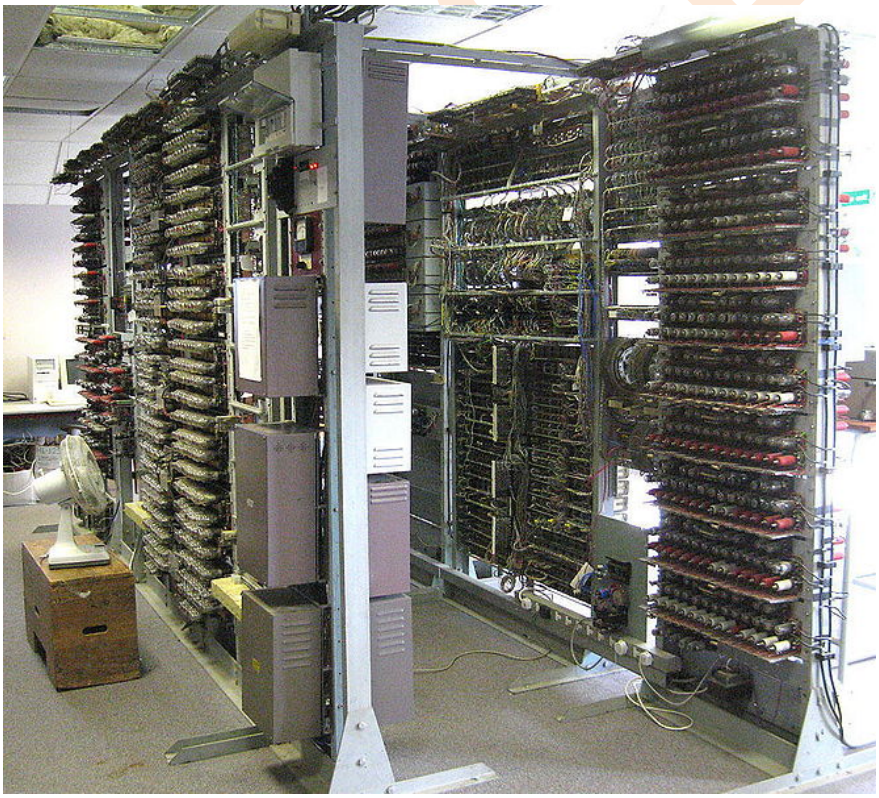


Colossus (1943 - 1944)





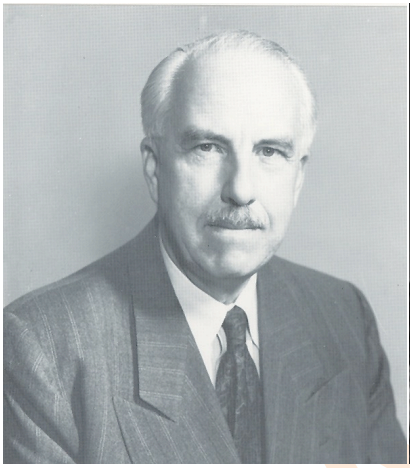
Colossus yeniden (1994 - 2007)



Marian Rejewski

Jerzy Różycki

Henryk Zygalski



John Tiltman

William Tutte

Max Newman

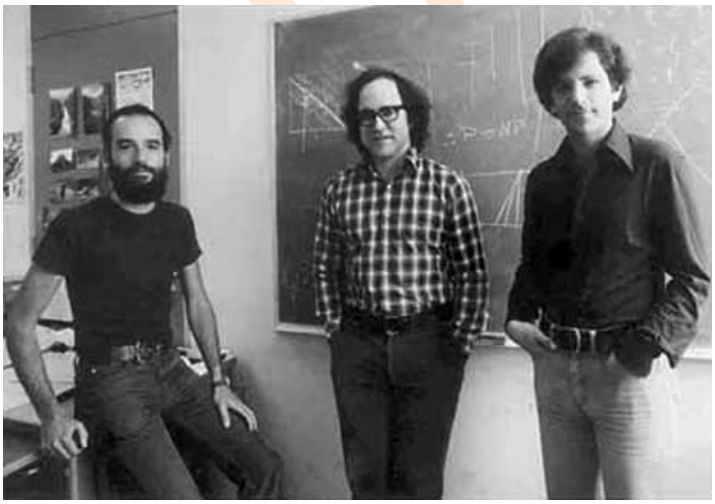
Alan Turing

Tomy Flowers



James Ellis Clifford Cocks Malcolm Williamson

Whitfield Diffie Martin Hellman RalphMerkle



Ronald Rivest Adi Shamir Leonard Adleman

MATEMATİKÇİNİN ÖZRÜ

Kriptoloji ile ilgili bir derlemede İngiliz matematikçi Godfrey Harold Hardy tarafından kaleme alınmış olan *Matematikçinin Özrü* (*A Mathematician's Apology*) adlı denemeden söz etmek gerekir. Niçin?.. Çünkü, asimetrik kriptografinin öncülerinden İngiliz matematikçi Clifford Cocks anahtar aktarımı meselesinin pratik çözümünü bulduğunda G.H. Hardy'ni yanılmış olduğu söylenir. Peki ne demişti Hardy?..

Söz konusu olan, affedilmeyi bekleme anlamında bir özür değil, daha ziyade savunma amaçlı gerekçe bulmadır -ve hatta bu vesileyle bir övgüdür matematiğe.

> Türkçemize "Bir Matematikçinin Savunması" diye çevrilmiş olan bu eser için ben, "Matematikçinin Özrü" başlığını tercih edeceğim. Af dileme değil, savunma anlamında bir özür beyanı olsa da, yazar alçakgönüllü bir ifade tercih etmiştir; saygı göstermek gerekir. (Hiç de alçak gönüllü olmayan metni dengelemek için başlıkta böyle bir ifadeyi tercih etmiş olabilir, ya da bir istihzadır belki.)

Bu denemede Hardy, altmış, hatta elli yaşını geçkin birinin -özellikle matematik söz konusu olduğunda- artık yaratıcı olamayacağı, değer içeren bir üretimde bulunamayacağı gibi oldukça keskin ve tartışmaya hayli açık bir iddiada bulunmaktadır.

"Matematikçi unutmamalıdır ki matematik, hiçbir bilimin olmadığı kadar, gençlerin işidir," diyecek kadar ileri gider.

> Tartışılır…

Gerçek bir matematikçinin başka hiçbir şey yapmaması gerektiğini söyler. Öte yandan, bir meslek erbabının yaşlandığında mesleği ile alakalı yazılar yazmasını dahi -acıklı demese de- melankolik bulur. Matematikçinin işlevinin yeni teoremler ıspatlamak, matematiğe katkıda bulunmak olduğunu, kendisi veya başka matematikçilerin neler yaptığını anlatmak olmadığını söyler, Açıklama, beğeni, eleştiri çalışmalarının "ikinci sınıf" beyinlerin işi olduğunu iddia eder.

> Kendisinin matematik hakkında yazıyor olmasını da yaşının altmışı geçmiş olmasına, mesleğini gerektiği şekilde yapabilecek zihin tazeliğine, sabır ve enerjiye sahip olmadığını söyler.

Hardy'nin bu iddiaları bu derlemenin konusu ile pek alakalı değildir; ancak bir başka iddiası daha vardır ki kriptoloji camiasını yıllar boyu ilgilendirmiştir. Şunu iddia eder G.H. Hardy: "Gerçek matematik asla savaş ile alakalı olamaz. Kimse henüz sayılar kuramının savaş ile alakalı bir amaca hizmet ettiğini gösterememiştir."

> Hardy, matematiğin çeşitli dalları içerisinde sayılar kuramını öne çıkarır.

Hardy, "gerçek" ve "saf" dediği temel matematik ile uygulamalı matematik arasında ayırım yapmakta ve uygulamalı matematiğin değerini azaltan ifadeler kullanmaktadır.

(Çirkin, cansız, önemsiz, hatta benim tırı vırı diye çevirdiğim trivial gibi sıfatlar kullanır.) "Yaptığım işin hiçbir faydası yok" diyerek kendi temel matematik çalışmalarını önemsizleştiriyormuş gibi görünse de aslında temel matematiğin güzelliğine vurgundur.

> Bir seferinde Bertrand Russel'a şöyle demiştir: "Beş dakika içerisinde öleceğini ıspatlayabilirsem öleceğin için üzülürüm ama yaptığım ıspatın vereceği zevk bu üzüntümü azaltacaktır." (Bertrand Russel, Hardy'e hak vermiştir.)

Matematikçinin, yaptığı işin yararı ile övünmemesini söyler; çünkü matematiğin yararı diğer bilim dallarında sonuç gösterir ki diğer bilimler "iyi" amaçlar için olabileceği gibi "kötü" amaçlar için de kullanılabilirler. Bu da ister istemez matematiğin kötü amaçlar için kullanılıyor olması sonucunu doğurur.

> Birinci Dünya Harbi'nde patlayıcıların ve kimyasal silahların sebep olduğu vahşeti gören ve kendisi savaş karşıtı bir pasifist olan Hardy için bu denli övündüğü, vurgunu olduğu temel matematiğin suçsuz hatta sorumsuz olması gerekiyordu. Bu yüzden, temel matematik ile uygulamalı matematik arasında böylesi bir ayrım tezi ortaya atarak bir bakıma kendi düşünsel bütünlüğünü korumak istemiş olsa gerek. Ancak, Maxwell ve Einstein söz konusu olduğunda ne yapacağını bilememiş, onları da Fermat gibi "gerçek" matematikçiler olarak niteleyerek kendini ikna etme yoluna gitmiştir.
>
> Tezinin pek geçerli ve anlamlı olmadığını kendisi de fark etmiş olmalı ki kaleme aldığı bu denemesine "An Apology - Özür" başlığını uygun görmüştür. Denemenin altıncı bölümünde bu konudaki düşünsel çelişkisi açığa çıkar. "Matematik 'zararsız' mıdır?" sorusunu sorar, ancak cevabın kolay olmadığını söyleyerek geçiştirir. Tabii ki bilimin savaş üzerindeki etkisinden bahisle kimyanın pek de zararsız olmadığını belirtmeden geçmez.

G.H. Hardy tarafından öne sürülen matematiğin, özellikle sayılar kuramının savaş üzerinde etkisi olamayacağı tezi, asimetrik kriptografinin öncüsü matematikçiler tarafından çürütülmüştür.

> Kriptografik ürünler "silah" olarak sayılsa, kriptografik ve kriptanalitik çalışmalar askeri boyutta değerlendirilse de insana doğrudan zarar vermeleri söz konusu değildir. Sayılar insana çarptığında yaralamaz, solunduğunda zehirlemez. Ben derim ki çarpım tablosu ne kadar zararlıysa kriptografik bir algoritma veya bir kriptanaliz yöntemi de o kadar zararlıdır -veya masumdur. Bu bakımdan G.H. Hardy haklı olabilir. Ama şunu da kabul ederim ki Üçüncü Dünya Savaşı muhakkak matematikçilerin arenası olacak.

KRİPTOLOGLAR YEMEKTE

Ülkenin önde gelen birkaç kriptoloğu âdet edinmişler; her ay toplanıp lüks bir lokantada yemek yerlermiş. Yine adet gereği, her seferinde hesabı içlerinden biri ödermiş ama diğerlerine belli etmeden. Yemeğin sonunda garson masaya gelir, "Hesap ödendi," dermiş. O gün artık hangisi ödediyse, ne o söylermiş ne de diğerleri sorarmış.

Bir gün bakmışlar ki terör örgütünün finans kaynağı olduğunu bildikleri birileri de aynı lokantada oturmuş, yemek yiyorlar. Hatta o gruptan biri, uzaktan hafifçe selamlamış bizim kriptologların masasını. Gerçi hiçbiri almamış bu selamı ama kurt düşmüş içlerine ya hesabı bu terör finansörleri öderse diye. Hiç hoş olmaz, tabii ki.

Yemeğin sonunda garson gelip, "Hesap ödendi," deyince düşünmüşler; öyle bir algoritma bulmalılar ki hem hesabın terör finansörleri tarafından mı yoksa kendilerinden biri tarafından mı ödenmiş olduğunu bilsinler, hem de âdet olduğu üzere içlerinden hangisinin ödemiş olduğunu anlamasınlar.

Matematik koşmuş hemen yardımlarına. Her bir kriptolog sağındaki (veya solundaki) arkadaşı ile yazı-tura atar. Sonra söyler: eğer iki tarafında da aynını gördüyse, "Aynı"; farklı gördüyse, "Farklı" diye; ancak, hesabı ödemiş olan bunun tersini söyler. Sonuçta, "Farklı" diyenlerin sayısı tekse hesap içlerinden biri tarafından ödenmiştir (mesele yok); çiftse başkası ödemiştir.

> 1988'de David Chaum tarafından gündeme getirilen bu protokolün bilgi güvenliği ile olan alakasını ve matematiksel çözüm yöntemini bulmayı okurlara bırakıyorum. Bilgi güvenliği ile olan alakası uzmanlık gerektirse de matematik çözümü için lise matematik bilgisi yeterli sanırım.

AKTRİS VE MUCİT

> * Hedy Lamarr için Wikipedia'daki meslek tanımı: aktris, mucit.
>
> Bir dönemin güzeller güzeli sinema yıldızı mıydı günümüzün en yaygın haberleşme tekniklerinden birinin mucidi; yoksa kendini gizleyen bir bilim kadını mıydı Hollywood'un tahtına yerleşen?

1913 Avusturya doğumlu Hedwig Eva Maria Kiesler ülkesinde tanınmış bir aktris ve önde gelen bir silah sanayicisinin eşiydi. Siyasi liderler ve askeri teknoloji uzmanları ile yapılan toplantılara eşiyle birlikte katılır ve o kişilerle bire bir konuşma fırsatı bulurdu. 1937'de eşini ve ülkesini terk etti ve ismini Hedy Lamarr olarak değiştirip Amerika'ya yerleşti. Kendinden önce Hollywood'a ulaşmış olan ünü onu hemen zirveye taşıdı ve uzun süre orada kaldı.

İkinci Dünya Harbi'nin Atlantik'te kızıştığı dönemde Alman denizaltılarına karşı geliştirilen radyo kumandalı torpidolar pek etkin olamıyorlardı; çünkü radyo kumanda sinyali Almanlar tarafından karıştırılıyor ve torpidonun hedefi vurması engelleniyordu. 1941 yılında Hedy Lamarr ve komşusu, besteci George Antheil tarafından birlikte yapılan "Gizli Haberleşme Sistemi" başlıklı patent başvurusu ile bu soruna bir çözüm öneriliyordu. 1942 yılında tescil edilen patentlerinin tüm haklarını ABD silahlı kuvvetlerine terk etmelerine rağmen bu buluş uzun zaman uygulamaya konulmadı.

Buluş, o zamanlar frekans atlamalı (frequency hopping) denilen tekniğin esasını oluşturuyordu. Buluşun esası, torpidoya kumanda eden radyo sinyalinin

karıştırılmasına karşı koymak amacıyla frekansın belirli zamanlarda değiştirilmesinden ibaretti. Hem komuta merkezindeki vericinin hem de torpidodaki alıcının aynı anda aynı frekansa geçebilmesi için önceden hazırlanmış delikli kartlar kullanıyorlar ve bu şekilde programlanmış olan verici-alıcı çifti daha önceden belirlenmiş olan seksen sekiz farklı frekansa atlıyordu. Seksen sekiz farklı frekans ve delikli kartların esin kaynağı muhtemelen o zamanlar yaygın olan delikli kağıtlarla çalışan otomatik piyanolardı.

Frekans atlamalı haberleşme sistemi, günümüzde askeri telsizlerden cep telefonlarına çok yaygın kullanılan "spread spectrum" tekniğinin temelidir. 1997 yılında Electronic Frontier Foundation, bu alandaki öncü rolünden ötürü Hedy Lamarr'ı onurlandırmıştır.

KARA ODALAR

1628 ilkbaharında Fransız kraliyet ordusu güneydeki Réalmont kalesini kuşattığında oldukça ciddi bir direnişle karşılaşmıştı. Fransızlar bilmiyorlardı ama kaleyi başarıyla savunmalarına rağmen kuşatılanlar aslında çok zor durumdaydılar. Kaledekilerin yardım istemek amacıyla dışarıya gönderdikleri habercinin taşıdığı şifreli mektubu ele geçiren Fransızlar, şifreyi çözemeyince, yakındaki Albi kasabasında yaşayan ve şifre çözmede usta olduğunu öğrendikleri genç Antoine Rossignol'dan yardım istediler. Rossignol çok kısa sürede mektubun şifresini çözdü. Fransızlar mektubun çözülmüş halini kuşatma altında olanlara gönderince kaledekilerin direnci sona erdi ve Réalmont teslim oldu. Bu başarısının ardından Antoine Rossignol kralın hizmetine girdi. Kral XIII. Louis ölüm döşeğindeyken Rossignol'ün kraliyet için en önemli kişilerden biri olduğunu söyledi. Kral XIV. Louis de kendi odasının hemen yanı başında bir oda tahsis etti ona. Bu görevde Rossignol, Fransa'nın hasımlarının, özellikle İngilizler ve İspanyolların şifreli mesajlarını çözdü. Baba Antoine Rossignol'dan sonra oğul Bonaventure üstlendi bu önemli görevi. Baba, oğul birlikte, kriptografi tarihinde Büyük Şifre diye bilinen yöntemi geliştirdiler. Bonaventure bir kazaya kurban gidince kardeşi Antoine-Bonaventure sürdürdü bu görevi ve aile mesleğini.

> Kriptanaliz gibi müthiş yaratıcılık gerektiren mesleği en iyi icra eden kişinin oğullarına isim koyarken biraz daha yaratıcı olmasını beklerdim.

1700'lerde birçok Avrupa ülkesi, başkalarının şifreli yazışmalarını okumak için *Kara Oda* (*Black Chamber*) diye adlandırılan özel ofisler kurmuştu. Bunların arasında en bilineni Viyana'daki Kara Oda (Geheime Kabinets-Kanzlei) idi ki en iyisi olduğu söylenirdi. Elçiliklere gelen ve giden mektupları gizlice açıp çok kısa sürede şifrelerini çözüyor ve okuyorlardı. Elde ettikleri gizli, özel bilgileri sadece Avusturya için kullanmakla kalmıyor, başkalarına da satıyorlardı. O zamanlar ve daha sonraları Kara Odalar çok önemli kurumlar haline gelmişlerdi.

Birinci Dünya Harbi'nin akabinde, 1919'da Herbert Osborne Yardley tarafından Amerika Birleşik Devletleri Kara Odası kurulmuş ve kriptanalistler çalışmaya başlamıştı. Bu sayede Almanların ve Japonların bir sonraki savaş öncesi niyetlerini, hatta planlarını öğrenme imkân ve fırsatlarına kavuşmuşlardı. Ancak, 1929'da Dışişleri Bakanlığına

atanan Henry Lewis Stimson, Amerikan kara odasını lağvetti. Gerekçesi: Centilmenler başkalarının mektuplarını okumazlar...

> Centilmenler başkalarının mektuplarını okumazlar diye kara odayı lağvedecek kadar, düşman dahi olsa, haberleşme mahremiyetine saygı duyan Dışişleri Bakanı Stimson, Birinci Dünya Harbi öncesinde ve İkinci Dünya Harbi boyunca Savaş Bakanlığı görevini yürüttü (O dönemlerin görev tanımları daha dürüstmüş.) Yetmiş üç yaşında ikinci kez atandığı Savaş Bakanlığı döneminde Manhattan Engineering District diye adlandırılan atom bombası projesini başlattı ve yönetti. Sadece idari sorumluluğun ötesinde, balayını geçirmiş olduğu için sempati duyduğu Kyoto'yu hedef listesinden çıkarıp yerine Nagasaki'yi koyacak kadar içerisindeydi işin. İnsan düşünmeden edemiyor, haberleşme mahremiyetini bu denli önemseyen nazik beyefendiyle hangi on binlerin öleceğine karar veren adam aynı kişi olabilir mi diye. Keşke haberleşme mahremiyetini o denli önemsemeseydi de savaşın gidişatını erkenden kontrol edebilecek, hatta savaşı önleyebilecek tedbirlerin alınmasını mümkün kılsaydı. Bu ne çelişki!..
>
> Şunun altını çizmek isterim ki kimyacıların, fizikçilerin savaşı çok kirli, ölümcül; halbuki **matematikçilerin savaşı ölümleri engelliyor** bir bakıma.
>
> Bu noktada bahsetmeden geçmek haksızlık olurdu: Almanya'da Arthur Scherbius elektromekanik şifre makinesi Enigma'yı icat ettiği yıllarda Amerika'da Edward Hugh Hebern de benzer bir cihaz icat etmiş, ancak yeterli ilgiyi görmediği için iflas etmişti. Kurduğu şirkete para yatırmış olan yatırımcılar onu mahkemeye vermiş, mahkum ettirmişlerdi. Yıllar sonra inatla başka cihazlar yapıp askeriyeye sattıysa da para kazanamadan, değeri bilinmeden öldü zavallı adam.
>
> Centilmenler başkalarının mektuplarını okumazlar diyen veya Hebern'i iflasa sürükleyen zihniyetin şimdi gelmiş olduğu yeri düşündükçe gülümsemeden edemiyor insan.

R.I.P.

> İngilizce ölüm ilanlarının alt köşesinde genellikle R.I.P. yazar, "Huzur içinde yat" anlamında "Rest in Peace" ifadesinin kısaltması. Aslında İngilizce ifade de Latinceden uyarlanmıştır: "Requiescat in Pace."
>
> Bilgi harbinin ölüm ilanı ile ne alakası var?

İngiltere'de yerli veya yabancı kişiler, sivil veya resmi kurumlar arasında yapılan haberleşmenin izlenmesi, mektupların okunması, telefonların dinlenmesi öyle gelişigüzel olmaz; her şey yasal düzenleme altına alınmıştır. Önceleri, araştırma erkini düzenleyen yasa tasarısı (Regulation of Investigatory Powers Bill - RIP Bill) adıyla gündeme gelen düzenleme, 2000 yılında Regulation of Investigatory Powers Act (RIPA) adıyla yasalaşmıştır.

Dikkati şayandır ki aslında haberleşme mahremiyetini hiçbir düzene riayet etmeden, umarsız ve saygısızca ihlal etmenin yolunu açıyor olmasına rağmen yasanın başlığında "düzenleme" kelimesi öne çıkarılmaktadır. İroninin böylesi...

RIP yasası (RIPA) uyarınca kişilere veya kurumlara yönelik araştırma beş şekilde gerçekleştirilebilir:

-- Haberleşmenin içeriğinin izlenmesi: Telefon görüşmelerinin dinlenmesi, mektup veya e-posta mesajlarının okunması…

-- Haberleşme bilgisi (Communications Data - CD): Haberleşmenin içeriği yerine sadece kayıtlarının izlenmesi. Örneğin, kullanılan servis bilgisi, trafik bilgisi, abone bilgisi gibi konuşmanın veya yazışmanın içeriğini değil de kimin kimle, ne zaman, hangi vasıtayla haberleştiğini gösteren bilgi bu kapsamda değerlendirilir.

-- Girişimsel izleme: Evin, özel aracın veya benzeri yerlerin gözlenmesi, fotoğraf veya filminin çekilmesi, buralara gizli dinleme veya gözleme cihazları yerleştirilmesi ve benzeri… İzleme veya dinleme cihazı evin veya aracın dışında olsa da, eğer içerideymişçesine nitelikli ve ayrıntılı bilgi sağlıyorsa girişimsel izleme olarak kabul edilir. Kişinin veya aracın nereye gittiğini veya nerde olduğunu takip eden cihazlar vasıtasıyla yapılan izleme girişimsel izleme kapsamında değildir. (Girişimsel izleme amacıyla özel konut veya işyerine cihaz yerleştirilmesi polis ve istihbarat teşkilatları ile ilgili özel yasalara tabidir.)

-- Yönlendirilmiş izleme: Doğrudan gizli takip. Kişinin halka açık yerlerde gizlice izlenmesi, gözetlenmesi, görüntülü veya sesli kayıt altına alınması…

-- Gizli insan istihbaratı kaynağı: Kişisel bağlantılar (yerleştirilmiş ajanlar veya muhbirler) vasıtasıyla bilgi edinilmesi…

Bu yasa gereği, ilgili bakanın izniyle, istihbarat kuruluşlarının (*) yanı sıra bazı polis departmanları haberleşme bilgisini veya haberleşmenin içeriğini izleyebilir ve kaydedebilir. Dahası, özel konut, işyeri veya arabanın içerisinden ses veya görüntü alabilir, kaydedebilir.

(*) GCHQ, Savunma (Bakanlığı) İstihbaratı, Güvenlik Servisi (Secret Service - MI5), Gizli İstihbarat Servisi (Secret Intelligence Service - SIS - MI6)

İçeriğe girmeden sadece haberleşme bilgisi (CD) toplamak veya kişileri gizlice takip etmek, sözü edilen istihbarat kuruluşlarının yanı sıra -mesela sanayi ve ticaretten tarıma, çevre korumadan sağlığa- bir dolu yerel resmi kurumun yetkisindedir. Hatta, haberleşmenin taraflarından biri izin veriyorsa (boyun eğiyorsa) diğer taraf için izin almaya gerek bile yoktur. Kasım 2012'ye dek gerek haberleşme bilgisinin (CD), gerekse haberleşme içeriğinin izlenmesi için sadece "yürütme"den izin alınıyordu; "yasama"dan değil. İzleme talebinde bulunan kurumun üst amirinin izni yeterliydi. Özgürlüklerin korunmasına yönelik Protection of Freedoms Act adlı yasayla bu keyfi duruma bir nebze olsun sınırlama getirilmiş, yerel resmi kurumların taleplerinin sulh hakimi tarafından onaylanması koşulu konmuştur. Ancak, bu koşul sadece haberleşme bilgisi (CD) ve doğrudan izleme talebinde bulunan kamu kurumları için söz konusudur; haberleşmenin içeriği dahil her türlü bilgiye erişimi olan GCHQ, MI5, MI6 gibi istihbarat kuruluşları için

geçerli değildir. (Her ne kadar eski bir yargıç olması gerekse de, izin veren "izleme komiseri" yürütme erkine bağlı olarak görev yapmaktadır.)

> Haberleşmenin içeriğinin izlenmesi amacıyla istihbarat kuruluşları veya bazı polis departmanlarının yetkilendirilmesi için gerekçeler şunlardır:
>
> -- Ulusal güvenlik
>
> -- Ciddi suç eylemini tespit etmek veya önlemek
>
> -- Ciddi suça karşı uluslararası karşılıklı anlaşmaların gereğini yerine getirmek
>
> -- Birleşik Krallığın (UK) ekonomik refahını korumak
>
> Herhangi bir konuda "ulusal güvenlik" söz konusu olduğunda akan sular durur, zaten. Olur olmaz her şey ulusal güvenlik gerekçesiyle yapılabilir. Birçok ülkede bu bahane çok yaygın olarak kullanılmaktadır ama ülkenin ekonomik refahını korumak sık başvurulan bir bahane olmasa gerek. (Aslında böyle açıkça belirtmelerine gerek yoktu; ulusal güvenlik kisvesi altında bunu da halledebilirlerdi, nasıl olsa.)
>
> 2009'daki G20 zirvesinde Türkiye Cumhuriyeti Maliye Bakanı'nın ve delegasyonunun telefon görüşmelerinin dinlenmiş, elektronik yazışmalarının okunmuş olduğu haberi 2013 yılında basında yer aldığında Türkiye'de şaşkınlık ve kızgınlık, İngiltere'de mahcubiyet yaratmıştı. Türkiye'nin kızgınlığını anlamak mümkün ama İngiltere'nin mahcubiyeti biraz göstermelik gibi. Ne diyeceklerdi ki? "Kusura bakmayın, bizim kanunumuz böyle; biz dinleriz," mi diyeceklerdi? Mahcubiyetleri, dinledikleri için değil, yakalandıkları için olsa gerek.

Haberleşmede veya bilgiyi saklamada eğer şifre kullanılıyorsa, RIP yasası gereği bu şifrenin anahtarının -talep edilmesi halinde- güvenlik kurumlarına verilmesi gerekiyor; aksi takdirde para ve hapis cezası söz konusu.

Neredeyse hemen herkesin dinleme ve izleme yetkisi almasına imkân tanıyan yasa yetkisiz dinleme ve izlemeyi cezalandırmaktadır ama dinleyen ve izleyen yetkili devlet kurumu olduğu sürece bunda beis görülmemektedir. RIP yasası için esas olan yetkilendirmedir, işin ahlaki veya insan hakları boyutu değil.

Peki dinleme ve izleme bu denli fütursuzca uygulanıyor olduğu halde nasıl oluyor da açığa çıkmıyor, kamuoyuna yansımıyor? Çünkü, yetkisiz dinleme ve izlemeye verilen cezanın çok daha fazlası yetkili dinleme ve izlemenin ifşa edilmesi halinde veriliyor. Dinleme ve izlemeyi ifşa etmek çok ciddi bir suç olduğu için mezara kadar götürülen bir sır olarak kalıyor.

> Schrödinger'in kedisi...

Sonuç olarak, kimin, ne zaman, nerede, nasıl dinlendiği veya izlendiği asla bilinmediği bir durumda dinlemenin yapıldığı iddia edilemez ama yapılmadığı da söylenemez.

> Burada mesele, bireyin özeline devletin müdahale ediyor olması değil. Bu ayrı bir tartışma konusu olabilir. Şahsi görüşüm, belirli kurallar çerçevesinde ve mutlaka yargı denetiminde bu müdahalenin yapılmasından yana. Ancak burada vurgulamak istediğim, İngiltere gibi kendisini demokrasi havarisi ilan eden ve daha önemlisi

başkaları tarafından öyle görülen bir ülkenin kendi vatandaşlarını ve yabancıları gizlice dinleme veya izlemede, yargı denetiminden vareste, hayli pervasızca hareket ediyor olması. Üstelik, bu konuda bize ve başkalarına ders vermeye kalkışırken…

Başbakan Tony Blair döneminde yasalaşan RIP yasası (RIPA) karşıtı kampanyaya imza koyanlar arasında bir isim dikkatimi çekti: Richard Blair.

-- Kim bu Richard Blair?

-- Eric Blair'in evlatlık oğlu.

-- Tony Blair ile alakası var m?

-- Hayır.

-- Peki, Eric Blair kim?

-- Büyük Birader'in herkesi izlediği distopik roman "1984"ün yazarı George Orwell.

Ey İngiliz demokrasisi, huzur içinde yat!.. R.I.P.

TAMAM O ZAMAN

-- Ulusal güvenlik mi? Tamam o zaman.

Özel -olması gereken- bilgi ve haberleşmeyi elde etmek için sadece İngilizler değil, Amerikalılar da aynı bahaneye başvuruyorlar: ulusal güvenlik… Akar sular duruyor, ulusal güvenlik söz konusu olduğunda.

Mali konularda mahremiyetle ilgili 1978 tarihli Mali Mahremiyet Yasası, kanun uygulayıcının bir şirketle ilgili mahrem mali bilgiyi elde etmek amacıyla önceden haber vermesi koşulunu getirmektedir. Kanun uygulayıcı -ki genellikle FBI- yabancı istihbarat kuruluşları veya suç örgütleri ile ilgili para trafiğini izlemek amacıyla yasadaki bu maddeye dayanarak finans kuruluşları veya şirketlere mektup gönderip onlardan bilgi talep edebiliyordu. Ancak, bu talebe cevap vermek mecburi değildi. 1986 yılında yasalaşan değişiklikle bu taleplere riayet etme mecburiyeti getirildi. Bilahare, FBI bu mektupları sadece finans kuruluşlarına değil, haberleşme kuruluşlarına da göndermeye başladı. 11 Eylül saldırısından sonra kabul edilen Yurtseverlik Yasası, bu tür talepleri gerekli kılan koşulları hafifletmenin yanı sıra, Amerikan yurttaşlık hakları ihlalleri ile ilgili denetimi de kaldırdı. Artık, "terörizm veya casusluk şüphesi" yeterliydi. Tabii ki iş çığırından çıktı… 2003-2005 arasında FBI 140.000'den fazla bu tür talepte bulunmuş.

Ulusal Güvenlik Mektubu (National Security Letter - NSL) adı verilen bu mektuplar herhangi bir yasama merciinin onayından veya denetiminden geçmeden gönderilse de yine de itiraz için yasal yollara baş vurulabilir. Ancak, bu noktada "gag order" denilen "susma emri" devreye giriyor. Bu mektuplar, beraberinde konuşma yasağı da içerdiği için talebin neyle alakalı olduğu ve hatta talep mektubunun alındığıyla ilgili konuşmak veya açıklama yapmak ciddi müeyyide getirmektedir.

> Bu numarayı İngilizler mi Amerikalılardan, Amerikalılar mı İngilizlerden, yoksa her ikisi de Ruslardan mı almışlar; emin olamıyor insan. Çok önceleri de vardı, muhakkak.

Böyle bir NSL alan bilgi depolama, bilgi güvenliği veya haberleşme firması bu talebin gereğini yapmakla yükümlüdür. İnternet servis sağlayıcılar, işletim sistemi geliştirenler, güvenlik yazılımı veya donanımı tasarlayanlar ve bu hizmetleri sunanlar FBI veya NSA gibi güvenlik kuruluşlarının bilgiye ulaşmasına imkân tanırlar. Kimi zaman güvenlik kuruluşlarının yerleştirdiği "arka kapı" donanım veya yazılıma göz yumar, kimi zaman kendileri yerleştirirler.

> Mesela, kuvvetli bir kriptografik algoritma tasarımcısı kullanmakta olduğu rastgele sayı üretecinin (RNG) rastgeleliğini biraz bozabilir.

ABD güvenlik kuruluşlarının -herhangi bir yasama denetimine tabi olmadan- haberleşme ve bilgi mahremiyetini ihlal etmekte olduğu bilinen bir gerçektir.

> Ed Snowden, Laura Poitras ve Glenn Greenwald'a teşekkür edilebilir, belki; ancak, göz önünde bulundurmakta yarar var ki Snowden, diğer ülkeleri paniğe sevk edip "yılan yağı"na yönelmelerini sağlamak için düzenlenmiş bir mizansenin oyuncusu da olabilir.

DİNLEMEK, DİNLENMEK

> Dinlemek ve dinlenmek; ikisi de olumlu çağrışımlar yapan kelimelerdir dilimizde. En azından yakın zamana kadar böyleydiler. Dinlemek, karşıdakine değer vermenin, saygı duymanın göstergesiydi; (sözü) dinlenmek ise saygıdeğer olmanın...
>
> Şimdilerde dinleyene kötü gözle bakılır, dinlenmekten korkulur oldu. Bu anlam değişikliği birçok kişinin kendini önemli sanmasına yardımcı oluyor belki ama bir nevi toplumsal paranoyaya yol açmakta.

Başkalarının mektuplarını okumak, telefonlarını dinlemek, mektubun veya telefonun icadından bu yana yapılagelen bir iştir. İştir; çünkü istihbari değeri vardır; askeri, siyasi, ekonomik avantaj sağlar; kuvvet dengesini değiştirir; suçu önler, suçluyu yakalamaya yardımcı olur, adaleti sağlar...

Başkalarının mektuplarını ele geçirip gizlice okumak için kara odalar kurulmuş, yazılı mesajların muhatabı dışında okumasını engellemek için gizli yazım (kriptografi, steganografi); gizli yazıyı açık hale getirmek içinse kriptanaliz, steganaliz teknikleri geliştirilmiştir. Yazılı mesajlar söz konusu olduğunda esasen matematik temelli kriptografi ve kriptanaliz teknikleri uygulanmaktadır. Haberleşmenin en temel hali olan konuşmanın dinlenmesi veya dinlemenin önlenmesi için yine en temel yöntemlere başvurulmakta; konuşmada iletilen bilginin ele geçmesini önlemek için ya dinlemeyi engellemeye, ya da -dinlense bile- anlaşılırlığı bozmaya çalışılmaktadır.

GSM, DECT, VoIP hariç, ev veya işyerinde yaygın kullanılan sabit telefon sisteminde konuşma genellikle -en azından telefon cihazı ile santral arasında ve santralın bir

bölümünde- analog sinyal olarak iletilir. İşte bu aşamada sisteme girerek konuşma dinlenebilir. Dinlenmeyi engellemek için müdahale edilemeyen, güvenli bir iletişim sistemine ihtiyaç vardır ki çoğu zaman bu pek mümkün olmaz. Daha ziyade, dinlense bile anlaşılırlığı bozan veya azaltan yöntemlere başvurulur. Bu amaçla kullanılan bazı yöntemler frekans bandını ters çevirmek veya konuşmanın üzerine gürültü eklemekle gerçekleştirilir. Bu ve benzeri, "analog" yöntemlerin genel adı, karıştırmadır (scramble).

> Çocukken oyun olsun diye konuştuğumuz kuş dili basit bir karıştırma yöntemiydi. Biraz daha zor olsa da kelimeleri tersten söylemek de öyle… Kimsenin Fransızca bilmediği bir ortamda Fransızca konuşmak da bir nevi karıştırmadır; nihayetinde, istenen gizliliği sağlamaktadır. İkinci Dünya Harbi'nde Japonlarla savaşan Amerikalılar telsiz operatörü olarak Navajo yerlilerini kullandılar, nasıl olsa Japonlar Navajo yerli dilini anlamazlar diye. Oldukça etkili olmuştur bu yöntem. (Aslında bu tür karıştırmalar da matematiksel yöntemlerdir. Türkçeden Fransızcaya tercüme yapmak bile bir bakıma yerine koyma (substitution) yöntemidir.)

GSM, DECT, VoIP ve benzeri sistemlerde olduğu gibi ses sinyali eğer "analog"dan "digital"e (sayısal) çevrilir ve bu sayısal veri üzerinde şifreleme uygulanırsa bu tür karıştırma artık kriptografinin alanına girer. DECT telefonlarda el cihazı ile evdeki veya işyerindeki baz cihazı arasındaki iletişim sayısal telsiz sinyali vasıtasıyla gerçekleştirilir. Benzer şekilde, GSM cep telefonlarında el cihazı ile baz istasyonu arasındaki iletişim sayısal olarak gerçekleştirilmektedir. Analog ses sinyali telefon cihazında sayısala çevrilmiş olduğundan, el cihazı ile baz cihazı veya baz istasyonu arasına giren bir kimse duyduğundan bir şey anlamaz. Bu sayısal sinyal ayrıca şifrelenmiş olduğu için sayısal sinyali analoga çevirmek de pek işe yaramaz. Buraya kadar sistem oldukça güvenli görülse de ne var ki uygun donanım ve yazılım yardımıyla şifre kırılabilir ve böylece konuşma dinlenebilir.

> GSM el cihazı ile baz istasyonu arasında havadan aktarılan bilgi (konuşma, görüntü, veri) şifrelenerek aktarılır. Bu şifreleme algoritması yıllar önce kırılmıştır ama önemli sorun teşkil etmez bu. Özel ekipmana sahip olmayan, ortalama bir kullanıcının bir başkasını dinlemesini engellemektir amaç.

GSM el cihazı ile baz istasyonu arasında havadan aktarılan konuşma özel ekipman vasıtasıyla dinlenebilir. Ancak, yetkili dinleme yapıldığında, dinlemenin santralde yapılması çok daha pratiktir.

Ortam dinlemesi (bug, böcek) de çoklukla uygulanan bir yöntemdir ki bu durumda dinlenen konuşmanın veya izlenen görüntünün şifrelenmesi söz konusu değildir. Ortamdaki konuşma ve görüntü ham haliyle elde edilir.

Halihazır teknoloji telli, telsiz, GSM ve benzeri telefon görüşmelerini, internet üzerinden gerçekleştirilen haberleşmeyi ve ortam dinlemesini oldukça kolay hale getirmiştir.

Bireysel hakların ve özgürlüklerin güvence altında olduğu ülkelerde gerek açıkta gerekse santralde gerçekleştirilen telefon ve ortam dinlemesi yasal düzenlemelere tabidir; yetkisiz dinleme muhakkak cezalandırılır; cezalandırılmalıdır.

KARDA YÜRÜMEK

Bu kitapta birçok örneğine yer verildiği üzere,

Binlerce yıl boyunca, haberleşmenin izlenmesi ve değiştirilmesi ve yönlendirilmesi (monitoring and manipulating), güvenliği sağlamanın ve sürdürmenin en önemli aracı olagelmiştir. Siyasi, askeri dengelerin ve ittifakların kısa, orta veya uzun vadede değişebileceği, hatta mutlaka değişeceği göz önüne alındığında, dinlemek ve dinlenmek gerçek bir olgu olarak değerlendirilmelidir. Bundan ötürü yerinmek veya övünmek gereksiz ve anlamsızdır.

Doğrusu, dinleme ile ilgili yeteneğin gerçek seviyesi asla ifşa edilmez; edilmemeli. Ancak, bazıları, bir algı yönetimi yöntemi olarak gerçeği abartıyor olabilir. Tabii ki bu propagandanın teknik altyapı ile uyumlu olması gerekir.

Ülkelerin birbirini dinlemiş olduğu ile ilgili haberleri aslında dinleyen taraf bakımından bir fiyasko olarak nitelendirmek gerekir. Açığa çıkmak, en utanç verici durum olmalı. Ancak, karşı tarafta kuşku, panik, bezginlik ve kendini zayıf görme hissi yaratmak ve onu hata yapmaya yöneltmek amacıyla kullanılabilir.

Bu sayfa bilhassa boş bırakılmıştır

İKİNCİ BÖLÜM

Bu bölümde, bilgi harbini operasyonel düzeyde uygulayan Amerika Birleşik Devletleri, Rusya Federasyonu ve Çin Halk Cumhuriyeti bilgi harekâtı doktrinleri ile ilgili açık kaynaklardan derlenmiş malumat değerlendirilmektedir.

- . -

KIYASLAMALI BİLGİ HAREKÂTI DOKTRİNLERİ (ABD, ÇİN, RUSYA)

Modern harbin planlanmasını, yürütülmesini, sonuçlanmasını, bir başka ifadeyle gidişatını etkileyen önemli bir unsur olması sebebiyle bilgi harekâtı oldukça ayrıntılı ele alınan, çerçevesi, kapsamı ve kuralları mümkün olduğunca belirlenmeye çalışılan bir harp tarzı haline gelmiştir günümüzde. Dolayısıyla, önde gelen askeri güçlerin bu olguyu göz ardı etmesi beklenemez. Hemen hepsi bu konuda kapsamlı çalışmalar yapmışlar ve Bilgi Harekâtı (Information Operations - IO)doktrinlerini oluşturmuşlardır.

ABD, Rusya ve Çin'in yanı sıra tabii ki Almanya, Brezilya, Bulgaristan, Fransa, Hindistan, İngiltere, İran, İspanya, İsrail, İsviçre, İtalya, Japonya, Malezya, Pakistan, Polonya, Türkiye, Güney Afrika, belki Yeni Zelanda, tüm ülkeler muhtemelen hazırlamışlardır kendi doktrinlerini.

> Bugüne dek hazırlamadılarsa da mutlaka hazırlayacaklardır; hazırlamalılar.

Mevzuun esasını ve temel kavramları tanımlamada yardımcı, hatta belirleyici olması ve uluslararası terminolojiyi oluşturması sebebiyle ABD Bilgi Harekâtı (IO) doktrinini ilk olarak ele almayı ve ardından Rusya ve Çin doktrinlerini de incelemeyi uygun gördüm.

1996-2012 yılları arasında güncellenen ABD Bilgi Harekâtı doktrini temel kavramlar, uygulama pratikleri, tanımlar ve terminolojiyi açık ve ayrıntılı şekilde ortaya koymaktadır. Yirmi seneye yakın dönemi kapsayan güncellemeler bir bakıma bilgi harekâtının tarihsel gelişimini de göstermektedir.

> Tarihsel gelişimi gösterme bakımından yirmi sene kısaymış gibi görünse de söz konusu modern bilgi çağında hızla değişen ve gelişen bilgi ortamı ve bilgi teknolojileri olduğunda yeteri kadar uzun sayılır.

Konu ile ilgili neredeyse eğitim dokümanı sayılabilecek ABD Bilgi Harekâtı doktrinleri diğerlerine (Rusya, Çin) nazaran çok daha ayrıntılı ele alınmayı hak etmektedir.

1996, 1998, 2003, 2006 ve 2012 Bilgi Harekâtı (IO) doktrinleri ekte ayrıntılı olarak ele alınmaktadır.

İncelendiğinde görülmektedir ki Rusya Federasyonu ve Çin Halk Cumhuriyeti doktrinleri ABD doktrinlerinden oldukça etkilenmekte; uygulamada farklılık gösterseler de kavramlarda ve terminolojide fazlasıyla yararlanmaktadırlar. Pek tabiidir ki diğer ülkelerin -eğer varsa- bilgi harekâtı doktrinleri de ABD'ninkinden etkilenmişlerdir.

AMERİKA BİRLEŞİK DEVLETLERİ

Bilgi Harekâtının (Information Operations - IO) amacı bilgi üstünlüğünü elde etmek ve muhafaza etmektir. Bilgi üstünlüğü, daha etkin karar almayı ve uygulamayı mümkün kılar. Komuta kademesi, ortaya çıkan fırsat pencerelerini daha çabuk ve doğru şekilde değerlendirir; dolayısıyla, daha az zayiatla daha etkili ve yararlı sonuç alınır.

Taarruz amaçlı bilgi harekâtı, düşmanın karar vericilerini, haber alma ve komuta-kontrol mekanizmasını etkilemek, yanıltmak, aldatmak, faydalanmak, karıştırmak, bozmak, hatta yok etmek amacıyla yürütülür. Savunma amaçlı bilgi harekâtı ise, dost kuvvetlerin komuta-kontrol mekanizmasının sağlıklı çalışmasını ve doğru karar vermesini sağlamak amacıyla yürütülen koruyucu ve önleyici tedbirlerden oluşur.

1996 tarihli FM 100-6, eski tabirle Sahra Talimnamesi (Field Manual), askeri anlamının ötesinde genel hatlarıyla tanımlıyordu bilgi harekâtını. Daha önceleri, bilgi veya komuta-kontrol (C^2) ile alakalı harekât söz konusu olduğunda akla Elektronik Harp - EH (EW) ve Elektronik Karşı Tedbirler - EKT (ECM) ve Elektronik Karşı Karşı Tedbirler - EKKT (ECCM) geliyordu. Özellikle haberleşmeye yönelik elektronik harp ve kripto ve istihbarat vasıtasıyla bilgi üstünlüğünün sağlanabileceği sanılıyordu; belki sağlanabiliyordu da. Ancak, zaman hızla -talimnameleri umursamadan- değişiyor. 1990'larda, özellikle Körfez Savaşı'nda, bilgi harbinin tamamen kendine özgü, yeniden tanımlanması ve geliştirilmesi gereken bir kavram olduğu görüldü. Tabii ki hemen talimnameler gözden geçirildi, hatta gerektiğinde, yenisi yazıldı.

Modern silahların hassasiyeti, menzili ve ölümcüllüğü, komutanları ademi merkeziyetçiliğe, kuvvetlerini dağıtmaya, komutayı merkezden uzaklaştırmaya yöneltmiştir. Böylesi dağıtılmış kuvvetler ve komuta kademesinden fayda elde etmek için doğru ve güvenilir haberleşme elzemdir. Haberleşmenin sekteye uğraması veya güvenilirliğini yitirmesi bu gelişmiş silahların ve modern muharebe yöntemlerinin işe yararlığını zedeler. Bu yüzden, savaşın gidişatını değiştirmede insanların ve savaş makinelerinin imhasından ziyade düşmanın sahip olduğu bilgiye ve bilgi sistemlerine saldırmak daha etkilidir.

İçinde bulunduğumuz bilgi çağında bilgi iletişim sistemlerinin sürati ve yaygınlığı, askeri harekâtların doğasında devrim niteliğinde değişime sebep olmaktadır. Bilgiyi hedefleyen bilgi harekatı, kendi bilgisini muhafaza ederken düşmanınkini bozmaya veya ele geçirmeye çalışmanın ötesinde, askeri olmayan kaynaklarca yayınlanan bilgi ile de ilgilenmeyi gerektirmektedir. Bilgi harekâtı, sadece askeri bilgi ortamında değil, çok

daha geniş küresel bilgi ortamında yürütülmek durumundadır. Küresel bilgi ortamı ve altyapısı, askeri bilgi sistemlerinin yanı sıra ulusal ve küresel bilgi sistemlerini, medyayı ve kamuoyunu kapsamaktadır. Bu bağlamda, bilgi harekâtı artık karargâhın, garnizonun, cephenin ötesinde; medya, endüstri, müttefikler ve tüm dünyaya yayılmış bilgiyi hedef almaktadır.

Herhangi bir ihtilafta müşterek veya çokuluslu operasyon söz konusu olduğunda silahlı kuvvetlerin görevini tam yerine getirebilmesi için bilgi ortamına hakim olması gerekir. Yine de insanın müdahalesi, bilgiyi, teknolojiyi ve eylemi bir araya getiren komutanların ve askerlerin etkisi olmadan bilgi harekâtı atılımını gerçekleştirmek mümkün olamaz. Bilgi harekâtı mucize çözüm getirmiyor; nihaî hedef askeridir.

° Temel Beceriler

Bilgi harekâtının yürütülmesinde, harekât güvenliği, psikolojik harekât, askeri yanıltma, elektronik harp, fiziki imha, sivil ve halkla ilişkiler gibi temel becerilerden yararlanılmaktadır. Zamanla tanımlarda değişiklikler yapılmış; bazı çıkarmalar ve istihbarat, istihbarata karşı koyma, bilgisayar ağları, siberuzay ile ilgili eklemeler yapılmış olsa da temel kavramlar pek değişmemiştir.

° Temel Yaklaşım

Amerikalılar, bilgi harekâtını tüm yönleriyle ele almakta, kavramları ve uygulama yöntemlerini ayrıntılı şekilde tanımlamakta ve kamuoyu ile açıkça paylaşmaktadırlar.

ABD Bilgi Harekâtı (IO) doktrini, bilgi harekâtını önceleri bir destek unsuru olarak ele almaktayken, zamanla askeri harekâtın esas unsuru olarak değerlendirmektedir. Ama her halükârda nihai hedef askeridir; uygulama askerler tarafından ve/veya askerlerin denetiminde yürütülmektedir.

Savaşın yanı sıra krizde veya barışta, askeri ortamın ötesinde ulusal ve uluslararası ortamda yürütülen bir harekât tarzı olması sebebiyle uygulamada birtakım kurallar konmuştur ki bunların içerisinde kendi ülkelerinde, kendi vatandaşlarına yönelik psikolojik harp uygulamamak kuralı dikkate değer.

Bu kural ABD Anayasa'sı ve yasalarından kaynaklanmaktadır.

RUSYA FEDERASYONU

Bilgi harbi söz konusu olduğunda Rusya Federasyonu (RF) ile Sovyetler (SSCB) dönemini birlikte değerlendirmek gerekir. Her ne kadar özellikle bir Bilgi Harekâtı doktrini kaleme alınmış olmasa da (en azından ben henüz bulamadım) askeri doktrin içerisinde bilgi harekâtının önemi vurgulanmaktadır.

Ruslar için bilgi her durumda çok önemlidir; elde edilmesi, manipülasyonu, üstünlük sağlanması… Amerikalılar gibi doktrine etmeseler de aslında bilgiyi bir harp unsuru olarak kullanmada hayli tecrübelidirler ve kavramsal olarak bilgi harbi veya bilgi harekâtı ile fazlasıyla aşinadırlar.

Rusların yaklaşımını değerlendirirken Bilgi Harbi (Information Warfare - IW) terimini kullanmak daha doğru olur; çünkü onlar öyle görüyorlar.

> Bilgi harekâtı terimindeki "harekât" kelimesi İngilizce "operasyon" kelimesini karşılığı olarak kullanılmaktadır. Hemen her sektörde bu kelimeyi çok yaygın kullanan Amerikalılar askeri literatürde de bu tercihi sürdürmüşlerdir. Bunun psikolojik avantajı da göz ardı edilmemeli; nihayetinde harp etmiyor, operasyon yürütüyorlar. Halbuki Ruslar pek böyle düşünmek ihtiyacı hissetmiyorlar.

Informatsionnoy voyny, bor'boy, protivoborstvom; harp, muharebe, mücadele, harekât veya operasyon… Adı ne olursa olsun, Rusya Federasyonu Güvenlik Konseyi'ne sunulan tanım şöyledir: *bilgi modellerinin oluşturduğu evrende özellikle bilgi silahlarını kullanarak yürütülen ülkeler arası mücadele*. Bu tanım gereği bilgi silahının hedefi, belli bir bilgi sistemini anlamak ve düşmanın kurmuş olduğu modeli bozmak olmalı.

Ruslar için bilgi harbi sadece kriz ve savaş hali ile sınırlı bir harekât değil, gerek barışta gerekse kriz ve savaş boyunca ve sonrasında yürütülen topyekun bir harp tarzıdır. Hatta, daha net bir ifadeyle, üstlenilen görevi yerine getirmek amacıyla yürütülen eylemler dizisi olarak görürler bilgi harbini.

> Amaç, görevi yerine getirmek; nokta!..

Ruslar, düşmanın düzenini bozmayı galebe çalmanın bir göstergesi olarak görürler. Bu sebepledir ki düşmana karşı bilgi harbi, düşmanın düzenini, organizasyonunu, yapısal bütünlüğünü bozmayı hedefler. Buna karşın, kendi organizasyonunu, düzenini korumak ise bilgi üstünlüğü (Information Superiority - IS) sağlar. Rus teorisyenler düşmanın düzenini bozmaya ağırlık verdikleri kadar bilgi üstünlüğünü elde etmeye de önem verirler; hatta, birincinin ikinciyi yaratacağına inanırlar.

> Bu düşünce tarzı, taarruzu müdafaanın önüne koymaktadır. Kendi güvenliğini sağlamak için dahi saldırmayı yeğleyen bu yaklaşım pek tabiidir ki saldırı amaçlı teknolojiyi ve uygulamaları öne çıkarmaktadır.

Rusların çok eskiye dayanan bilgi harbi ile olan ilişkisi Sovyet döneminde kalın gizlilik perdesi ardında sürmüştür. Demirperde'nin kalkmasından sonra bilgi harbi ile ilgili anlayış ve uygulamalar hakkında makaleler yayınlanmaya başlamışlardır. Sovyet döneminde ve izleyen yakın dönemde gerek iç gerekse dış baskılar ve kısıtlamalar nedeniyle haberleşme ve bilgi teknolojilerindeki gelişmelere, özellikle modern donanıma erişimleri çok kısıtlı olduğundan Ruslar daha ziyade teorik çalışmalara, matematiğe, algoritma geliştirmeye ağırlık vermişler, bu konu üzerinde çok sayıda matematikçi ve fizikçinin çalışmasına fırsat sağlamışlar ve yazılım söz konusu olduğunda hayli ileri bir düzeye erişmişlerdir. Sınırlamalara rağmen, sınırları aşan yazılım sayesinde bilgi harbinin yazılım bileşeni üzerinde çalışma imkânı bulmuşlardır.

Şimdilerde nispeten kolay erişebildikleri donanımın da yardımıyla bilgi harbi uygulamalarında oldukça ileri bir konuma gelmişlerdir.

> Kısıtlı olanaklardan yakınmak yerine bunu fırsata dönüştürmenin güzel bir örneğidir bu. Ve tabii matematik, matematik, matematik…

Rusların haberleşme altyapılarının yetersizliği de haberleşme ve bilgisayar teknolojilerinin sunduğu fırsatları yeterince değerlendirebilmelerinin önünde ciddi engel teşkil ediyordu.

Yirminci yüzyılın son çeyreğinde ve sonraki yıllarda özellikle elektronik, haberleşme ve bilgisayar teknolojilerindeki gelişmeyi ıskalayan Ruslar bunun bedelini Kosova, Çeçenistan, Gürcistan krizlerinde elektronik harp ve komuta kontrol zafiyeti olarak ödediler. Kötü tecrübelerden ders alan Rus güvenlik uzmanları hiçbir şeyin bilgi kadar önemli olmadığının altını çizmekte ve stratejik, ulusal bir değer olarak tanımlamakta; hatta net bir ifadeyle, ulusal güvenliğin temelinin bilgi güvenliği olduğunu belirtmektedirler. ABD dahi henüz yayınlamamışken, ulusal bilgi güvenliği dokümanı yayınlamışlardır 1995'te ve takip eden yıllarda bilgi güvenliği ve bilgi harbi literatürüne önemli katkıda bulunmuşlardır.

Geçmişteki mali, siyasi ve fiziki kısıtlamalardan dolayı kendi sınırları içinde kalarak teorik çalışmalara ağırlık veren bilim insanları sınır aşamayan donanımın tersine, yazılımın ve matematiğin sınırları kolayca aşabilmesinin avantajından yaralanıyorlardı. Şimdi de bilgi harbi uygulayıcıları geliştirdikleri uygulamaları sınırlar ötesine taşımada aynı kolaylıktan yararlanmaktadırlar. Günümüzde internet, bilgi harbi tekniklerinin gerek ülke içerisinde gerek başka ülkelere yönelik uygulanmasında en önemli kolaylığı sağlamaktadır Ruslara.

> Sınır tanımayan ortam, sınır tanımayan operasyonlara imkân tanımaktadır.

> Bilgi harbi uygulamalarının iki tarafı keskin bıçak olduğunu unutmamalıyız; hem saldıran hem de savunan taraf için. Teknolojiye ulaşmak, geliştirmek ve saldırı düzenlemek ne denli kolaysa saldırıya uğramak da o denli kolaydır.

Gittikçe büyüyen, tek bir küresel bilgi ortamı (bilgi uzayı - information space) oluştuğu tespitinde bulunan Ruslar, bu ortamı kendi çıkarına kullananın dünya güç dengesini değiştirebileceğine inanmaktadırlar. Öte yandan, bu hususta uluslararası kanuni önlemler ve yaptırımların yeterli olmadığının da farkındadırlar. Dolayısıyla, henüz tam endoktrine etmemiş olsalar da, küresel bilgi ortamının hayli elverişli bir harp ortamı olduğunun bilincinde ve geçmişten gelen zafiyetlerini kapatmak ve öne geçmek için yoğun gayret içerisindedirler. Bir yandan bilgi harbinde geride kalmamaya çalışırken, diğer yandan bilgi harbi eylemlerini sınırlamada uluslararası bilgi güvenliği politikası oluşturmak için uluslararası platformlarda çaba harcamaktadırlar.

> Güzel taktik; zayıf olduğun hususta bir taraftan kendi becerini geliştirirken diğer taraftan uluslararası korumaya sığınmak...

Bilgi harbi söz konusu olduğunda ne denli ciddi olduklarının göstergesi olarak, Ruslar ülkelerine ve silahlı kuvvetlerine yönelik bilgi harbi girişimini -zarar verse de vermese

de- askeri olmayan, sivil bir girişim olarak görmemektedirler; hatta karşılığında nükleer dahil her türlü tepkiyi gösterme hakkını saklı tutmaktadırlar.

> Neler yapabileceklerini bildikleri için kendilerine de neler yapılabileceğini iyi biliyorlar.

° Psikolojik ve Teknik Bilgi Harbi

Rusların bilgi harbine yaklaşımları temelde iki boyuttadır: teknik (information-technical) ve psikolojik (information-psychological).

> ABD bilgi harbi doktrininde Psikolojik Harekât bir bilgi harekâtı becerisi olarak sıralanırken Ruslar işin psikolojik boyutunu en öne çıkarmışlardır.
>
> Batı kaynaklı dokümanlarda, bilgi harbinin psikolojik boyutunda Rusların beyin yıkamadan astrolojiye, yirmi beşinci kareden mistisizme dek oldukça marjinal yöntemleri denediğinden de söz edilmektedir; ancak bu tür yöntemler bu derlemenin konusu değildir.
>
> Bunların içerisinde tepkisel (refleksif) kontrol konusuna bir paragraf ayrılabilir. Tepkisel kontrol, sizin arzu ettiğiniz karara gönüllü olarak varması ve istediğiniz davranışı göstermesi için muhatabınıza (partnerinize veya düşmanınıza) önceden tasarlamış olduğunuz bilginin aktarılmasıdır. Burada anahtar, aldığı kararı veya gösterdiği davranışı muhatabınızın kendi arzusuyla yaptığını zannetmesidir.

Ruslar, vatandaşlarının psikolojik güvenliği için bireylerin ve toplumun psikolojik istikrarını önemser ve bir bütün olarak ele alırlar. Bu kaygılarının sebebi, ülkenin baskın ideolojik yapısının son yirmi beş yılda değişmekte olmasının yanı sıra denetimsiz bilginin internet ve diğer yollarla topluma yayılıyor olmasıdır.

Bilgi harbinin psikolojik boyutunun amacı -düşman, dost veya kendi ülkesinde- bireyin ve toplumun psikolojik davranışını etkilemek; öte yandan kendi toplumunun düşman tarafından etkilenmesini önlemek olmalı. Gerek savaşta, gerekse barışta, hem askeri hem de sivil otoritenin ilgisi, amacı hatta tasası bu doğrultuda olmalı.

Sovyet dönemi ertesi, baskın ideolojinin ortadan kalktığı, daha önce erişilemeyen bilgiye kolaylıkla erişilebildiği, bireylerin ve toplulukların her türlü yönlendirme ve manipülasyona açık olduğu ortamda Rusların kendi toplumlarının psikolojik bütünlüğünü koruyabilme kaygıları bilgi harbinin psikolojik boyutunu öne çıkarmalarında önemli bir nedendir. 2000 tarihli güvenlik doktrini, stratejik bakımdan önemli bilginin Rusya Federasyonu'nun menfaatine yönelik eylemlerden korunması gerektiğini belirtmektedir.

> Rejim değişmiş olsa dahi kaygılar ve tedbirler aynı kalmıştır; öyle ki devleti korumak için bilgi ve medya ağının kontrol altına alınması ve hatta serbest medyanın millileştirilmesi (devletleştirilmesi) önerilmektedir. Söz konusu güvenlik doktrininde, bilgi ve medya ağının kontrol altına alınmasının yanı sıra, genç nesillerin ahlaki değerlerini, vatanseverliğini ve yurttaşlık sorumluluğunu geliştirmek amacıyla

kültürel mirası muhafazası ve milli kimliğin kuvvetlendirilmesi gereği gündeme getirilmektedir.

Batının, özellikle Amerikalıların haberleşme, bilgi ve komuta kontrol teknolojilerinde ulaşmış oldukları ileri seviye yeni Rusya için örnek itici güç olmuştur. (Giriştikleri askeri operasyonlardaki teknik başarısızlıkları da etkili olmuştur, mutlaka.) NATO'nun bilgi destek sistemlerinin teknolojik üstünlüğünü gördüler Kosova'da ve bizzat tecrübe etmiş oldular fiziksel olarak karşı karşıya gelmeden bilgi ortamında mücadele edilebileceğini. Bilgi harbi Ruslar için nükleer üstünlüğün ötesinde önem taşımaktadır, çünkü bu sayede gelişmiş askeri güçlerle asimetrik mücadele imkânı elde edebileceklerini fark ettiler.

Bilgi ortamını entegre hale getirmenin ne denli önemli olduğu anlaşılmış, operasyonların azami özenle yürütülmesi ve hedeflerin yüksek hassasiyette vurulması gerektiğinin farkına varılmıştır. . Bu bağlamda keşif ve komuta-kontrol teknolojileri, bilgi harbinin teknik boyuttaki önemli unsurları olarak öne çıkmakta; isabet yüzdesi yüksek, hassas -güdümlü veya güdümsüz- silahlara komuta-kontrol ve istihbarat desteği sağlayan sistemlerin de bu hassasiyetle uyumlu olması gerekmektedir. Tüm bunlar, ileri düzeyde teknoloji içeren haberleşme ve bilgi sistemlerinin var olması gereğini ortaya çıkarmaktadır.

Ruslar, bilgi harekâtının teknik boyutundaki gelişmeyi neredeyse bir devrim gibi değerlendirmektedirler. Bu açıdan bakıldığında, yıllar önce gündeme getirdikleri Askeri Teknik Devrim (Military Technical Revolution - MTR) kavramının hayata geçirilmesine örnek teşkil etmektedir bilgi harekâtı.

> Sovyet döneminin teknolojik bakımdan geri kalmış, hayli hantal askeri gücü ve bir o kadar hantal komuta kademesinin ülkenin geleceğine olan tehlikesini fark eden ileri görüşlü Rus askeri analistlerin seksenli yıllarda gündeme getirdikleri Askeri Teknik Devrim (Military Technical Revolution - MTR) kavramı şunu söyler:
>
> Yirminci yüzyılda iki temel devrim yaşandı askeri konularda: Birinci Dünya Harbi'nin kimya ve mekanik devrimi (patlayıcılar, kimyasal ajanlar, içten yanmalı motorlar, motorlu taşıtlar, uçaklar) ve İkinci Dünya Harbi'nin fizik devrimi (roketler, nükleer silahlar). Mikroelektronik, yönlendirilmiş enerji, hassas güdüm, otomatik kontrol sistemleri, gelişmiş sensörler ve benzeri teknolojiler bir sonraki askeri teknik devrimi yaratacaktır. [Birinci Bölümde sözünü ettiğim Simon Singh'in, Birinci Dünya Harbi kimyacıların, İkinci Dünya Harbi fizikçilerin savaşıydı; ancak, Üçüncü Dünya Harbinin matematikçilerin savaşı olacağı öngörüsünün bir başka ifadesi...]
>
> Birçok teknolojik gelişmede* olduğu gibi, Rusların bu teorik öngörüsü ve çözüm önerisi, başta ABD olmak üzere birçok batılı askeri güç tarafından benimsenmiş ve Askeri Konularda Devrim (Revolution in Military Affairs - RMA) adıyla hızla hayata geçirilmiştir. Bilgi harbinin teknolojik temelindeki en önemli taşlardan birini -teorik düzeyde de olsa- Ruslar döşemiştir.
>
> (*) Bu derlemenin konusunun dışında olsa da, bilinen, hoş bir hikâyedir: Radara yakalanmayan "görünmez" uçak F-117'nin o garip, çirkin şeklinin sorumlusu bir Rus matematikçidir aslında. Radar kesiti hakkında yayınlanmış bir makalesinden esinlenen ABD askeri uçak üreticisi Lockheed Martin'in efsanevi mühendislik grubu

> "Skunk Works" mühendisleri F-117'yi yarattılar. Peki, Ruslar yapabilirler miydi? Hayır. Çünkü bu garip şekilli uçağın uçmasını mümkün kılacak elektronik uçuş kontrol sistemini geliştirecek teknolojiye sahip değillerdi.

Askeri Teknik Devrim (MTR), Rusların büyük ve hantal askeri güçten teknoloji yoğun operasyonlara geçmelerini, kitle imha silahları yerine bilgi teknolojileri kullanmalarını öneriyordu. Savaşın, vurucu sistemlerin mücadelesinden ziyade bilgi sistemlerinin mücadelesine dönüşeceğini söylüyordu.

> Bu bakımdan devrim niteliğindedir ve tüm devrimler gibi tarihin sürekliliği içerisinde yer almaktadır; bir atlama değildir, zamanı gelmişti.

° Bilgi Harbi Becerileri

Bilgi harbinin zamanlamasında Rusların yaklaşımı ABD bilgi harekâtı doktrinlerinde belirtilenden pek farklı değildir; barışta, savaş öncesi ve savaşta olmak üzere farklı dönemlerde, farklı şekilde ve farklı yoğunlukta uygulanabilir. (ABD doktrininde de barış, kriz ve çatışma (savaş) dönemleri olarak belirtilmektedir.) Zamanlama ile uyumlu olarak stratejik, taktik ve operasyonel düzeyde yürütülmesi söz konusu olabilir.

Rus silahlı kuvvetlerinin bilgi harbi becerileri şu şekilde listelenmektedir:

-- Elektronik Harp

-- Psikolojik Harekât

-- Keşif (İstihbarat)

-- Yanıltma (maskirovka)

-- Matematiksel Programlama (muhtemelen bilgisayar ağlarını da içermektedir)

Bilgi silahlarının özel imalat tesisleri gerektirmediğini belirten uzmanlar, küçük bir grup insanın, fiziksel olarak sınırları aşmadan yıkıcı eylemler gerçekleştirebileceği gerçeğinin altını çizmekteler. Bir başka deyişle, küçük bir hacker grubu düşmanın kritik sistemlerine oldukça ciddi zarar verebilir.

° Maskirovka

Maskirovka, kelime anlamıyla maske, maskeleme olarak tanımlanabilir; ancak, bilgi harbi çerçevesinde kandırma, yanıltma, kamuflaj, gizleme anlamlarını da kapsar. ABD Bilgi Harekâtı doktrinindeki Askeri Yanıltma (MILDEC) karşılığı olarak düşünülebilir. Aynı zamanda hem pasif kamuflaj, hem de aktif dezenformasyon olarak kandırma anlamını da taşımaktadır. Pasif manada uygulanan maskirovka, düşmanın keşif faaliyetini etkisizleştirirken, aktif manada uygulandığına düşmanın bilgi sistemlerini ve bilgiyi manipüle ederek hem sentaktik hem de semantik düzeyde etki yaratmayı amaçlar.

Rusların bilgi harbi konsepti içerisinde maskirovka çok önemli yer tutmaktadır. Geçmişten gelen köklü maskirovka geleneğine sahip Ruslar günümüzün teknolojik imkânlarıyla bu geleneği modern yöntemlerle uygulamaktadırlar. Maskeleme, gizleme,

kamuflaj gibi pasif anlamının yanı sıra dezenformasyon, yanıltıcı bilgi anlamı içeren maskirovka, günümüzün teknolojik imkânlarıyla donatıldığında farklı bir boyuta ulaşmaktadır. Bu açıdan bakıldığında, radar yanıltan elektronik harp yöntemleri veya zararlı kod barındıran yazılımlar veya sistemin davranışını değiştiren algoritmalar da maskirovka olarak sınıflandırılabilir. Mesela, belirli koşullar oluştuğunda veya belirli bir tarihte aktif hale gelen (zaman ayarlı) virüsler…

° Aktörler

ABD ve başka ülkelerde olduğu gibi Rusya Federasyonu'nda da bilgi harbi aktörleri çeşitlidir. Bazıları Sovyet döneminden miras alınmış, bazıları yeni oluşturulmuştur ki bu yeniler içerisinde özel şirket ve sivil topluluk kisvesi altında olanlar dikkat çekmektedir.

Sovyet döneminin efsanevi istihbarat teşkilatı KGB bünyesindeki sekizinci haberleşme baş direktörlüğü ve on altıncı elektronik istihbarat direktörlüğü, 1991'de Sovyetler yıkıldıktan sonra Devlet Haberleşme ve Bilgi Federal Ajansı (FAPSI) olarak yeniden yapılandırıldı. Geçiş dönemi Rusya'sında birçok kurumun içine düştüğü çürümeden payını alan FAPSI 2003'te lağvedildi.

Özel amaçlı haberleşme, kripto güvenliği, teknik istihbarat, istihbarata karşı koyma, şifre çözme, devletin haberleşme ve bilgi güvenliğinin yanı sıra bankacılık ve finans sektörünün bilgi güvenliği ve yabancı ülkelerin haberleşmesinin izlenmesi FAPSI'nin sorumluluk alanı içerisindeydi. (ABD'nin Ulusal Güvenlik Ajansı NSA benzeri ve ötesi…) Rusya'da internet kullanımını denetim altına almak isteyen FAPSI bu amaçla internet servis sağlayıcısı RELCOM'u satın aldı ve bir süre yönetti. Faal olduğu dönemde FAPSI'nin onaylamadığı bir kripto sistemini kullanmak suçtu Rusya'da.

Lağvedildikten sonra, FAPSI'nin ilgilendiği konular Rusya Federal Koruma Servisi (FSO), Federal Güvenlik Servisi (FSB), Yabancı İstihbarat Servisi (SVR) ve (Askeri Yabancı) Merkezi İstihbarat Direktörlüğü (GRU) arasında paylaştırıldı.

Federal Koruma Servisi (FSO) devletin üst düzey (telli, telsiz, uydu, internet) haberleşmesini gözetir.

KGB'nin dönüştüğü Federal Güvenlik Servisi (FSB) bir devletin istihbarat teşkilatının ilgileneceği tüm görevleri üstlenir ki bunların içerisinde sinyal istihbaratı da (SIGINT) bulunmaktadır. Bu amaçla geliştirilen SORM sistemi vasıtasıyla ve ISS/telekom operatörleri yardımıyla FSB'nin internet ve telefon trafiğini ve içeriğini izlediği veya dinlediği iddia edilmektedir. Bu vasıtasıyla dinlenen veya izlenen hedefler ile ilgili olarak operatörlere bilgi verilmemekte, izleme otomatik olarak gerçekleşmektedir.

> SORM, Sovyet döneminin son yıllarında -o zaman için gündemde olan- telefon haberleşmesinin izlenmesi için geliştirilmiş bir sistemdi. İngilizceye, System for Operative Investigative Activities olarak tercüme edilebilir ama harflerin uyumu bakımından System of Operative Research Measures veya System of Operational Research Measures diye yazılır, genellikle. *(Burada sözü edilen Operational Research'ün bir matematik disiplini olan Operational Research veya Operations Research - OR ile alakası yoktur.)* SORM, ilk haliyle sadece telefon haberleşmesinin

> izlenmesi için geliştirilmiş olsa da şimdilerde internet, VoIP dahil tüm haberleşmenin izlenmesi ve gerektiğinde üç yıl boyunca depolanmasını mümkün kılacak yetkinliğe erişmiştir. SORM donanım ve yazılımı tüm telefon ve mobil telefon operatörleri ve internet servis sağlayıcılarına yerleştirilmiştir. Mevzuat gereği, haberleşmeyi izlemek için her ne kadar mahkeme emri gerekse de, yine mevzuat gereği FSB bu emri göstermeye mecbur değildir; dolayısıyla kimse FSB'ye bunu sormaya teşebbüs dahi etmez. Tam bir Catch-22 durumu!.. *(Catch-22'yi merak edenlere tavsiyem; Joseph Heller'in muhteşem romanını okusunlar. Zihin kışkırtıcı hiciv diye tanımlanır ama benim için zihin açıcıydı. Her halükârda çok eğlenceli…)*

Yabancı istihbarattan sorumlu SVR, aynı zamanda stratejik sinyal istihbaratına ilaveten telsiz haberleşmesi ve askeri ve ticari uydu sistemlerinden istihbarat toplar ve değerlendirir.

Askeri istihbaratın sorumlusu GRU, tüm servisler içerisinde en eski ve tecrübeli olanıdır.

> Tarihçesi 1918'e, Troçki'ye dek uzanır. Benim için muammadır: elinde GRU gibi bir teşkilat varken nasıl oldu da yenildi Stalin'e?

Rusya içerisindeki askeri misyonlar ve yurt dışındaki askeri tesisler ve operasyonların yanı sıra, askeri haberleşme istihbaratı (COMINT), elektronik istihbarat (ELINT), görüntü istihbaratı (IMINT) ve açık kaynak istihbaratı (OSINT) ile ilgilenir.

Görüldüğü gibi, Rusya Federasyonu'nda istihbarat ve bilgi harbi faaliyeti birçok kurum arasında paylaşılmaktadır.

> FAPSI 2003'te lağvedildiğinde 54.000 kişilik bir teşkilattı. 2003'teki yeniden yapılanmada FSO'nun 20.000, FSB'nin 270.000, GRU'nun 27.000, SVR'nin 12.000 personeli olduğu ve geçen süre içerisinde bu sayıların çok daha artmış olacağı göz önüne alındığında ne denli devasa bir istihbarat ve bilgi harbi teşkilatından söz edildiği anlaşılabilir.
>
> Resmi kurumlara ilaveten, muhtemelen devlet denetiminde, gençlik örgütü veya illegal örgüt kisvesi altında -gerektiğinde inkâr edilebilecek- oluşumlar da mevcuttur. Mesela, 2005'te 120.000 üyesi olan NASHI gençlik örgütü bunların en bilinenidir. Devletin "iç ve dış düşmanları"na karşı birçok siber saldırının sorumlusunun bu örgüt olduğu iddia edilir.
>
> 2008'deki Gürcistan krizinde Gürcistan web sitelerine yönelik siber saldırının askeri harekât ile birlikte yürütülmesi; bu saldırının koordine edildiği stopgeorgia.ru adlı web sitesini ve daha başkalarını barındıran steadyhost.ru sunucusunun coğrafi adresinin bir askeri araştırma kuruluşu ve GRU ile aynı binada olması ilginç rastlantılardır. Bu saldırıların birçoğu hükümeti yıpratmaya yönelik propaganda saldırılarıydı. Cumhurbaşkanı Mikhail Saakashvili'yi Adolf Hitler'e benzeten fotoğraflar yüklüyorlardı Cumhurbaşkanı'nın kişisel sitesine. (Bu yüzden, bir devlet adamını Hitler'e benzeten fotoğraf gördüğümde şüphe ile yaklaşırım.)

Rusya'nın bilgi harbi esaslarının belirlenmesinde önemli rol sahibi olanların başında Amiral Vladmir Pirumov gelmektedir. Sovyet donanmasında kruvazör komutanlığı dahil çeşitli kademelerde görev yapan 1926 doğumlu Vladimir Pirumov, 1974-1985 arası

Deniz Kuvvetleri Kurmay Başkanlığı görevini yürüttü. 1985-98 arasında Hava Kuvvetleri Akademisi ve Genelkurmay Akademisi'nde görev yapan Pirumov, Rusya Federasyonu Güvenlik Konseyi bünyesinde Bilim Konseyi Başkanlığı, Doğal Bilimler Akademisi Başkanlığı, Jeopolitik ve Güvenlik Akademisi Başkanlığı, Devlet Başkanı Bilim Danışmanlığı görevlerini üstlendi. Bu görevlerini yürütürken elektronik harp ve bilgi harbi üzerine çalışmalar yapan Pirumov Rusya'nın modern bilgi harbi doktrininin esaslarını ortaya koymuştur.

ÇİN HALK CUMHURİYETİ

Çin Halk Cumhuriyeti, 1995'ten itibaren savunma yapılanmasında, bilgi harbinde üstünlük sağlamayı hedeflemektedir. Çin bilgi harbi esaslarının belirlenmesinde önemli rol üstlenmiş olan General Dai Qingmin şöyle tanımlar bilgi harbini: Bilgi ortamının muharebe alanı, bilgi ve bilgi sistemlerinin harekât hedefi, elektronik harp ve bilgisayar ağı harbinin esas muharebe unsurları olduğu harp şekli. Dahası, bilgi kontrolü için verilen mücadelenin gelecek harplerin odağını oluşturacağını iddia eder.

Çinliler için bilgi harbi -jeopolitik duruma göre- üç amaçla kullanılabilir: bir muharebe aracı olarak, savaşmadan zafer kazanma aracı olarak, yeni askeri teoriler geliştirerek istikrarı sağlama aracı olarak. Açıkta ulaşılabilen yayımlanmış bir doküman olmasa da, bilgi üstünlüğünü (Information Superiority - IS) ele geçirmeyi hedef olarak belirten Çin bilgi harbi doktrininin temel unsurları olarak şunlar sıralanmaktadır: 1) Harekât Güvenliği, 2) Yanıltma, 3) Psikolojik Harp, 4) Fiziki İmha, 5) Elektronik Harp, 6) Bilgisayar Ağı Harbi. Bunların içerisinde elektronik harp ile bilgisayar ağı harbi, Entegre Ağ ve Elektronik Harp (Integrated Network-Electronic Warfare - INEW) kavramı olarak öne çıkmaktadır. Bu entegre elektronik harp ve bilgisayar ağı harbi kavramı Çin Bilgi Harbi doktrininin belirlenmesinde önemli rol sahibi General Dai tarafından ortaya konulmuştur. Çinliler, kendi Bilgi Harbi doktrinlerini oluşturmada genellikle açık ortamda yayınlanmış olan ABD Bilgi Harekâtı doktrini ve ilgili birçok çalışmadan yararlanmışlar, ancak kendi koşullarına uyarlamışlardır.

> Hatırlamak için: Ruslarınki teknik ve psikolojik iki temel boyutluydu, Amerikalılarınki ise -doktrinin kaleme alındığı döneme göre- OPSEC, MILDEC, PSYOP, EW, CNO, CI, IA, CMO, PA, fiziki emniyet, fiziki imha ve benzeri bir dolu unsurdan oluşuyordu.
>
> Çin bilgi harbi doktrini, Ruslarınki gibi sadece iki boyutlu değil daha ziyade Amerikalılarınki gibi çok boyutludur. Çinli uzmanlarca incelenen ve örnek alınan ABD doktrinlerinin oldukça kapsamlı ve ayrıntılı olmasının rolü vardır bunda. Öyle ki, önceleri Bilgi Harbi (Information Warfare - IW) söz konusu iken, bilahare Bilgi Harekâtı (Information Operations - IO), nihayetinde Ağ Harbi (Network Warfare) kavramlarını öne çıkarmışlardır.

° Stratagemler

Hile demek olan stratagem, daha ziyade savaş hilesi anlamında kullanılır.

Milattan beş yüz yıl önce yaşamış olduğu tahmin edilen bir Çinli general ve savaş teorisyeni Sun Tzu tarafından tanımlanan otuz altı stratagem, geleneksel Uzak Doğu savaş hileleri olsalar da günümüzde hala geçerliliklerini sürdürmektedir. Daha sonra bazı Romalı ve Makedon generaller de savaş hilelerini kitap halinde derlemişlerdir.

Batı'nın üstün savaş teknolojisi ile baş edebilmek için modern teknolojiyi geleneksel savaş hileleri ile birleştirerek güçlerini artırabileceklerini fark eden Çinliler özellikle bilgi harbi söz konusu olduğunda bu stratagemlerin pratik faydalar sağladığını gördüler. Çinlilerin geleneksel savaş felsefesi ile hayli uyumlu olan bilgi harbi yöntemleri Halkın Kurtuluş Ordusu (People's Liberation Army - PLA) tarafından da benimsenmekte ve geliştirilerek uygulanmaktadır. Çinli liderler ve savaş teorisyenleri batının teknolojik üstünlüğüne karşı bu stratagemlerin yararına inanmaktadırlar.

Uzak doğu savaş sanatının en belirgin özelliği zayıfın kuvvetliyi yenmesinin yollarını gösteren savaş hileleri, stratagemlerdir. Savaş Sanatı adıyla bilinen kitapta Sun Tzu tarafından ortaya konulmuş olan stratagemlerin birçoğu esasında günümüz bilgi harbi becerilerinin veciz ifadeleridir.

Staratagemlerin modern bilgi harbine uyarlanmasına birkaç örnek vermek gerekirse:

1. "Açıkta gizle." Göz önünde olanı görmek zordur; gerçek niyetini rutin, gündelik aktivitenin arasına gizle. Steganografi uygula. *Her zaman kullanılan e-posta veya internet siteleri üzerinden zararlı yazılım bulaştır.*

2. "Zhao'yu almak için Wei'yi kuşat." Kuvvetli olduğu yerde düşmana saldırmak yerine onun için daha kıymetli olan başka bir yere saldır. *Sana daha çok zarar verecek askeri bir saldırı yerine internet üzerinden düşmanın değerli kurumlarına saldır.*

3. "Ödünç bıçakla öldür." Başkasından yararlan, onun imkânlarını kullan. *Zararlı yazılımı başka bir ülke üzerinden gönder.*

4. "Düşman yorulurken sen dinlen." Düşmanın kendini yormasını sağla ve sen gücünü muhafaza et. *Çok sayıda önemsiz saldırı ile düşmanın savunma sistemini ve personelini meşgul ederken asıl önemli saldırıyı sona sakla.*

Mao Zedung, bu stratagemden yola çıkarak halk savaşının ilkelerini şöyle koymuştur:

düşman gelirken kaçarız
düşman dinlenirken vururuz
düşman yorulduğunda savaşırız
düşman kaçarken kovalarız

5. "Yanan evi yağmala." Ülke iç meselelerle, çatışmalarla meşgulken dış tehditlerle baş edemez. *Bilgisayar korsanlarını (hacker) çeşitli kimliklerle saldıracağın yere (ülkeye, tesise, kuruma) yerleştir ve saldırı başlat; karışıklık baş gösterdiğinde bilgi sistemlerinden bilgi sızdır veya bilgi sistemlerine zarar ver.*

Sun Tzu'nun stratagemleri, amaç askeri üstünlük elde etmek olduğunda ne denli geçerliyse, amaç bilgi üstünlüğü elde etmek olduğunda da geçerlidirler.

° INEW

General Dai Qingmin tarafından geliştirilen Entegre Ağ ve Elektronik Harp (Integrated Network-Electronic Warfare - INEW) kavramı çerçevesinde Halkın Kurtuluş Ordusu'nun elektronik harp imkânları ile yaygın bilgisayar ağı harbi imkânları birlikte kullanılmaktadır.

> Anlaşılan o ki General Dai, Batı'da, özellikle Amerikan elektronik harp çevrelerinde süregelen tartışmayı pek umursamamış, belki de bu tartışmanın yarattığı sinerjiden yaralanmıştır. Amerikalı elektronik harp uzmanları, bilgisayar ağı harekâtını (CNO) elektronik harbin bir alt dalı olarak değerlendirirken yeni nesil bilgisayarcılar daha ziyade sayısal ortamda yürütülen bilgisayar ağı harekâtının elektromanyetik spektrumda yürütülen elektronik harbin parçası olmadığı tezini savunmaktadırlar. Amerikalılar böyle tartışa dursun, Çinliler bu iki kavramı birlikte kullanarak üstünlük sağlamanın avantajlarını değerlendirmektedirler.

Elektronik harp ile bilgisayar ağı harbini entegre etmekle muharebe alanında bilgi üstünlüğünü ele geçirmek mümkün olabilir. Elektronik harp becerisiyle düşmanın bilgiye ulaşma ve aktarma imkânı engellenir; bilgisayar ağı harbi becerisiyle ise bilgiyi işleme ve karar verme yetisi zayıflatılır. Birlikte kullanıldığında Bilgi Harbinin (IW) nihai hedefine ulaşılır; bilgi sisteminin bilgiyi elde etme, aktarma, işleme ve kullanma süreci sekteye uğratılır.

> İlginçtir; silah sistemleri veya istihbarat bilgi ağı yerine Çinliler daha zayıf koruma tedbirleri alınan lojistik bilgi ağına saldırmayı yeğlemektedirler. Genellikle tasnif dışı ve sivil ağlarla bağlantılı olan lojistik bilgi sistemi Çinliler için çok daha kolay ve maliyet etkin bir hedef teşkil etmektedir. Biliyorlar ki Amerikalılar için Pasifik aşırı bir harekât söz konusu olacaksa lojistik hayati önem taşıyacaktır. (İkinci Dünya Harbi'nde Alman denizaltılarının hedefinde lojistik konvoylarının olduğu düşünüldüğünde bu yaklaşım daha anlaşılabilir olmaktadır.)

Bilgisayar ağı harbini gerçekleştirmek için birtakım kaynaklara ihtiyaç vardır: bilgisayar, bağlantı (internet), siber saldırı araçları (genellikle yazılım) ve siber savaşçılar (korsanlar, hackers). Bunların ilk üçü elde edilebilir ama dördüncüsünü yetiştirmek gerekir.

> Kremlin'in hoşgörüsü (kontrolü) altında olduklarına inanılan Rusya'daki NASHI ve benzeri gruplar gibi Beijing'in hoşgörüsü (kontrolü) altında olduklarına inanılan çok sayıda "yurtsever" siber savaşçı vardır Çin'de.

Barışta ve savaşta ihtiyacı karşılayabilecek bir askeri/sivil ortak haberleşme sistemi kullanılan Çin'de haberleşme sektöründe çalışan binlerce mühendis ve teknisyenden oluşan yedek kuvvetler savaş halinde derhal görev üstlenebilecek ve en son teknolojiyi uygulayabilecek şekilde eğitimli ve hazır durumdadırlar.

> Maliyet etkin olması için Amerikalıların uygulamaya koydukları COTS yaklaşımının izleri sezilmektedir burada. Askeri olanlara nazaran çok daha gelişmiş olan sivil haberleşme sistemlerini kullanmak ve bu sistemlerde eğitilmiş, tecrübeli personelden

savaş halinde de yararlanmak, maliyet etkin olmanın ötesinde, hayli pratik bir yaklaşım olarak dikkat çekmektedir.

Haberleşme ve bilgi teknolojilerinde eğitimli tecrübeli insan gücü, bilgi harbi/bilgi harekâtı uygulamaları söz konusu olduğunda derhal kullanılabilecek yedek kuvvetler olarak değerlendirilmektedir. Halkın Kurtuluş Ordusu (PLA) bünyesinde bir askeri bilgi harbi görev gücü oluşturmaya gerek bulunmamaktadır. Askeri beceri daha ziyade Elektronik Harp (EW) alanında kullanılır; düşmanın bilgi sistemlerine (jamming, EMP, sabotaj, vs) saldırılar düzenlenirken sivil yedek kuvvetler ile de bilgisayar ağı harbi yürütülür. Böylece Entegre Ağ-Elektronik Harp (INEW) gerçekleştirilmiş olur.

Savaş gücü olarak büyük ölçekte sivil unsurlardan yararlanmak Mao'nun "halk savaşı" kavramıyla uyumludur.

Bu durum, teknolojik olarak nispeten geri kalmış olan askeri donanım zafiyetini gidermeye yardımcı olur.

Ayrıca,

-- Bilgi işlem yetisi ve kapasitesini artırmak;

-- Haberleşme yetisi ve hacmini artırmak;

-- Sistemin güvenilirliğini artırmak;

-- Keşif yetisini artırmak gerekmektedir.

Bilgi harbinde yararlanılabilecek yedek kuvvetlerin sayısının bir buçuk milyonun epey üzerinde olduğu tahmin edilmektedir. Hemen hepsi Beijing kontrolündeki bu yedek kuvvetler büyük şehirlerde daha alt birimler halinde organize olmuşlardır.

Büyüklüğü anlamak için Türkiye nüfusuna oranladığımızda seksen bin kişiden meydana gelen bir yapı söz konusu.

Özellikle bilgisayar ağları üzerinden yürütülen bilgi harbi Çinliler için birçok olanaklar sunmaktadır:

-- Maliyet etkindir; sınırlı imkânlarla etkili sonuçlar alınabilir;

-- Hayli uzağa erişmek mümkündür;

-- Fiziksel temas gerekmemektedir;

-- İnkâr edilebilir.

Çinliler, bilgisayar ağı üzerinden yürütülen harbin yıkıcı, imha edici değil, paralize edici ve sonuç verici olmasını önemsemektedirler. Amaç yenmek değil, düşman için savaşın maliyetini artırmak veya düşmanın savaşma azmini kırmaktır.

Mao Zedung demiştir ki "Zafere ulaşmak için düşmanı mümkün olduğunca kör ve sağır etmek ve kafalarını karıştırarak komutanların dikkatini dağıtmak gerekir." İşte, bilgi harbinin amacı ve yöntemlerini özetleyen bu cümle Halkın Kurtuluş Ordusu'nun da temel felsefesiydi.

Modern komuta, kontrol, haberleşme, bilgisayar ve istihbarat (C^4I) sistemlerinin bilgisayar ağı üzerinde olması düşmanın kör, sağır hatta paralize edilmesine ve komuta bütünlüğünün çözülmesine imkân tanımaktadır. Ayrıca, konvansiyonel harbe başvurmadan düşmana zarar vermek mümkün olmaktadır.

Çinliler, savaşın erken aşamalarında saldırmanın düşman için çok daha fazla zarar verici olduğuna inanırlar ve bu sebeple bilgisayar ağı harbini bir kuvvet çarpanı olarak değil, henüz savaş başlamadan önemli merkezlere saldırarak düşmanı şaşırtmayı hatta paralize etmeyi mümkün kılan bir temel harp vasıtası olarak değerlendirirler. Bu değerlendirme onların temel savaş felsefeleri ile de uyumludur.

ABD başta olmak üzere batılı güçlerin bilgisayar ağına ve bilgi sistemlerine -Çin'e nazaran- çok daha fazla bağımlı olması Çin için avantaj yaratmaktadır. Ancak, Çin C^4I sistemlerinin de bilgisayarlara gittikçe bağımlı hale gelmesi ile bu avantaj zamanla nötralize olacaktır.

NE ÖĞRENDİM?

Amerika Birleşik Devletleri, Rusya Federasyonu ve Çin Halk Cumhuriyeti'nin bilgi harbi yaklaşımları kıyaslandığında ABD'nin bu konuda en kapsamlı çalışmaları yaptığı ve açıkça, ayrıntılı şekilde dokümante etmiş olduğu görülmektedir. Bu sayede, hem müttefik, hem de hasım cenahta birçok ülke kendi bilgi harbi doktrinini ortaya çıkarma, geliştirme ve güncelleme imkânı bulmaktadır. ABD Bilgi Harekâtı (IO) doktrini tüm unsurları, yöntemleri ve terminolojisi ile bilgi harbi veya bilgi harekâtı ile ilgilenenler için önemli ve değerli kaynaktır.

Rusya Federasyonu, daha ziyade kendine özgü, geçmişten gelen gizli ve baskıcı bir yaklaşımı tercih etmektedir.

Çin Halk Cumhuriyeti, Bilgi Harbi doktrinini geliştirmede ABD doktrininden önemli ölçüde esinlenmekle birlikte geleneksel harp hilelerinden de yararlanmakta, dolayısıyla oldukça özgün bir yaklaşım koymaktadır ortaya. *(Ancak, bireysel hak ve özgürlüklerin kollanmasında Amerikalıları örnek aldıkları iddia edilemez.)*

Amerikalılar, bilgi harbinin esaslarını belirlerken kendi vatandaşlarının bireysel hak ve hürriyetini kollayıcı önlemleri yasal güvence altına almışlardır. (Özel haberleşme ve kişisel bilginin elde edilmesine yönelik uygulamada aksi örnekler olmasına rağmen yasal düzenleme bu güvenceyi sağlamaktadır.) Altını çizerek belirtmek gerekir ki her ne sebeple olursa olsun, kendi vatandaşlarına yönelik psikolojik harekât yürütmeyi ciddi suç olarak görmektedirler.

Amerikalılar için bilgi harbi, askeri hedeflere ulaşmada yararlanabilecekleri bir harekât şeklidir; dolayısıyla, esasları ve uygulama yöntemleri bu amaca uygun olarak, askerlerin uygulayacağı tarzda tanımlanmıştır. Halbuki Ruslar ve Çinliler -askeri hedef söz konusu olsa dahi- bilgi harbinin tüm ülke sathında ve sivil unsurların desteğiyle yürütülmesinin

yararı ve gereğine inanmaktadırlar. (Daha ziyade müdafaa durumunda olanların benimsediği bir tarzdır bu.)

Ruslar ve Çinliler, müdafaa harbinde tarihten gelen tecrübelerini modern çağın teknolojisi ve imkânları ile harmanlayarak bilgi harbinde kendi tarzlarını ortaya çıkarabilmişlerdir ki bizim de yabancısı olmadığımız bir tecrübedir bu. Biz de yeri geldiğinde müdafaa harbini tüm vatan sathına yayarak zafere ulaştık.

> Hattı müdafaa yoktur, sathı müdafaa vardır ve o satıh bütün vatandır.
>
> Mustafa Kemal Atatürk 1921

Çinlilerin yaptığı gibi eldeki teknolojiyi geleneksel yöntemlerle harmanlamanın yanı sıra Rusların yaptığı gibi meselenin esasına, teorik altyapıya ve mutlaka matematiğe önem ve değer vermeliyiz. Sathı müdafaa ancak bu şekilde sağlanabilir.

> Popüleriteden, güncel eğilimlerden, izlenimlerden veya haberlerden yola çıkarak siber savunma sistemlerine veya teknolojilerine ilgi duymak, biraz yatırım yapmak iyidir ama altyapı olmadıktan sonra buza yazılmış koddan ileri gitmez. Altyapı, ancak sathı müdafaa ile yaratılabilir.
>
> Birinci bölümün sonunda, "Ne Yapmalı(yız)?" sorusuna cevap ararken değindiğim, toplumdaki matematik bilincinin ve yetisinin artırılması bir bakıma "sathı müdafaa"nın modern bilgi çağına yansıtılması demektir. Kendi içine dönük kurumlarda, kapalı kapılar ardında üretilen çözümlerle geleceğin bilgi harbi dünyasında söz sahibi olunamaz.

İnternet, sosyal medya, televizyon ve yazılı basın sayesinde küresel bilgi ortamı ile sürekli ilişki içerisinde olduğumuz çağda bilgi harbi -geleneksel anlamda harbin ötesinde- gündelik hayatın bir parçası olarak değerlendirilmesi gereken bir olgu haline gelmiştir. Kaçamayız, engelleyemeyiz… Gerek de yok.

> Son olarak şu önemli uyarıyı yapmadan geçmek doğru olmaz düşüncesindeyim; hatta, tüm bu derlemeyi bu uyarının ışığında değerlendirmekte yarar görüyorum:
>
> Popüler komplo teorilerinde birçok olay genellikle ABD, Rusya, Çin başta olmak üzere, zaman zaman İsrail, Almanya, İngiltere, Fransa'nın da adlarının zikredildiği "birtakım" güçlerin bilgi harekâtları (operasyonları) olarak izah edilir. Aslında izah olmaktan çok uzak, hani yolda yürürken başına saksı düşen birinin Newton'u suçlaması gibi absürt bir yaklaşımdır bu. Tabii, demek değil ki adı geçen ülkeler diğerlerine yönelik bilgi harekâtı uygulamıyorlar. Bilgi harbi çerçevesinde değerlendirilebilecek böylesi uygulamalar vardır mutlaka. Ancak, bu konuda güçlü ülkelerin bilgi harekâtı doktrinleri bile küçük grupları hatta bireyleri dahi bir nevi bilgi harbi uygulayıcısı (tehdit) olarak görüyorken, her aktiviteyi mutlaka hükümetler veya askeri otoritelerle ilişkilendirmek pek doğru olmaz. Ne paranoya, ne de umursamazlık hali; önemli olan, dengeyi, akılcılığı koruyabilmektir. Çoğu kez bilinçsizce, bazen de bilinçlice, sloganvari, "Bilgi Harekâtı" veya "Bilgi Harbi" olarak değerlendirilen birtakım uygulamaları, günümüz teknolojisinin imkânlarını göz önüne alarak, sağlıklı ve akıllıca değerlendirilmek daha doğru olur. Sloganlar meseleyi soyutlaştırır, analizi engeller, değerlendirmeyi zayıflatır, yanlış sonuca yönlendirir. Tıpkı, "Trafik Canavarı" gibi... Tıpkı çözülmesi gereken ve iyi analiz edildiğinde, doğru değerlendirildiğinde, akıllıca

> bir yaklaşımla çözülebilecek somut bir mesele varken ortada, bunları bir kenara bırakıp, popüler bir sloganla soyutlaştırarak, hatta karikatürize ederek çözümden uzaklaşmak gibi… Nedense, hepimiz çok meyilliyiz buna.

Yapmamız gereken: (şikâyet etmek ve başkalarını suçlamaktan ziyade) paniklememek, bilgili olmak, farkında olmak, bilinçli davranmak; kendimizi, yakın çevremizi ve dünyayı iyi değerlendirmek; hedef belirlemek; kendimizle, çevremizle ve dünya ile uyumlu, akıllıca çözümler geliştirmek; amaç ve uygulamada istikrarlı olmak.

> Üçüncü harbin matematikçilerin arenasında yürütüleceğinden bahisle, "Ne?" ve "Nasıl?" sorularının ötesinde "Niçin?", hatta "Ya değilse?" sorularını sormayı içselleştiremeyen toplumların kaybedeceklerini söylemiştim Birinci Bölümde. Ancak altını bilhassa çizmeliyim ki bu harp, belirli bir mekânda, belirli bir sürede yürütülen bir harp olmayacaktır. Mekân ve zamanda yayılmış halde, tüm dünyada, tüm zamanlarda yürütülen bu harbi kaybeden, kaybettiğini anlamayacaktır bile. Tıpkı yavaşça ısıtılan suyun içerisindeki kurbağa gibi… Harp, çoktan başlamış ve halen sürmektedir.

Bu sayfa bilhassa boş bırakılmıştır.

İKİNCİ BÖLÜME EK

1996 - 2012 yılları arasında yayınlanan dokümanlar temel alınarak ABD Bilgi Harekâtı (IO) doktrinin gelişimi gözden geçirilmiştir. Milli Askeri Stratejiyi (National Military Strategy) destekleyen ve esas olarak Kara Kuvvetleri (Army) için bilgi harekâtının temellerini açıklayan 1996 tarihli sahra talimnamesi FM 100-6 Information Operations adlı doküman, o gün itibariyle Savunma Bakanlığının (DOD) Komuta Kontrol Harbi (C^2W) politikasını yansıtmakta, hatta ötesine geçmektedir. ABD Bilgi Harekâtı (IO) doktrini ilk kez 2003 yılında, tüm kuvvetleri kapsayan FM 3-13 ve parantez içerisinde (100-6) başlığıyla yayınlanmış; bilahare, tüm kuvvetler için ortak yayın JP 3-13 şeklinde yayınlanmaya devam etmiştir. Bugün (2013) itibariyle JP 3-13 dokümanın sonuncusu 27 Kasım 2012 tarihlidir.

- . -

1996 - ABD IO DOKTRİNİ

ABD ordusunun 1996 tarihli sahra talimnamesi FM 100-6 Information Operations (Bilgi Harekâtı) dokümanı bilgi harekâtının kapsamını tanımlıyor ve şunları belirtiyor, özet olarak:

-- Harekât üzerinde taktik ve stratejik seviyede önemli bir etki unsuru olarak tanımlar bilgiyi.

-- Komutanların bilgiyi, bilgi sistemlerini ve etkilerini askeri harekâtın tümü ile bütünleştirmesini mümkün kılar. Böylesi bir bütünleşme, muharebe unsurlarının olanaklarını ve gücünü artırır.

-- Muharebenin etkinliğini artırıcı sinerji geliştirilmesine yardımcı olur.

Ama hepsinden önemlisi, bilgi çağına geçişi mümkün kılan bir üst* dokümandır. Artık, bilgi çağı ile uyumlu olmak, onun gereklerini yerine getirmek önemli bir mecburiyet olarak kabul görülmektedir askeri çevrelerde. Bu, kayda değer bir kilometre taşıdır.

> * Söz konusu FM 100-6 dokümanı, kendi içerisinde "capstone document" olarak tanımlanmaktadır ki bu tür dokümanlar genellikle önemli, sistemik bir değişikliğe adım atmadan evvel, geçişin sorunsuz gerçekleştirilmesi amacıyla yayınlanan bir nevi uyum ve eşgüdüm dokümanlarıdır. Sadece bu niteleme bile ABD askeri otoritesinin bu geçişi ne denli yapısal bir değişiklik olarak değerlendirdiğini ve bilgi çağı ile uyum sağlamaya ne kadar önem verdiğini göstermeye yeter.

Ordu yeni bir çağı karşılamaya hazır olmalı. Bilgi çağı olarak adlandırılan bu yeni çağ, beraberinde eşsiz fırsatlarla birlikte zorlu bir meydan okuma sunmaktadır. Bilgi harekâtı vasıtasıyla bilgi çağı ve bilgi tüm veçhesiyle askeri harekâta destek olmaktadır.

Tüm harplerde uygulanmakta olan bilgi harekâtı, en basit haliyle, bilgiyi elde etmek, onu dost kuvvetlerin yararına kullanmak ve düşmanın yararlanmasını engellemek şeklinde tanımlanabilir.

° Harekât Ortamı

Bilgi Çağında komutanlar ve kurmayları gittikçe karmaşıklaşan harekât ortamı ile karşı karşıya kalmaktadırlar. Günümüzün Küresel Bilgi Ortamı (GIE), komutanın ulaşabileceğinin, müdahale edebileceğinin ötesinde bilgi sistemlerini ve süreçleri kapsamaktadır ki bunların içerisinde Askeri Bilgi Ortamının (MIE) yanı sıra medya, uluslararası kuruluşlar, hatta kişiler vardır.

Hızlı teknolojik gelişme sayesinde küresel iletişimin yaygınlaşması ile jeopolitik ortam oldukça karmaşık hale gelebilmektedir. Olaylar karşısında toplulukların tepkileri çok daha çabuk gelişmekte, öfkeler ateşlenmekte, derine itilmiş duygular açığa çıkmakta, topluluklar menfaatlerini öne çıkarmakta; bu durum çoğu zaman zararsız , bazen yararlı olmakla birlikte, kimi zaman kaos, karışıklık, hatta çatışmaların tetiklenmesine sebep olabilmektedir. Böylesi çatışmalar geleneksel muharebe alanının ötesine geçmekte; espiyonaj, sabotaj, terör, ekonomik mücadele veya kamuoyunun algısını şekillendirecek faaliyetleri de içermektedir.

(FM 100-6 dokümanının yayınlandığı 1996 yılı itibariyle) Modern bilgi teknolojisinin önde gelen uygulayıcısı olan Amerika Birleşik Devletleri'nde ekonomik ve sosyal hayat, yerel ve federal kurumlar hızlı ve güvenilir bilgi akışına bağımlıdır. Amerika aynı zamanda, çokuluslu ticaret, medya ve eğlence endüstrisi vasıtasıyla tüm dünyayı etkilemekte; kendisi de diğer ülkelerden etkilenmektedir.

°° Küresel ve Askeri Bilgi Altyapıları ve Bilgi Ortamları

Dünya üzerinde yaygın iletişim ağı -gayri resmi ve resmi- bilimsel, endüstriyel, kamusal, askeri, ticari kuruluşları ve medyayı içermektedir. Birbiriyle oldukça sıkı ve karmaşık ilişki içerisinde olan bilgi altyapıları tüm dünyada bireyleri, cemaatleri, ulusları içine alan ve herkesin bilgiye hızla ulaşmasını sağlayan bir şebeke şeklinde evrimleşmiştir.

> 1970'ten sonra ARPANET, 1985'ten sonra NSFNET belirli çevrelerce kullanılıyordu. 1990'ların başından itibaren bu net'ler INTERNET olarak herkesin kullanımına açık, bir şebekeye dönüştü. [Tam burada, J.C.R. (Lick) Licklider'i saygıyla selamlıyorum.] FM 100-6 numaralı doktrinin yayınlandığı 1996 yılında internet henüz -şimdilerde olduğu gibi- çok yaygın kullanılıyor değildi ama yine de söz konusu doktrin bu gelişmeyi öngörür şekilde kaleme alınmıştır.

Askeri ve sivil bilgi şebekelerinin birleşmesiyle meydana gelen Küresel Bilgi Altyapısı (GII), dünya üzerinde kişileri, kurumları elektronik olarak birbirine bağlamaktadır. Benzer şekilde, Ulusal Bilgi Altyapısı (NII), Savunma Bilgi Altyapısı (DII) gibi bilgi altyapıları da söz konusudur.

Küresel Bilgi Altyapısı (GII), iletişim mekanizmaları, bilgi gereçleri, içerik ve insanlardan oluşan ve haberleşme şebekeleri, bilgisayarlar, veritabanları ve kişisel

elektronik cihazların birbiriyle bağlanmasıyla vücut bulan, dünya çapında, kesintisiz ve dinamik bir bilgi ağıdır.

Küresel Bilgi Altyapısı, bilgiyi işlemeye, depolamaya, iletmeye yarayan temel gereçler ve çevre birimlerini içermenin yanı sıra, dünya çapında organizasyonları, kişileri, askeri ve sivil bilgi şebekelerini birbirine bağlar ve bünyesindeki bilgiye küresel erişim ve kullanım imkânı sağlar.

Ulusal Bilgi Altyapısı (NII), tüm ülkeyi kapsayacak ölçekte oluşturulmuş bilgi altyapısıdır. Tüm ülkelerin Ulusal Bilgi Altyapılarının birleşimiyle Küresel Bilgi Altyapısı meydana gelir.

Kamusal ve özel, dar bant, geniş bant şebekeler; telsiz, uydu ve karasal yayın şebekeleri; bu şebekeler üzerinde akan içerik (ses, görüntü, analog veya sayısal bilgi vb); bu altyapıya erişimi sağlayan gereçler, bilgisayarlar, depolama birimleri; bilgiyi üreten, işleyen ve yöneten bireyler meydana getirmektedir Ulusal Bilgi Altyapısını.

Savunma Bilgi Altyapısı (DII), Savunma Bakanlığı (DoD) görev destek, komuta kontrol (C^2) ve istihbarat bilgisayarlarını ve kullanıcıları birbirine bağlar

Küresel Bilgi Altyapısı (GII), Ulusal Bilgi Altyapısı (NII) ve Savunma Bilgi Altyapısı (DII), birbiri ile ilişkili bilgisayar şebekeleri ve bireysel cihazlar, bilgisayarlar vasıtasıyla bireyler muazzam miktarda bilgiye ulaşabilme imkânına sahiptir.

Küresel Bilgi Ortamı (GIE): Tüm bu bağlantıları mümkün kılan altyapılar ile devlet kurumları, politik liderler, uluslararası örgütler, ortak sistemler, endüstri, medya ve bireylerin meydana getirdiği topyekun bir Küresel Bilgi Ortamı (GIE) kümesi ortaya çıkar ki Askeri Bilgi Ortamı (MIE) bunun sadece bir altkümesidir.

Küresel Bilgi Ortamının askeri ve ulusal otoritelerin denetim ve kumandasının dışında olduğu aşikârdır. Öte yandan, tüm askeri harekâtlar Küresel Bilgi Ortamı (GIE) içerisinde yürütülmek durumundadır.

> İşte bu gerçek -ki buna ister *durum* deyin, ister *vaziyet*, ister *olgu*, ister *çelişki*, ister *paradoks*, ne derseniz deyin, günümüzde bu bir gerçek- Bilgi Harekâtını (IO) ve Bilgi Harbini (IW) askeri çerçevenin dışına çıkarmakta ve tabii ki bir dolu yeni kavram, bakış ve uygulamayı da askeri çerçevenin içine sokmaktadır. Dolayısıyla, bilgi harbi esasında paradigmal bir değişim gerektirmektedir. (Bu sebeptendir ki daha önce de belirtildiği gibi, ABD IO doktrini bir "capstone document" olarak yayınlanmıştır.) Bu yeni paradigma, asker ve sivil birçokları için uyum sağlanması oldukça güç bir geçiş sürecini de beraberinde getirmektedir. Nihayetinde, sınırları belirsiz -neredeyse sınırları olmayan- bir ortamda kuralları belirsiz -neredeyse kuralları olmayan- yepyeni bir harp şeklidir söz konusu olan. (1996 tarihli ABD IO doktrininin 1998, 2003, 2006 ve 2012'de tekrar tekrar gözden geçirilerek yayınlanmış olması boşuna değil.)

Küresel Bilgi Ortamının bir unsuru olan yazılı ve özellikle görsel medya, askeri harekâtların yön ve kapsamını etkileyebilir. İkinci Dünya Harbi'nden bu yana medyanın harekât ortamında yer alması gittikçe yaygınlaşmıştır. Normandiya çıkarmasını 150 muhabir izlemişken, Çöl Fırtınası harekâtında sadece Kuveyt'te görev yapan

muhabirlerin sayısı neredeyse on misli artmıştı. Süratle gelişmekte olan teknoloji, herhangi bir askeri harekâtın küresel boyutta bilinmesini engellemeye yönelik her türlü çabayı geçersiz kılmaktadır.

> Harekâtın icrasının ötesinde, kimler tarafından, nerede ve nasıl planlandığı dahi ortaya çıkmakta ve medya vasıtasıyla kısa sürede dünya kamuoyuna yayılabilmektedir artık.

Küresel, ulusal ve askeri bilgi altyapısını meydana getiren bilgi şebekelerine girebilme imkânlarının artmasıyla birlikte bilgiyi kontrol etme, sınırlama, bastırma, sansürleme gibi yöntemler gittikçe imkânsızlaşmakta; çoğu zaman uygun görülmemekte, arzu edilmemektedir ama şu da gerçektir ki bir çatışmada taraf olan açık ve gizli hasımlar, bazen bağlantısızlardan veya taraf olmayanlardan da destek bularak, sivil toplum kuruluşları (NGO), uluslararası ajanslar, akademik kurumlar, endüstri, medya ve bilgi ağına erişim sahibi bireylerin yardımıyla küresel, ulusal ve askeri bilgi altyapısına ve bilgi ortamına tesir edebilmektedirler.

> Tabiatındaki bu çelişki, bilgi harbinin icrası kadar planlanmasının da incelikle ve akıllıca yapılmasını gerektirir. Aksi takdirde basit bir harekât, ulusal veya uluslararası boyutta fiyaskoya, hatta felakete dönüşebilir.

Dahası, gelişen teknoloji sayesinde kişiler, gruplar, kuruluşlar veya devletler Küresel Bilgi Altyapısı vasıtasıyla Küresel Bilgi Ortamına bağlandıklarında onun bir alt kümesi olan Askeri Bilgi Ortamındaki bilgi akışını ve içeriğini kendi menfaatleri doğrultusunda manipüle edebilirler.

Askeri Bilgi Ortamı (MIE) olarak tanımlanan bilgi ortamı, Küresel Bilgi Ortamının GIE) bir alt kümesidir. Askeri harekâtları mümkün kılan, destekleyen veya önemli derecede etkileyen dost ve düşman, askeri ve sivil bilgi sistemleri ve oluşumlar Askeri Bilgi Ortamını meydana getirir. Değişik mekân, zaman, amaç ve muhataplara ulaşan Askeri Bilgi Ortamı çerçevesinde askeri liderler yeni zorluklar ve fırsatlarla karşılaşırlar. Günümüzün hayli karmaşık Askeri Bilgi Ortamının zorlukları ile baş edebilmek için yine aynı bilgi ortamının yarattığı fırsatlardan yararlanılır. Bunun için güncel Askeri Bilgi Ortamını ayrıntılı şekilde tanımak ve ona tamamen hakim olmak gerekir.

Komutanın muharebe alanı artık küresel ölçekte bilgi akışını içermektedir. Taktik bir askeri harekât birdenbire geniş ölçekte politik ve sosyal etkiler yaratabilir. Komutan, bunun bilincinde olarak planlamalı harekâtı ve icra etmeli. Muharebeyi kazanmanın en önemli şartı olan *vaziyet hakimiyeti*, yani durum hakkında bilgi sahibi olma mecburiyeti, muharebe alanının çok daha ötesinde ve askeri olmayan unsurları da kapsamaktadır artık.

°° Bilgi Altyapısına/Ortamına Yönelik Tehditler

Bilgi altyapılarına yönelik genellikle özgün, teknik bakımdan çok yönlü, dünya çapında kaynaklı ve gittikçe büyüyen tehditler söz konusudur. Tehdit, herhangi bir coğrafi sınırlamaya tâbi olmaksızın, dünya çapında askeri, politik, sosyal, kültürel, etnik, dinî veya kişisel güdülerle yönlendirilmiş şahıslar veya gruplardan kaynaklanabilir. Ayrıca,

herhangi bir zaman veya durum sınırlamasına da tâbi değildir; savaşta veya barışta, her an gelebilir, kaynağını tespit etmek de imkânsız olabilir.

Bilgi altyapısının güvenilirliğini sarsmak, kullanıcıyı şüpheye düşürmek oldukça etkili bir yöntemdir.

> Hani, bozuk saat-durmuş saat kıssasındaki gibi; doğruluğundan emin olunmayan bilgi, doğru olmayan veya hiç olmayan bilgiye nazaran daha çok zarar verir. Güvenlik jargonunda buna, "yalancının mumu" taktiği denebilir.
>
> Bu nedenledir ki -birinci bölümde bir nebze değindiğim üzere- istihbarat kavramında haber almadan ziyade analiz ve değerlendirme (intelligence) öne çıkmalıdır. Gerisi dedikodudur.

Bilgi altyapılarına/ortamlarına yönelik tehditlere örnek vermek gerekirse:

-- Bilgi elde etmek veya bilgi zerk etmek amacıyla yetkisiz erişim.

-- Bilgi yönetim sisteminin (bilgisayarın, terminalin, sunucunun, kontrol sisteminin, vs.) istenilenin veya beklenenin haricinde çalışmasını sağlayan (virüs, vb.) zararlı yazılım veya donanım.

-- (virüs, vb.) Zararlı yazılım vasıtasıyla bilgiyi değiştirmek veya zarar vermek.

-- Veri, sinyal veya radyasyon vasıtasıyla elektronik istihbarat toplamak

-- Bastırma, karıştırma, elektromanyetik darbe (EMP) gibi elektronik taarruz yöntemleri. (sadece hedefe yönelik olabileceği gibi tüm sivil altyapıya da yönelik olabilir)

-- Aldatma ve/veya psikolojik harekât.

-- Bilgi sistemlerine ve şebekelerine fiziki taarruz. (patlayıcı yerleştirmekten hava saldırısına kadar çeşitli şekilde ve ölçekte olabilir)

°° Tehdit Kaynakları

Bilgi altyapısının tabiatı gereği, şahıslardan terörist gruplara veya askeri birliklerden istihbarat teşkilatlarına, çok çeşitli kaynaklardan gelebilir tehditler.

> Günümüz teknolojisinin sağlamış olduğu olanaklar çoğu zaman komplo teorilerini ateşlemektedir. Kimi zaman çok yetenekli bir hackerin marifeti zavallı bir küresel güç odağının üzerine yıkılabilir. Veya tersi de mümkündür.

Yetkisiz kullanıcılar: Bilgi sistemlerine yönelik saldırıların çoğu barış zamanında daha ziyade kişisel bilgisayarlara yönelik bireysel saldırılar şeklinde olmaktadır.

> "olmuştur" demek daha doğru. FM 100-6 IO doktrininin yazıldığı 1996 yılında durum böyle olabilir ama bu derlemenin yazıldığı 2013'e dek yetkisiz şahısların kamu veya askeri kurumların bilgi sistemlerine yönelttiği birçok saldırı gerçekleşmiştir.

İçerdekiler: Bilgi sistemlerine erişim yetkisi bulunan kullanıcılardan kaynaklanan saldırılar oldukça yaygındır. Para karşılığı veya kendine göre sebeplerle motive olan

saldırganlar, dışardan gelmesi muhtemel saldırılara karşı korunmuş bilgi sistemlerine içerden kolayca nüfuz edebilir. Bu tür sızmalar çoğunlukla tasarım, üretim, yer değiştirme veya bakım esnasında gerçekleştirilebilir.

> Yıllar önce çalıştığım işyerinde kullanılan bazı önemli yazılımın, geliştiren mühendisin işten ayrılmasından sonra çalışmaz hale gelmesi kayda değer maddi kaybın yanı sıra büyük prestij kaybına sebep olmuştu.

Devlet harici organizasyonlar veya teröristler: Aktivistlerden anarşistlere, uyuşturucu kartellerinden teröristlere uzanan geniş bir yelpazede tehdit kaynakları bilgi sistemlerine saldırı düzenleyebilirler. Bu saldırılar, bilgi altyapısını imha girişimleri şeklinde olabileceği gibi, yetkisiz erişim veya hizmeti engelleme veya mahcubiyet yaratıcı saldırılar şeklinde de olabilir. Bazı durumlarda, gündemden kalkmış sorunları gündeme taşıyan, huzursuzlukları ateşleyen, tahrik edici girişimler de denenebilir.

> "Devlet harici" sıfatı bir anlamda devletin yapma hakkı olduğunu ima ediyor. Alıntı yapılan kaynak bir askeri doktrin olduğu için bu bakış geçerli olabilir; ancak, geniş anlamda küresel bilgi altyapısı/ortamı konu olduğunda devlet kurumlarının yetkisiz ve yasa dışı müdahalesi de tehdit olarak değerlendirilmelidir.

Siyasi veya askeri düşmanlar: Düşman faaliyeti genellikle çatışma veya savaş zamanı artar; ancak barış zamanında da, özellikle çatışma öncesinde, bilgi sistemlerinin ve bilhassa medyanın yoğun şekilde manipüle edilmesi söz konusu olur.

Yabancı istihbarat servisleri: Gerek barış, gerekse savaş zamanında yabancı istihbarat kuruluşları ileri teknolojik imkânlardan yararlanarak her türlü saldırı yöntemini uygulayabilir, bizatihi kendisi saldırabilir veya yukarıda bahsedilen diğer kaynakları kullanabilir.

°° Tehdit Seviyeleri

Barış zamanında genellikle bilgi sistemlerine, özellikle kişisel bilgisayarlara veya sunuculara yetkisiz giriş türünde saldırılar gerçekleştirilmektedir. Ayrıca, gerek endüstriyel, gerekse askeri kuruluşlarca kullanılan haberleşme, ulaştırma, bankacılık ve enerji sistemlerine zararlı yazılım enjekte etme girişimleri de oldukça yaygındır. Bu girişimler vasıtasıyla kritik sistemlerin kırılganlığı, yani saldırıya ne denli açık olduğu test edilir.

Kriz, açık çatışma veya savaşa doğru ilerledikçe, bilgi sistemlerine yönelik saldırıların türü değişir; sıklığı ve şiddeti artar. Bu arada, barış zamanında gerçekleştirilmiş olan saldırıların meyveleri toplanır: kırılganlık derecesi bilinen sistemlere yönelik saldırılar düzenlenir; daha önceden yerleştirilmiş olan zararlı yazılımlar sayesinde zayıflatılmış olan sistemler savaş zamanında çalışmaz hale getirilir.

> Günü geldiğinde sistemleri işe yaramaz hale getirecek, önceden yerleştirilmiş zararlı yazılımlardan ABD IO doktrininde söz edilmiş olması, oldukça yaygın kabul gören bir paranoyayı desteklemektedir. ABD veya bir başka yabancı ülkeden alınan sistemlerin içerisine yerleştirilmiş ve zamanı geldiğinde aktive olacak zararlı yazılım kodlarından şüphe duyulmaktadır. -- Mümkün mü? -- Evet. – Mantıklı mı? -- Belki. – Pratik

> mi? -- Hayır. Unutmamalı ki kapitalist dünyada ticaretin güvenilirliği çok önemlidir. Ama ne yazık ki bu şüphe bir nevi ulusal paranoyaya dönüşmekte ve olumsuz sonuçlara yol açmaktadır. Teknolojik üstünlüğe erişimi engellemek isteyenler tarafından bilhassa yaratılıyor olabilir bu paranoya.

Düşmanın savaşta sadece askeri unsurları değil, destek altyapısını da hedef alması beklenmeli. Bu hedeflere yapılacak saldırılar sadece bilgi sistemleri vasıtasıyla değil, fiziki imha yöntemleriyle de gerçekleştirilebilir. Özellikle güç kaynaklarını hedef alan saldırıların zararları çok daha fazla ve telafisi zor olur. Seyir (cruise) füzeleri, hassas güdümlü silahlar, küresel konumlama sistemleri (GPS), insansız hava araçları (İHA), gerçek zamanlı görüntüleme uyduları geliştikçe hedefleri çok daha hassas vurmak, imha etmek mümkün olmaktadır. Bunun yapılamadığı durumlarda ise kimyasal veya biyolojik silahlarla kirleterek kullanılamaz hale getirilir.

> Bilgi harekâtı ile ilgili doktrinde füzelerden, bombalardan, kimyasal ve biyolojik silahlardan bahsediliyor olması ister istemez şaşırtıyor insanı. Ancak, bu ve sonraki tarihli doktrinlerde fiziki taarruz ve imha, bir tür bilgi harekâtı becerisi olarak belirtilmektedir. Sonuçta, bilgi harbi de olsa, bahse konu olan harptir; ne zaman, nerede, nasıl duracağı belli olmaz.

Bilgi harekâtı doktrininin yayınlandığı 1996 yılı itibariyle ABD Savunma Bakanlığı'nın haberleşmesinin yüzde doksan beşi askeri otoritenin etkisi ve denetimi dışında, korunmasız telefon şebekesi üzerinden yapılmaktadır. Ayrıca, önemli miktarda açık kaynak istihbaratı ticari yollardan toplanmaktadır.

Sivil ve askeri liderler, bilgi iletişim teknolojisindeki hızlı değişim ve bunun Küresel Bilgi Ortamı üzerindeki etkisi sayesinde operasyonların küresel ölçekte görünür olmasının yaratacağı etkileri öngörmeli ve onlarla baş edebilmeli.

Askeri harekâtların küresel görünürlüğü, medyadaki dramatik gösterimi ve uzman yorumları kamuoyunu, dolayısıyla askeri harekâtın yürütülmesi ile ilgili politikayı etkilemektedir. Küresel görünürlük, harekâtı yöneten komutanın kararlarını etkiler. Öte yandan, gerçeği yansıtmayan haberler, dedikodu ve dezenformasyon da harekâtın sağlıklı yürütülmesini olumsuz etkiler, hatta sona erdirilmesini dahi gerektirebilir. Bu sebeple komutan, düşmanın haberleri ne şekilde manipüle edebileceğini değerlendirmek ve ona göre tedbir almak durumundadır.

Askerler, komuta zinciri içerisinde kendilerine ulaşana nazaran daha hızlı ve kolay şekilde medya ve bilgi sistemleri ağı vasıtasıyla -doğru ya da yanlış- bilgiye ulaşma imkânına sahiptler. Askerin savaşma azmi, kazanma arzusu, davaya olan inancı ve silah arkadaşlarına olan bağlılığı küresel ortamda yer alan haberlerden, yayınlanan görüntülerden etkilenir; duruma göre, zayıflar. Harekâtın görünürlüğünün askerin morali üzerindeki olumlu ya da olumsuz etkisi askerin muharebe kabiliyetini ve gücünü önemli derecede etkiler.

Bilgi sistemlerine ulaşımı denetleyen çok az kural vardır. Hassas bilginin veya kritik ağ bağlantılarının korunmasına yönelik kurallar belirgin değildir. Öte yandan, mevcut kuralların çoğu bilgiye serbest ulaşımı teminat altına almak amacıyla konmuştur. Askeri Bilgi Ortamının birçok unsuru askeri dost kuvvetlerin kontrolünün dışında olabilir veya

birtakım hukuki kısıtlamalar bazı sivil kaynakların düşman tarafından kullanılmasını engellemeyi imkansız kılabilir.

> Bazı televizyon ya da sosyal medya yayınlarını engellemede ne denli zorlandığımızı hatırlayalım.

Örneğin, kriz anında kritik görüntü istihbaratı sağlayan uydudan alınan veriyi korumak için uyduya erişim kodlarının değiştirmek gerekebilir. Ancak hizmet eğer uluslararası ticari bir kuruluştun alınıyorsa, mevcut sözleşme buna müsaade etmeyebilir ve dahası, düşman da aynı kuruluşla yapmış olduğu sözleşme sayesinde görüntü bilgisine ulaşıyor olabilir.

> Kendi görüntü ve haberleşme uydularına sahip olma ihtiyacı acil ve gerçek ve acildir.

°° Bilgi Üstünlüğü

Tüm bunların ışığında ortaya çıkmaktadır ki harekât ortamını kontrol edebilmek ve avantaj elde edebilmek için bilgi üstünlüğüne sahip olmak elzemdir. Bu üstünlüğün iki önemli unsuru vardır: dost kuvvetlerin bilgi harekâtı yetisini artırmak ve düşmanın benzer yetisini zayıflatmak. Başarılı liderler insan istihbaratı ile teknik istihbaratı birlikte değerlendirmek suretiyle bu üstünlüğü elde edebilirler.

> Bilgi üstünlüğü kavramı yeni değildir; tarih boyunca sivil ve askeri birçok taktisyen ve stratejist tarafından önemi vurgulanmıştır.

Yönlendirilmiş teleskop: Bilgi üstünlüğünü elde etmenin yollarından biri, geçmişte çokça örneği görülen "yönlendirilmiş teleskop" veya dürbün diye adlandırabileceğimiz yöntemdir. Geleneksel, hiyerarşik bilgi elde etme usullerinin göz ardı edildiği bu yöntemde, özel harekât veya keşif elemanları, bilhassa atanmış kişiler veya teknolojik imkânlar vasıtasıyla noktasal hassasiyette bilgi elde edilebilir.

> Yönlendirilmiş teleskop yöntemi askeri harekâtların haricinde birçok sivil kurumda veya şirkette çokça kullanılmaktadır. Birçok kurumda ya da şirkette yok mudur doğrudan genel müdüre bilgi aktaran bir şoför veya teknisyen veya depo görevlisi? Rivayet edilir ki Mareşal Montgomery, önemli brifinglerin öncesinde, sadece kendisinin görevlendirmiş olduğu en fazla binbaşı rütbesindeki subaylardan bilgi aldıktan sonra generalleriyle brifinge katılırmış.
>
> Günümüz teknolojik imkânları, mevcut haberleşme ve bilgi sistemleri birlikte değerlendirildiğinde, yönlendirilmiş teleskop yönteminin kullanılma sıklığı, çokluğu ve fırsatlarının hayli artmış olduğu görülmektedir.

Harekât Ortamının Görüntülenmesi: Harekât ortamının görüntüsünü gerçek zamanda elde ediyor olması, komutanın gidişatı sağlıklı değerlendirmesi ve arzu edilen sonuca ulaşması bakımından çok önemlidir.

Durum Farkındalığı: Harekâtın amacı ve gidişatı arasındaki ilişkiyi komutanın değerlendirebilmesi ve duruma göre amaca yönelik doğru kararlar alabilmesi için

durum farkındalığının olması gerekir. İlaveten, gerektiğinde bu farkındalığın daha alt kademelere ve diğer dost kuvvetlere aktarılabilmesi de önemlidir.

Genişletilmiş Bakış: Düşmana üstünlük sağlamak ve dost kuvvetleri korumak amacıyla harekâta yönelik bakış -bilgi harekâtının imkânlarını da içerecek şekilde- genişletilmeli; komutanın değerlendirmesi hem kendi denetimindeki, hem de dışındaki unsurları kapsamalı. Bu genişletilmiş bakış, zaman, mekân, hedef ve kişilerin muhtelif kombinezonları şeklinde olabilir. İyi bir manevra nasıl ki düşmana nazaran daha fazla avantaj sağlıyorsa, olumlu algı ve destek de aynı şekilde avantaj sağlar. Bu avantajı elde etmenin ve muhafaza etmenin yolu Psikolojik Harekât (PSYOP), Sivil İşler (CA) ve Halkla İlişkiler (PA) gibi bilgi harekâtı unsurlarının başarılı kullanılmasından geçer.

> PA Public Affairs Halkla İlişkiler Public Affairs deyimini kamu veya amme işleri diye tercüme etmek doğru olurdu; ancak yapılan iş daha ziyade Public Relations, yani Halkla İlişkiler şeklinde tanımlanabilir.

Düşmanın muharebe imkânlarını ve savaş azmini ortadan kaldırmayı amaçlayan ateş gücünün Askeri Bilgi Ortamındaki karşılığı sayılabilecek Komuta Kontrol Harbinde (C^2W) düşmanı alt etmek veya dost kuvvetleri korumak amacıyla aldatma, psikolojik harekât, elektronik harp, harekât güvenliği ve fiziki imha becerilerinden yararlanılmaktadır.

Bu beceriler ABD silahlı kuvvetleri tarafından daha önceleri de kullanılmaktaydı; ancak, bahse konu IO doktrinin yayınlandığı 1996 itibariyle bu beceriler C^2W çerçevesinde operasyonlara entegre edilmektedir. Bu entegrasyon sayesinde, geleneksel saldırı yöntemlerine ilaveten aldatma, psikolojik harekât, elektronik harp, harekât güvenliği becerilerinin gücünü düşmanın karar çevrimine yönlendirmek ve bu sayede çevrimin kontrolünü ve bilgi üstünlüğünü ele geçirmek mümkün olmaktadır.

Komuta ve Kontrol Harbinin alt unsurları olan Psikolojik Harekât (PSYOP) ile Halkla İlişkiler (PA) ve Sivil İşler (CA) uygulamalarında özen gösterilmeli; özellikle halkın gözünde halkla ilişkilerin güvenilirliği, inanılırlığı ve bütünlüğünü korumak için PA ve PSYOP arasında ayrım yapılmalı.

Açık Medya Kapsaması: Bilgi harekâtının yürütülmesinde, medya ve küresel görünürlüğe dikkat etmek gerekir. ABD Savunma Bakanlığı (DoD) politikası, silahlı kuvvetlerin görevleri ve yetenekleri hususunda Amerikan kamuoyunun bilgilendirilmesi için komutanların medyaya açık ve bağımsız haber imkânı sağlamasını gerektirir. Halkla ilişkiler (PA), haber medyasıyla ilişkide komutanın önemli enstrümanıdır. Kamuoyunun doğru bilgilendirilmesi, askerin moralinin yükseltilmesi ve bu sayede görevin başarıyla tamamlanması için medya mensuplarının doğru haber almasına imkân verecek şekilde komutanlar hem kendilerini, hem de astlarını eğitmelidirler.

Bu doktrinin amacı harekâtın gidişatına medyanın etkisi hususunda komutanların dikkatli olmasını sağlamak olmakla birlikte, medyanın yanıltılması veya manipüle edilmesi hiçbir şekilde amaçlanmamaktadır. Medyanın askeri harekâtlarla ilgili olarak kamuoyunu mümkün olduğunca bilgilendirme talebine karşın komutanın bilgi ortamını

kontrol etme arzusu arasındaki sağlıklı çatışma kabul edilmekte ve hatta uygun görülmektedir.

Bilgi Yönetimi: Hızla değişen bilgi teknolojisi, küresel görünürlük ve bunların küresel bilgi ortamına etkisi karşısında *bilgi yönetimi* gittikçe artan önem kazanmaktadır. Çok büyük miktarda verinin elde edilmesi ve hızla bilgi ve anlayışa dönüştürülmesi gerekmektedir. Karar verme süreci gittikçe dinamik ve çok boyutlu hale gelmiştir. Güncel durum ile ilgili karar veriyorken aynı zamanda gelecek ile de ilgili karar vermek söz konusudur; dolayısıyla karar sürecinin hızı, durum farkındalığındaki değişim hızı ile uyumlu olmalı.

Öte yandan, bilgi miktarındaki fazlalık, beraberinde doğruluğu getirmemekte; aksine, belirsizliği artırmaktadır. Mesele, sadece daha hızlı değil, daha iyi analiz ve karar verme mekanizmasını geliştirmektir.

° Esaslar

ABD ordu harekât doktrini FM 100-5, modern muharebe alanında gelişmiş silahların etkinliğini onları kullananların becerisinin tayin edeceğini kabul eder. Bu tespit muhakkak ki bilgi harekâtı için de geçerlidir.

Bilgi harekâtının temel unsurları içerisinde ***harekâtın icrası***, ***alakalı bilgi ve istihbaratın* (*RII*) *değerlendirilmesi***, ***bilgi sistemleri* (*INFOSYS*)** yer almaktadır. Bilgi harekâtının sağlıklı ve salimen icrasında bilgiyi ***elde etmek***, ***kullanmak***, ***korumak***, ***faydalanmak***, ***esirgemek*** ve ***yönetmek*** gibi eylemler söz konusudur.

°° Bilişsel Hiyerarşi

Enformasyon veya malumat anlamında bilgi, ortamdan elde edilen ve kullanılabilir hale getirilen veridir. (Birinci Bölümdeki bilgi hiyerarşisi piramidini burada tekrarlamakta yarar var.)

Veri, tek başına pek anlam ifade etmez; işlemden geçirilip malumat (enformasyon) haline geldiğinde anlam kazanır. Test edilip doğruluğu kabul edildiğinde ise yararlı bilgi (yararlı malumat) haline gelir.

Malumat halindeki bilgi zihinsel idrak sürecinden geçerek yararlı bilgi halini alır. Bu süreçte, doğrulanmamış malumatın gerçek olarak kabulü veya deneyerek doğrulanması söz konusu olabilir. Bu sebepledir ki inanç ve bilgi arasındaki farkı algılamada komutanlar ve planlamacıların dikkatli olmaları gerekir. Yaygın dahi olsa, denenmemiş inançlar -ileride yanlış olabilecekleri ortaya çıkabilir düşüncesiyle- gerçeklerden farklı değerlendirilmelidir. İnanç üzerine inşa edilmiş karar her zaman tehlike arz eder.

> İnanç, görüş, kanaat, hissiyat üzerine inşa edilmiş kararlar doğru dahi olsa tehlikeli sonuçlar doğurabilir.

Bilgiyi belli bir durum bağlamında değerlendirme ve yargı sürecinden geçirdikten sonra anlama seviyesine ulaşılır. Durumu anlamış olmak, muharebe ortamını değerlendirmede ve buradan yola çıkarak planlar yapmada ve etkin eylemler gerçekleştirmede destek olur komutana. Muhakkak ki karar almadan önce durum hakkında tam ve ayrıntılı anlama seviyesine ulaşmış olmak tercih edilir; ancak komutanlar yine de mükemmel olmayan, eksik bilginin yarattığı belirsizlik ortamında karar almaya hazırlıklı olmalıdırlar.

> Komuta ve karar süreci, Bilgi Çağında dahi bilimden ziyade sanat olarak değerlendirilmektedir, hâlâ. İşte, sanat ile bilim arasındaki bu açıklığı azaltmaktır bilgi harekâtının amacı.

°° Strateji

Ulusal Askeri Strateji, ABD ulusal gücünün askeri unsurları içerisindeki yeteneklerden biri olarak tanımlar bilgi harbini. ABD Hükümeti'nin barış, kriz, çatışma ve çatışma sonrası dönemlerde stratejik angajman politikasını desteklemede bilgi harbinden yararlanılabilir. ABD Hükümeti'nin başkalarının algı ve kararlarını etkileme becerisi, caydırma, güç yansıtma gibi stratejik kavramların etkinliğini hayli artırmaktadır. Bilgi, kriz zamanlarında düşmanın ABD ve müttefikleri aleyhine harekete kalkışmasını engelleyebilir. Eğer iyi şekilde anlaşılır, koordine ve icra edilirse, bilgi harbi krizlerin etkisizleştirilmesine katkı sağlayabilir; karşı karşıya gelme süresini azaltarak diplomatik, ekonomik ve askeri çabaların etkinliğini artırabilir; askeri kuvvetlerin konuşlandırılması ihtiyacını ortadan kaldırabilir.

°° Bilgi Harbi (Information Warfare - IW)

Çatışmada düşmana karşı bilgi üstünlüğünü elde etmek amacıyla yürütülen işlemleri tanımlamak üzere, ABD Savunma Bakanlığı (DoD) ve Genelkurmayı tarafından kabul gören bir terimdir *Bilgi Harbi* (*Information Warfare - IW*). Bir yandan kendininkini korurken, öte yandan düşmanın sahip olduğu bilgiyi, bilgi tabanlı süreçlerini, bilgi sistemlerini ve bilgisayar şebekelerini etkileyerek bilgi üstünlüğünü elde etmek amacıyla yürütülen işlemler olarak tanımlanmaktadır.

Bilgi harbinin amacı düşmanı hızla denetim ve hakimiyet altına almayı mümkün kılacak düzeyde bilgi avantajı elde etmektir. Bilgi harbi her iki tarafa da güvenli şekilde, uzaktan vurma imkânı sunmaktadır.

°° Bilgi Harekâtı (IO)

Savunma Bakanlığı tarafından verilmiş olan mevcut tanımı oldukça dar kapsamlı bulan ABD Kara Kuvvetleri, bilginin kara harekâtı üzerindeki etkisini daha geniş bir bakış açısı ile değerlendirmeyi tercih etmekte ve *Bilgi Harekâtı* (*IO*) deyimini kullanmaktadır. Geleneksel harp bağlamının ötesinde olan bu geniş bakış tarzı, bilgi ile alakalı işlemlerin barıştan küresel savaşa uzanan askeri operasyonlara nüfuz ettiğini kabul etmektedir.

Askeri harekâtın tümüne yönelik avantaj elde etmek amacıyla dost kuvvetlerin bilgiyi toplama, işleme ve kullanmasını mümkün kılan ve askeri bilgi ortamı içerisinde yürütülen bir askeri harekât olarak tanımlanmaktadır Bilgi Harekâtı.

> ABD IO doktrininin -özellikle erken versiyonlarında- Bilgi Harekâtının tamamen askeri bir harekât türü olarak ele alınmakta olduğunu belirtmekte yarar var. Birinci bölümde de belirtildiği üzere, Bilgi Harbi (IW) ile Bilgi Harekâtı (IO) arasında belirgin bir fark, kesin bir sınır bulunmamaktadır. Bilgi Harekâtı (IO) tanımını ABD Kara Kuvvetleri daha geniş anlamda ele almakta; dolayısıyla, bu derlemenin sistematiğinde Bilgi Harekâtı (IO) daha geniş anlamda değerlendirilmekte, Bilgi Harbi (IW) ise çatışma süresince yürütülen muayyen bir eylem veya eylemler dizinini işaret etmektedir.

°° Bilgi Harekâtının (IO) Unsurları

Bilgi Harekâtının (IO) birbiriyle ilgili üç temel unsuru vardır:

- - - ***Harekâtın Yürütülmesi***
- - - ***Alakalı Bilgi ve İstihbarat (Relevant Information and Intelligence - RII)***
- - - ***Bilgi Sistemleri (Information Systems - INFOSYS)***

°°° Harekâtın Yürütülmesi

Harekâtın yürütülmesinde şu becerilerden yararlanılır:

- - - - **Komuta Kontrol Harbi *(Command and Control Warfare - C^2W)***
- - - - **Sivil İşler *(Civil Affairs - CA)***
- - - - **Halkla İlişkiler *(Public Affairs - PA)***

> - - - - ***Komuta ve Kontrol Harbi (Command and Control Warfare - C^2W)*** uygulamalarında yararlanılan beş temel beceri:
>
> - - - - - ***Harekât Güvenliği (Operations Security - OPSEC)***
> - - - - - ***Psikolojik Harekât (Psychological Operations - PSYOP)***
> - - - - - ***Askeri Yanıltma (Military Deception - MILDEC)***
> - - - - - ***Elektronik Harp (Electronic Warfare - EW)***
> - - - - - ***Fiziki İmha (Physical Destruction)***

Komuta ve kontrol harbine (C^2W) ilaveten yararlanılan destekleyici beceriler:

- - - ***Sivil İşler (Civil Affairs - CA)***
- - - ***Halkla İlişkiler (Public Affairs - PA)***

Public Affairs deyimini amme işleri diye tercüme etmek doğru olurdu; ancak yapılan iş daha ziyade Public Relations, yani Halkla İlişkiler şeklinde tanımlanabilir.

Bilgi Harekâtı (IO) unsurlarının uygulanmasında bilgi üzerinde yürütülen altı temel eylem vardır: bilgiyi - ***elde etmek***, - ***kullanmak***, - ***korumak***, - ***faydalanmak***, - ***esirgemek***, - ***yönetmek***.

°°°° Komuta ve Kontrol Harbi (Command and Control Warfare - C^2W)

Düşmanın komuta kontrol (C^2) becerisini zayıflatırken kendi C^2 becerisinin zayıflatılmasını engellemeyi amaçlayan Komuta ve Kontrol Harbinin (C^2W) iki temel bileşeni vardır:

-- C^2-taarruz

-- C^2-koruma (savunma)

Barış zamanından itibaren, kriz ve çatışma dönemi dahil, düşmanlığın sona erdiği ana kadar tüm askeri harekât boyunca C^2W planlanır. Önceleri, harbin temel amacı düşmanın personel ve teçhizatını; yani tanklarını, toplarını, uçaklarını, uçaksavarlarını tahrip etmeye yönelikti. Son dönem hava-kara muharebeleri, derinlik ve senkronizasyon elde etmek için hava ve kara harekâtlarının birlikteliğini ve beraberinde uzun menzilli silahlar ve özel kuvvetler vasıtasıyla derine ulaşan harekât stratejisini gündeme getirdi.

Günümüzde aldatma (MILDEC), psikolojik harp (PSYOP), harekât güvenliği (OPSEC) ve elektronik harp (EW) yöntemlerini entegre ve senkronize eden C^2W operasyonları sistemlerin ve kuvvetlerin bilgi harekâtı için kullanılmasını kolaylaştırmaktadır.

[Sözü edilen yöntemler (beceriler) daha sonra ayrıntılı olarak ele alınacaktır.]

Önceleri saldırı odaklı olan C^2W, şimdilerde C^2-taarruz ve C^2-koruma bileşenlerini içermektedir. Bu iki bileşen her ne kadar tarih boyunca birçok harpte kullanılmış olsa da, bilgiye ve bilgi sistemlerine bu denli önem verilen modern harbe yeni bir bakış gerekmektedir.

Şu üç olgu C^2W kavramını önemli ölçüde öne çıkarmaktadır:

-- Modern askeri teknoloji ve operasyonların gerektirdiği sürekli ve yüksek hacimli bilgi akışı.

-- Teknolojideki hızlı ilerlemenin sonucu olarak bilgi sistemleri (INFOSYS) ve istihbarat becerilerindeki köklü gelişme.

-- Bilgi sistemleri (INFOSYS) ve istihbarat için yaygınca kullanılan ileri teknolojinin saldırıya açık oluşu.

Bugünün askeri bilgi ortamı, tek bir hücum veya muharebe gücü ile düşmanın komuta ve kontrol becerisine ciddi zarar vermeyi zorlaştırmaktadır. Dolayısıyla, hücumlardan

azami faydayı elde etmek için fiziksel imha, elektronik harp (EW), aldatma ve psikolojik harp (PSYOP) yöntemlerinin etkin şekilde entegre edilmesi önem kazanmaktadır. Düşmanın saldırılarına karşı kendi bilgi sistemlerimizi (INFOSYS) ve istihbarat becerilerimizi koruyabilmek için de benzer şekilde entegrasyon ve senkronizasyon gerekmektedir. Hem C^2-taarruz hem de C^2-koruma bileşenlerinin uygulanmasında C^2W harbinin beş unsuru tam olarak entegre ve senkronize edilmediğinde zafiyet meydana gelir ve harekât etkinliği azalır.

C^2-taarruz: Saldırı amaçlı C^2W, yani C^2-taarruzun amacı düşmanın komuta kontrol işlevi üzerinde kontrolü ele geçirmek veya zaafa uğratmaktır.

> İkinci Dünya Savaşında Almanlar Rusya'yı işgal ettiklerinde öncelikle komuta ve kontrol amaçlı telli haberleşme şebekesine saldırdılar ve onu cephedeki komutanlar için güvenilmez, hatta kullanılamaz hale getirdiler. Bunun üzerine, Sovyet ordusu - özünde korunmasız ve müdahaleye açık olan- telsiz şebekesini kullanmaya başladı ki bu onlar için tam bir felakete yol açtı. Rus komutanlar telsiz haberleşmesini de yasaklayınca Sovyet komuta kontrol şebekesi tamamen sağır ve dilsiz hale geldi. Sonuç, Sovyetler için tam bir hezimet oldu.

C^2-koruma: Dost kuvvetlerin komuta kontrol işlevini etkin şekilde yürütebilmesini sağlamak için düşmanın zarar verici çabalarını engellemektir. Dost kuvvetlerin harekâtına, moraline ve kamuoyuna yönelik düşman propagandasına karşı koymak da C^2-koruma kapsamındadır. C^2-koruma, aktif ve/veya pasif tedbirlerle yürütülebilir. Dost kuvvetlerin C^2 zaafını giderici tedbirler pasif koruma olarak tanımlanır. Aktif tedbirler olarak ise beş temel C^2W becerisinden biri veya birkaçı kullanılabilir.

> Ayrıntılı C^2-taarruz planlayıp süreci tersine uygulamak oldukça etkin bir C^2-koruma yöntemi olabilir.

°°°° Sivil İşler (Civil Affairs - CA)

Barışta, krizde veya savaşta askeri operasyonların yürütülmesi, muharebe gücünün pekiştirilmesi ve bilgi üstünlüğünün elde edilmesinde sivil işler (CA) desteğinden yararlanılır ve bu sayede askeri kuvvetler, sivil otorite ve sivil halk arasında temas oluşturulur ve sürdürülür. CA eylemleri, askeri kuvvetlerle dost yabancı ülke halkı ve sivil otorite arasındaki ilişkiyi kapsar; ABD milli politikası ve amaçları doğrultusunda harekât bölgesindeki yerel altyapının denetiminin yanı sıra ABD kuvvetlerinin yerel destek ve kabul görmesini sağlar. Bu sebeple, birçok CA eylemi özel sivil beceriler gerektirir.

Kamu idaresi, kamu tesisleri, ekonomi, kültür, dilbilim, habercilik alanlarında becerilerini sergileyerek komutanın kritik bilgi ihtiyacının karşılanmasına yönelik haber toplayan CA unsurları askeri harekâtın yürütülmesine yardımcı olurlar. Harekâtın planlanmasında komutanlar CA operasyonlarını dikkate alırlar. Gerek istihbarat, gerekse harekâtın planlanması aşamalarında CA personeli oldukça girift, önemli rol oynar.

Yabancı ülkedeki sivil unsurlarla yakın ilişki içerisinde olan CA personeli aynı zamanda sosyal, kültürel, ekonomik ve politik konularda bilgi toplamak için oldukça avantajlı

konumdadırlar. CA personeli, temel bilgi kaynağı olan kişilere, doküman ve ekipmana ulaşma imkânına sahiptir. Toplanan bilgi, diğer kullanıcıların da yararlanacağı şekilde değerlendirilir. Bu bağlamda, CA eylemleri istihbarat eylemleriyle yakından alakalıdır. Herhangi bir sürprizle karşılaşmamak için ABD kuvvetleri zamanında ve doğru istihbarata ihtiyaç duyarlar ve bu amaçla CA ile istihbarat yakınlaşır. Ancak, her ne kadar insan istihbaratı ve teknik istihbarata destek olsalar da, CA personeli kesinlikle istihbarat ajanı gibi davranmamalı.

Çünkü değiller...

Başarılı bir harekât için CA ile yerel askeri kurumlar, koalisyon askeri kurumları, ABD kurmayları, ABD hükümeti, yabancı hükümetler, uluslararası ajanslar, sivil toplum kuruluşları (NGO) ve gönüllü kuruluşlar (PVO) arasında yakın koordinasyon ve işbirliğine ihtiyaç vardır.

NGO ve PVO'larla ilişkide karşılıklı saygıya riayet etmek gerekir; çünkü NGO ve PVO'ların kendi görevleri vardır ki bazen bu durum ABD kuvvetlerinin işini zorlaştırıyor olabilir. Komutan, askeri kuvvetlerle sivil unsurlar arasındaki irtibat ve koordinasyonu sağlamak için sivil-askeri operasyon merkezi (CMOC) oluşturur.

Mesela, sağlık ve yiyecek yardımı yapan bir gönüllü kuruluş, yerel halkın insan hakları ihlallerine maruz kaldığını tespit eder ve yardım ister; Dışişleri Bakanlığı yerel hükümeti uyarır ve askeri kuvvetler -diğer görevlerine ilaveten veya pahasına- yerel halkın yardımına gider.

Ayrıca, CA ile PA ve PSYOP arasında da yakın ilişki vardır. Üçü de aynı iletişim ortamını kullanmakta, ancak farklı muhataplara hitap etmektedir. CA ve PSYOP yerel muhataplara; PA ise ABD kuvvetleri, ulusal ve uluslararası medyaya hitap eder.

°°°° Halkla İlişkiler (Public Affairs - PA)

Birçok askeri harekât kamuoyunun gözü önünde yapılmaktadır. Ulusal ve uluslararası medya kamuoyunun oluşmasında ve şekillenmesinde önemli rol oynamaktadır. Haber medyası, neredeyse gerçek zamanda geniş kitlelere hızla ulaşan bilgi akışı sayesinde harekâtın amacının ve yürütülüşünün analiz ve kritik edildiği halka açık bir forum şeklinde hizmet etmekte; harekâtın siyasi, stratejik ve operasyonel planlamasını ve görevin başarısını etkilemektedir.

PA, komutanın yürütülmekte olan harekât hakkında Amerikan halkı ve askerlerinin bilgilendirilmesini sağlar. Amerikan halkının kendi silahlı kuvvetlerine olan güveni bu sayede sağlamlaştırılmış olur.

PA personeli;

-- Orduya güveni artıran koşulları oluşturarak komutana yardımcı olurlar.

-- Birliklere, askerlere erişim sağlayarak açık ve bağımsız haber elde edilişine destek verirler.

-- Doğru ve zamanında bilgi akışı vasıtasıyla ordunun söyleminin dengeli, adil ve güvenilir şekilde sunulmasını sağlarlar.

Komutan, iç haber ağı vasıtasıyla kendi askerlerini de bilgilendirir; bu sayede, harekâttaki rolleri, onlardan ne beklediği, görevin başarısına nasıl katkıda bulunacakları hususunda askerlerini bilgilendirmenin yanı sıra, düşman propagandasından etkilenmelerini engeller.

PA personeli bilgi ortamını değerlendirerek ve operasyonların halkla ilişkiler boyutu ile ilgili tavsiyelerde bulunarak komutana destek olurlar. Liderlerin, hem dahili, hem de harici muhataplara dengeli, dürüst ve güvenilir bilgi arzının önemini anlaması; durum değerlendirme ve planlama sürecine PA'yı da dahil etmesi; PA operasyonunun harekâtın diğer unsurlarıyla senkronize ve planlama sürecinden itibaren CA ve PSYOP ile koordine olmasını sağlaması gerekir.

> Haberlerin facebook veya twitter vasıtasıyla neredeyse dakikalar mertebesinde tüm dünyaya yayıldığı günümüzde PA personelinin işi artık çok zor. Hangi medya yöneticisini ikna edebilecekler ki?.. [Belki de daha kolayı, kendileri medya yöneticisi olabilirler.]

°°° Alakalı Bilgi ve İstihbarat (Relevant Information and Intelligence - RII)

Liderler tarih boyunca bilgiye sahip olmaya çalışmışlardır. Kendi kuvvetlerinin ve düşmanın yerini, ne yapmakta olduğunu ve muharebe etkinliğini bilmek tüm başarılı komutanların isteğiydi. Günümüzün komutanları, taktik, operasyonel ve stratejik seviyede çok hızlı bilgi akışı ve karar verme mecburiyeti ile karşı karşıyadırlar. Küresel bilgi ortamında kişiler, organizasyon ve sistemden gelen bir dolu bilgi de eklendiğinde durum çok daha karmaşık hale gelmektedir.

Etkin C^2, nihayetinde, doğru kişinin doğru zamanda doğru bilgiye sahip olmasına bağlıdır. Komutanın düşman hakkında bilgi kaynağı olan *istihbarat*, içinde bulunduğumuz Bilgi Çağında gittikçe artan önem taşımaktadır. Bilgi Harekâtı (IO), muharebe alanını küresel boyuta taşıdığı için mevcut ve olası düşmanlar hakkında istihbarat küresel ölçekte toplanmalı ve değerlendirilmelidir. Askeri bilgi ortamı, mevcut ve olası düşmanlarla ilgili kültürel, politik ve ticari cepheleri de kapsayan istihbarat gerektirmektedir.

Komutan, komuta edebilmek için bilgi sahibi olmalıdır. Alakalı bilginin toplanması, işlenmesi ve yayılması durum farkındalığını oluşturmanın anahtarıdır. Komutan, harekâtla uyumlu olarak durum farkındalığını artırmak amacıyla, küresel bilgi ortamı (GIE) içerisinde askeri bilgi ortamını (MIE) düzenler. Buna ilaveten, harekâta yönelik ihtiyaçları, kritik bilgi ihtiyacını ve dolayısıyla alakalı bilgi ve istihbarat (RII) toplama faaliyetini belirler. RII desteği barış zamanından itibaren harekâtın tüm evreleri boyunca sürdürülür. İstihbarat çevrimi, etkin olabilmesi için, daima harekâtın öncelikleri ile uyumlu bilgi sağlayacak şekilde yönetilmeli.

> Alakalı bilgi, düşman ile alakalı istihbarata ilaveten dost kuvvetlerle alakalı bilgiyi de içermektedir. (Alakalı bilgi, istihbaratı da içeren bir üst kümedir.)

Bilgi kaynakları mükemmel olmadığı, hatta bozulma ve yanılmaya yatkın oldukları için, komutanlar ve planlamacılar elde edilen bilgiyi kullanmadan önce dikkatli bir değerlendirmeye tabi tutmalılar.

Bilgiyi değerlendirmede şu kriterler kullanılır:

-- **Alakalı** (Relevant) Görev veya durumla alakalı.

-- **Doğru** (Accurate) Gerçek durumu gösteriyor.

-- **Zamanında** (Timely) Karar vermeye imkân verecek kadar erken zamanda.

-- **Kullanılabilir** (Usable) Kolay anlaşılabilir formatta.

-- **Tam** (Complete) Karar vermek için gereken tüm bilgi var.

-- **Hassas** (Precise) Gereken ayrıntı var.

Öncelik sırası şöyledir: Birinci öncelik; alakalı ve doğru. İkinci öncelik; zamanında ve kullanılabilir. En son; tam ve hassas.

> Veya, şöyle denebilir: Tam ve hassas olmayan bilgi, *hiç olmamasından iyidir*. Zamanında ve kullanılabilir olmayan bilgi, *hiç olmaması ile aynı değerdedir*; olsa da olur, olmasa da. Doğru ve alakalı olmayan bilgi, *hiç olmamasından daha kötüdür*, zararlıdır.

°°°° İstihbarat

İstihbarat, yabancı ülkeler veya bölgeler hakkındaki bilginin elde edilmesi, işlenmesi, entegrasyonu, analizi, değerlendirilmesi, ve yorumlanması sürecinin ürünü şeklinde tanımlanır. İstihbarat, düşmanla ilgili olarak gözlem, araştırma, analiz ve değerlendirme vasıtasıyla elde edilmiş bilgidir.

> Her iki tarif de dar anlamda askeri istihbaratı tanımlamak için geçerli olabilir ancak.

İstihbarat aynı zamanda, alakalı bilginin esasen yabancı ortama ve düşmana yönelik kritik bir alt unsurudur. Dost kuvvetler için istihbarat, belirsizliği gideren ve komutanın karar sürecini kısaltan, muharebe alanı ile alakalı güncel bir resim koyar ortaya.

Özünde, komutanın istediği bilgiyi toplamak, analiz etmek, elemek ve sunmak olan istihbaratın amacı, harekâtla ilgili olarak doğru durum değerlendirmesine dayalı kararları mümkün kılmaktır; alakalı olmayan bilgiyi eleyerek komutanın içinde bulunduğu belirsizliğin giderilmesine yardımcı olur.

İstihbaratın işlevlerinin başında dost kuvvetlerin zaaflarını tespit etmek gelir. Günümüz askeri bilgi ortamının akışkan ve geçirgen olması, Bilgi Sistemlerinin (INFOSYS) korunmasını oldukça zorlaştırmaktadır. İstihbarat, hayati Komuta Kontrol (C^2) unsurları ve becerilerini korumak amacıyla gerekli risk değerlendirmesini yapabilmesi ve risk yönetimi seçeneklerini geliştirebilmesi için komutana gerekli bilgiyi temin eder. Risk değerlendirmesi, belirli tehdit becerilerini, teknik becerileri, doktrini ve tehdit eden kuvvetin geçmişteki performansını dikkate alır. Risk değerlendirmesi bir kez yapılan ve tamamlanan bir iş değil, devam eden bir süreçtir.

İstihbaratın en temel işlevi, tabii ki düşmanın anlaşılmasıdır. Düşmanın bilgiyi nasıl kullandığını anlayarak nereye, ne şekilde müdahale edilmesi gerektiği belirlenir. Savaşın her aşamasında istihbarat, düşmanın C^2 ve INFOSYS becerilerini değerlendirir ve onlardan faydalanır; düşmanın hangi bilgiyi, ne şekilde topladığını, hangi kaynaklara ne kadar güvendiğini ve bilgiyi nasıl değerlendirdiğini belirler. İstihbarat elemanları, düşmanın karar sürecini tanımlar; -bilahare psikolojik harekât (PSYOP) ve yanıltma operasyonlarında yararlanmak üzere- karar verici liderlerin psikolojik durumu, sosyal ve kültürel çevresi hakkında ayrıntılı bilgi toplar. İlaveten, liderden gelen talimatları alt kademedekilerin nasıl yerine getirdikleri hususunu da değerlendirir.

°°° Bilgi Sistemleri (Information Systems - INFOSYS)

Bilgi Sistemleri (INFOSYS), halen süregiden ve gelecekteki harekâtlarla alakalı bilginin toplanması, işlenmesi ve yayılması faaliyetidir. Otomasyon tabii ki bilginin toplanması ve işlenmesinde önemli gelişme sağlamıştır ama alakalandırma ve kaynaştırma hâlâ en etkin şekilde insanlar tarafından yapılmaktadır.

INFOSYS sayesinde komutan, mevcut durumu izler; yakın, derin ve geri operasyonları tek bir operasyonmuş gibi kontrol ve senkronize eder, silah sistemlerinin hedef parametrelerini günceller.

Askeri gücün etkin şekilde tatbiki için INFOSYS elzemdir. Entegre INFOSYS mimarisi ordunun tüm harekât ortamlarındaki Komuta Kontrol (C^2) becerisini artırmaktadır.

Operasyonel mimari, süreçler, fonksiyonlar, organizasyonlar ile bilgi arasındaki gerekli bağı oluşturur; ne yapıldığını, onu yapmak için hangi bilgiye ihtiyaç olduğunu ve kuvvet içerisinde ne sıklıkta bilgi paylaşımı yapılması gerektiğini belirler. Sistem mimarisi, komuta, kontrol, haberleşme, bilgisayar ve istihbarat (C^4I) unsurları arasındaki ilişkileri ortaya çıkarır ve bilgi sisteminin fiziksel bağlantısını sağlar. Teknik mimari ise INFOSYS'i oluşturan parçalar arasındaki dizilişi, ilişkileri ve bağımlılıkları yöneten kuralları belirler.

> Fütürist yazar, karı koca Heidi ve Alvin Toffler'dan bir alıntı yer almaktadır IO doktrininde; öyle ki neredeyse tüm doktrinin ana fikrini özetlemektedir:
>
> Herhangi bir askeri güç - tıpkı bir şirket gibi- bilgi ile alakalı en az dört temel işlevi yerine getirmelidir. Bilgiyi *elde etmeli*, *işlemeli*, *yaymalı*, *muhafaza etmeli*; titizlikle seçerek dostlarıyla paylaşmalı ve hasımlarından esirgemeli. War and Anti-War…

Günümüzün gelişkin teknolojik ortamında komutan, askeri bilgi sistemlerinin yanı sıra, sivil bilgi sistemlerini de gittikçe daha fazla kullanmak durumundadır. Ancak, askeri olmayan bilgi sistemlerinin güvenliği hususunda Savunma Bakanlığı'nın sınırlı yetkisi vardır. Dolayısıyla, bilgiden en etkin şekilde yararlanabilmek için yeni düşünce ve davranış şekilleri geliştirmek gerekir.

Askeri olmayan bilgi sistemlerine örnek:

-- ABD ve ev sahibi ülkenin posta, telgraf ve telefon şebekeleri.

-- Ticari haberleşme ve uluslararası denizcilik uydu sistemleri (INTELSAT, INMARSAT).

-- GPS veya benzeri küresel konumlama sisteminden yararlanan haberleşme sistemleri.

-- Bilgi sistemlerini destekleyen elektrik dağıtım şebekeleri.

-- Ticari olarak geliştirilmiş yazılımlar.

-- Kamuya açık veritabanları ve bültenler.

> 1996 tarihli bu IO doktrininde internet ve bilgi sistemlerinin kontrol ettiği tesisler ilgi çekmiyor, henüz.

Askeri olmayan sistemlerin yaygınlaşması askeri kullanıcılara birtakım zorluklar da getirmektedir: Bilgi sistemleri teknolojisi hızla gelişirken eski ve yeni teknoloji aynı anda kullanılıyor. Yanı sıra, hazır ticari ürünler gittikçe yaygınlaşıyor. Öte yandan, elektromanyetik tayfın kullanımı gittikçe sınırlanıyor.

Geleceğin harekâtlarının yürütülmesinde tüm bu zorlukların üstesinden gelebilmek, bilgi sistemlerinden azami yarar sağlayabilmek için işinin ehli, kalifiye askerler ve liderlere ihtiyaç var.

°°° Bilgi Eylemleri

Bilgi harekâtının (IO) yürütülmesinde altı kritik eylem söz konusudur: Bunlar, bilgiyi ***elde etmek***, ***kullanmak***, ***korumak***, ***faydalanmak***, ***esirgemek*** ve ***yönetmek*** olarak listelenebilir. Birlikte ve kesintisiz ve etkin uygulandığında bu kritik eylemler komutanın insani becerisine katkıda bulunmakta, karar sürecini hızlandırmakta, bilinmezliği gidermekte, durum farkındalığını artırmakta ve böylece muharebe gücünü odaklamasına yardımcı olmaktadır.

°°°° Elde Etmek

Komutan, elde etmek için kaynaklarını tahsis etmeden evvel ihtiyacı olan bilgi hakkında fikir sahibi olmak amacıyla şu soruları sormalı:

-- Ne (hangi) bilgi gerekiyor?

-- Ne tür bilgi gerekiyor?

-- Ne şekilde elde edilebilir?

°°°° Kullanmak

Bilgi, toplanıp analiz edildikten ve harmanlandıktan sonra durum farkındalığını doğrulamak ve güncellemek üzere kullanılır. Bu sayede, süregiden harekât, mevcut planlar ve kararlar gözden geçirilir.

°°°° Korumak

Bilgi ve bilgi teknolojilerinin yaygınlaşması bir avantaj olduğu kadar ciddi tehlike oluşturmaktadır. Asker ve teçhizatın yanı sıra bilgi ve bilgi sistemlerinin de korunması hayati önem taşımaktadır. Dost kuvvetlere ait bilgi ve bilgi sistemleri mutlaka korunmalı; bu amaçla, zaafları incelenmeli ve düşmanın elektronik harp, aldatma,, propaganda, tahrip yöntemleri kullanarak uyguladığı C^2 saldırılarına karşı kuvvetlendirilmelidir.

Bir silah sisteminin çalışmasını engellemek için düşman bu silahın bilgi sistemine saldırabilir. Mesela, bilgi sistemine herhangi bir girişten zararlı yazılım kodu gönderebilir. Askeri bilgi ortamının bu tür saldırılara karşı korunması komuta ve kontrol harbinin (C^2W) kapsamındadır. (C^2-koruma) Küresel bilgi ortamı ile olan bağı, C^4I sistemlerini saldırıya açık hale getirmektedir. Dolayısıyla, küresel bilgi ortamının harekâtın gidişatını ve sonucunu etkileme potansiyeli göz ardı edilemez. Bu sebeple, bilgi ve bilgi sistemleri, etkin çalışmayı engellemeyecek şekilde, elektronik, insani ve fiziki boyutta korunmalıdır. Ancak her zaman, her şeyi tamamen korumak mümkün olamaz. Komutan bu hususta bir tehdit değerlendirmesi yapmak ve korunması gereken önemli bilgi ve bilgi sistemlerini belirlemek durumundadır. Korunması gereken altyapı unsurları arasında bilgisayarlar, haberleşme sistemleri ve destek tesisleri sayılabilir.

Bilgisayar ve haberleşme sistemlerini düşmanın saldırısından korumak sadece bir ilk adım olmalı. Komutan, bunun yanı sıra, düşmanın propaganda ve yanıltma çabalarına karşı da hazırlıklı olmalı. Yeterli kaynaklara sahip bir düşman, propaganda ve yanıltma sayesinde komutanı ve kurmaylarını belirli bir yönde karar almaya ve hareket etmeye sevk edebilir.

Oldukça karmaşık ve kırılgan bir yapıda olan bilgi sistemleri, düşman saldırısı olmasa dahi, başka sebeplerle bozulabilir; bu sebeple harekât, bilgi altyapısının zarar göreceği veya görmüş olabileceği göz önüne alınarak planlanmalı ve yürütülebilmeli.

°°°° Faydalanmak

Faydalanmak, askeri harekâtın başarısı için eldeki bilgiden mümkün olduğunca istifade etmek, çıkar sağlamak şeklinde tanımlanabilir.

> "Faydalanmak" eyleminin nüanslarını açıklamak gerekir. ABD IO doktrininde İngilizce "exploit" olarak yer alan tabir, kullanmanın ötesinde, istifade etmek, faydalanmak, yararlanmak, sömürmek, kötüye kullanmak veya suiistimal etmek anlamına gelir. Ancak, eylemin ayrıntılı açıklamasında belirtildiği gibi, burada daha ziyade avantaj elde etmek, çıkar sağlamak, hatta istismar etmek anlamında fayda sağlamak söz konusudur.

Bir harekâtı çevreleyen dost, düşman, askeri veya sivil tüm bilgi ortamları faydalanmaya açık fırsatlar sunmaktadır. Genellikle haberi olmadan düşmanın bilgi sisteminden bilgi almak şeklinde gerçekleştirilen faydalanma eyleminin derecesi duruma ve amaca göre değişebilir. Mutlaka düşmanın C^2 becerisini zayıflatmak, bilgi sistemine veya kullanmakta olduğu bilgiye zarar vermek şart değil. Barış zamanından itibaren başlatılan bilgi toplama, istihbarat faaliyeti sayesinde, personel, tesisler, sensörler,

işlemciler, karar mekanizması gibi, düşmanın bilgi altyapısı hakkında bilgi sahibi olmak ve değerlendirmek gerekmektedir.

Değerlendirme sürecinde şu soruya da cevap aranır: düşman, bilgi ihtiyacı için küresel bilgi ortamına ne denli bağımlı? Düşmanın bu ortamdan elde edeceği bilgiyi manipüle edebilmek için küresel bilgi ortamı içerisindeki medya, devlet kurumları, sivil toplum örgütleri ve yabancı devletler ile nasıl ilişki kurulabileceği belirlenir.

Faydalanma eylemi sonucu elde edilen istihbarat vasıtasıyla C^2W planlamasına ve özellikle yanıltma, psikolojik harekât (PSYOP) ve fiziki imha operasyonlarına destek sağlanır.

° ° ° ° Esirgemek

IO doktrininde yer alan "deny" eylemi, "yadsımak" veya "reddetmek" veya "inkâr etmek" hatta "kaçınmak" diye tercüme edilebilir; ancak, bilgi harekâtı kapsamında kastedilen daha ziyade "esirgemek" gibi -geçişli fiil- anlamıdır. Amaç, bilgiye düşmanın erişimini engellemek, yani esirgemektir. Bilgi, düşmanın kullanımından esirgenmektedir.

Bilgi harekâtında taarruzun hedefi düşmanın kendi sahip olduğu bilgi ve bilgi sistemlerini etkin şekilde kullanmasını engellemektir. Bu amaçla, düşmanın kendi sahip olduğu bilgiye güveni sarsılır, muharebe alanı algısı köreltilir, komuta kontrol yetisi zayıflatılır. Mesela uydu, hava keşfi, insansız hava aracı vasıtasıyla bilgi elde etmeye karşı elektronik karıştırma (jamming), kamuflaj, yanıltma yöntemleri kullanılabilir. Daha geniş çerçevede uygulandığında, elektronik harbin (EW) yanı sıra psikolojik harekâttan (PSYOP) da yararlanılabilir.

En uygun, optimum faydayı elde edebilmek için çoklu hedeflere karşı "faydalanmak" ve "esirgemek" eylemleri bir arada uygulanmalı ve değerlendirilmeli. Bunu yaparken, göreli faydayı tartmak gerekebilir; yani, düşmanın komuta-kontrol (C^2) becerisine saldırarak ona zarar vermek ile "faydalanmak" yoluyla oradan elde edilebilecek istihbarattan mahrum kalmak veya kendi istihbarat yöntemlerini ve kaynaklarını açığa çıkarmak arasında tercih yapmak söz konusu olabilir.

Sahip olunan istihbarat veya muharebe becerisi otaya çıkmasın diye bilhassa kaybedilen muharebelerin örnekleri çoktur harp tarihinde.

° ° ° ° Yönetmek

Güvenlik, bir yönetim meselesidir, esasında.

Çok boyutlu harekâtın yürütülmesinde bilgi ve bilgi sistemlerinin (INFOSYS) özenli koordinasyonu ve senkronizasyonu elzemdir. Bilgi yönetimi, harekât ihtiyaçları doğrultusunda elektromanyetik tayfın (EMS) yönetilmesini de kapsar. Bu kapsamda; haberleşme, istihbarat, karıştırma, elektromanyetik girişimin çözümlenmesi gibi işlemler, harekât planının önemli bir parçası olarak planlanır ve yürütülür.

Kaynakların ve bilginin etkin yönetimi sayesinde yatay ve dikey akış sağlanır. Bu bilgi akışında bağlanırlık ve esneklik önemlidir. Bağlanırlık, elektronik ve insan bağlantı unsurlarının sürekli faal tutulmasını; esneklik ise bilgi sistemlerinde zayıflama, bozulma meydana geldiğinde gerekli bağlanırlığın ve bilgi akışında sürekliliğin sağlanmasını gerektirir. Bu bağlamda, ticari sistemlere, uydu bağlantılarına veya dost ev sahibi ülkelerin haberleşme şebekelerine çok fazla bağımlı olmak birtakım sınırlamalar getirebilir bağlanırlık veya sürekliliğe.

°°° Beceriler

Bilgi harekâtının (IO) en temel unsuru olan Komuta ve Kontrol Harbinin (C^2W) yürütülmesinde beş temel beceriden yararlanılır ki bu temel (çekirdek) beceriler bilgi harekâtının yapı taşlarını oluştururlar:

-- *Harekât Güvenliği (Operations Security - OPSEC)*
-- *Askeri Yanıltma (Military Deception - MILDEC)*
-- *Psikolojik Harp (Psychological Operations - PSYOP)*
-- *Elektronik Harp (Electronic Warfare - EW)*
-- *Fiziki İmha (Physical Destruction)*

> IO yürütülürken, C^2W temel becerilerinin yanı sıra destekleyici becerilerden de yararlanılır:
> *Sivil İşler (Civil Affairs - CA)*
> *Halkla İlişkiler (Public Affairs - PA)*

°°°° Harekât Güvenliği (Operations Security - OPSEC)

Harekât Güvenliği (OPSEC), esasen, esirgeme (deny) eyleminin yapılandırılmış halidir; düşmanın elde edebileceği ve yararlanabileceği bilginin belirlenmesi ve elde edilmesinin engellenmesidir. Amaç, dost kuvvetlerle ilgili olarak düşmanın faydalanabileceği (exploit) işaretleri, kaynakları ve açıklıkları belirlemek; zararı engelleyecek veya azaltacak tedbirleri almaktır. Günümüz ticari teknolojilerinin düşman için mümkün kıldığı imkânlar harekât güvenliğinin planlanmasını ve uygulanmasını hayli güçleştirmektedir.

> Birinci bölümde bahsi edilen Nasrettin Hoca'nın türbesi OPSEC için sorun olagelmiştir hep.
>
> Yıllar önce, karlı bir kış günü Cumhurbaşkanlığı köşkünün yanından geçen işlek caddede yürürken harika manzaranın resmini çekmek istediğimde nöbetçiler uyarmışlardı. İşgüzar bir güvenlik görevlisi de beni alıkoymaya kalkışmıştı. Telefonda yaşımı soran amirine -o tarihte 48 olan- yaşımı söyleyince, amiri gerek görmemişti. Saçma, hatta komikti. İki gün sonra, bir derginin orta sayfalarında, Cumhurbaşkanlığı köşkünün uydudan çekilmiş, oldukça ayrıntılı kocaman bir fotoğrafı yer almıştı. Birkaç tane dergi satın alıp götürmüştüm güvenlik görevlilerine.

Dünya ölçeğinde bilgiyi nerdeyse gerçek zamanda yayınlayabiliyor olması medyayı düşman için oldukça yararlı bilgi kaynağı haline getirmiştir. Bu durumda, dost

kuvvetlerle alakalı kritik ve hassas bilginin halka açık ortama sızmaması için harekât güvenliği (OPSEC) planlamacıları ile halkla ilişkiler (PA) personeli birlikte çalışmalılar.

> Bu denli yaygın internet ortamında sızmaları engellemek için PA personelinin medya yöneticilerini ikna etmesi çok zor olsa gerek; aslında ikna edecek yönetici de yok ortada.

Harekât güvenliği (OPSEC) aynı zamanda istihbarata karşı koyma (CI), bilgi güvenliği (INFOSEC), iletişim güvenliği (TRANSEC), haberleşme güvenliği (COMSEC) ve sinyal güvenliği (SIGSEC) ile uyumlu olmalı.

°°°° Askeri Yanıltma (Military Deception - MILDEC)

Askeri Yanıltma (MILDEC), dost kuvvetlerin harekâtı, askeri imkânları ve niyetleri hakkında düşmanın karar mekanizmasını yanıltmak ve dost kuvvetlerin lehine olabilecek şekilde hareket etmesini sağlamak amacıyla yürütülür. Dost kuvvetlerin durumu, yeri, gücü, imkânları, hareket yönü, niyeti hakkındaki bilginin düşman tarafından anlaşılamaması veya yanlış anlaşılması için yapılan gizleme, değiştirme, tahrif etme şeklinde yapılır bu yanıltma

> Truva Atı, askeri yanıltmanın bilinen en eski örneklerinden biridir.
>
> İkinci Dünya Savaşının önemli harekâtlarından biri olan Sicilya çıkarması öncesi Müttefiklerin uyguladıkları askeri yanıltma örneği hayli ilginçtir. Almanlar, Müttefiklerin güneyde bir yere çıkarma yapacaklarını tahmin ediyor ama tam yerini bilmiyorlardı. Sardunya, Sicilya veya Yunanistan muhtemel çıkarma bölgeleriydi. Ancak Güney Avrupa sahilinin her yerine yığınak yapmaları mümkün değildi. Her türlü vasıta ve imkânı seferber ederek çıkarmanın yapılması ihtimalinin en yüksek olduğu yeri tespit etmeleri ve kuvvetlerini o bölgede yoğunlaştırmaları gerekiyordu Almanların. Müttefikler ise, çıkarmayı en az kayıpla ve başarıyla gerçekleştirebilmeleri için Alman kuvvetlerinin mümkün olduğunca seyrekleşmesini, çıkarma yapacakları yerden uzaklaşmasını istiyorlardı. Müttefikler aslında Sicilya'ya çıkmayı planlıyorlardı; dolayısıyla, Almanları diğer olası hedeflere yönlendirmeleri gerekiyordu. İngiliz Kraliyet Donanması'ndan Binbaşı Ewen Montagu muhteşem bir planla çıkageldi: Bir ceset, İngiliz subay üniforması giydirilip, çantasındaki sahte, yanıltıcı belgelerle beraber Almanların bulabileceği sulara bırakılacaktı. Nisan 1943'te morgdan aldıkları bir ceset için İngiliz Kraliyet Deniz Piyadesi Binbaşı William Martin kimliği oluşturdular ve cesede üniforma giydirdiler. (Ewen Montagu anılarında, donmuş bir cesede asker postalı giydirmenin nasıl da zor olduğunu ve üstesinden nasıl geldiklerini anlatır, saygıyla ve üzülerek.) Genelkurmaydan Sir Archibald Nye tarafından Kuzey Afrika'daki General Alexander'e hitaben kaleme alınmış, çıkarmanın Sardunya veya Yunanistan'a yapılacağına dair kesin olmayan imalar içeren, Kişisel ve Çok Gizli ibareli bir mektup ve başka rutin evrak dolu bir kurye çantasını bileğine kelepçelediler. Üniformasının iç cebine biraz bozuk para, birkaç banknot, bir kutu kibrit, bir paket sigara, kurşun kalem, ev anahtarları, birkaç fatura -ki bir tanesi de nişan yüzüğü faturasıdır- kimlik kartları ve sahte nişanlısının fotoğrafı ile mektubunu koydular. İnandırıcılığı artırmak için, İngiltere'den Kuzey Afrika'ya uçakla gidiş dönüş süresini de dikkate alarak, Sir Prince of Wales' tiyatrosundaki Sid Fields gösterisine ait kullanılmış iki bilet koymayı da ihmal etmediler. Her şey hazırıdır; Genelkurmaydaki

üst yetkililer onay vermiştir ancak Başbakan'ın onayı gerekmektedir. Planın sunumu sırasında olası riskler konuşulurken, başarısız olduğu takdirde Almanların artık Sicilya'dan kesinlikle emin olacakları riski bulunduğu söylendiğinde Chuchill, "Hiç önemli değil, nasıl olsa en aptal insan dahi Sicilya olacağını bilir," diyerek onay verir. İngiliz denizaltısı Seraph'ın güneybatı İspanya açıklarında bıraktığı Binbaşı Martin'in cesedini İspanyol balıkçılar buldu ama gerisini Alman askeri istihbaratı halletti. Alman yüksek komuta heyeti çıkarmanın Sicilya, Sardunya, Korsika ve Yunanistan'a yapılacağına hükmetti. Kuvvetler dağıtıldı, Sardunya ve Korsika kıyılarındaki tahkimat kuvvetlendirildi, Yunanistan açıklarına mayın döşendi, panzer ve piyade birlikleri kaydırıldı. Temmuz'da Sicilya çıkarması başladığında Almanlar önceleri inanmadılar. İşte, morgdaki isimsiz bir ceset üzerinden yürütülen başarılı bir askeri yanıltma (MILDEC) operasyonu...

Bir sene sonra, Almanların yine inanamadıkları bir başka askeri yanıltma operasyonunu Normandiya çıkarmasının hemen öncesinde gerçekleştirdi Müttefikler. Bu sefer Almanlar oldukça emindiler çıkarmanın kuzey Fransa'da Kale sahillerine (Pas-de-Calais) yapılacağından. Sebepleri vardı: birincisi, İngiltere ile kıta Avrupa'sı arasındaki en dar boğaz, en kısa geçişti; ikincisi ve en önemlisi, Hitler öyle olacağına inanıyordu. Müttefikler de tabii ki bu inancı destekliyorlar, ellerinden geldiğince kuvvetlendirmeye çalışıyorlardı. Çıkarma gemileri Normandiya'ya doğru yola çıktığında Müttefikler çok etkin elektronik harp (EW) uygulamaya başladılar Alman radarlarına karşı. Uçaklar tarafından bırakılan chaff bulutları Alman radarlarının görüşünü engelliyordu ama Almanlar bunu zaten bekliyorlardı, hatta alışkındılar. Gerekli tedbirleri (ECCM) aldıklarında gördüler ki bir sürü küçük tekne sekiz deniz mili süratle Kale'ye doğru seyir halinde. Müttefikler bir şey daha yapıyorlardı Alman radar sinyallerini yansıtan chaff bulutunun arkasından. Alman radar operatörleri, chaff bulutunun yarattığı karartmanın arkasında küçük teknelerle birlikte 10.000 tonluk büyük gemilerin olduğunu zannettiler. Tabii ki Kale ile ilgili tahminlerini destekleyen bu bulguya inanmaya hazırdılar. Müttefiklerin küçük teknelerindeki hoparlörlerden gelen, daha önce Salerno çıkarmasında kaydedilmiş gerçek çıkarma sesleri, emirler, bağırışlar da yardımcı olmuştur muhakkak. Sonuçta, Normandiya büyük sürpriz oldu Almanlar için. İşte bir başka başarılı askeri yanıltma (MILDEC) ve elektronik harp (EW) ortak operasyonu...

Bu operasyonlarda başarılı planlama ve yürütmenin yanı sıra şans ve rastlantı da önemli rol oynamıştır. Müttefikler Normandiya çıkarmasının hazırlıklarını çok ileri seviyede gizlilikle yaparken hemen her şey için kod adları kullanıyorlardı. Mesela; Utah ve Omaha, Amerikan tümenlerinin çıkarma yapacakları sahillerin kod adlarıydı; Juno, Gold ve Sword ise İngilizlerin. Mulberry, çıkarmada kullanılacak yüzer limanın kod adıydı. Neptune, deniz taarruzunun, Overlord ise tüm çıkarma harekâtının kod adıydı. Çıkarmadan yaklaşık iki sene önce, 1942 ağustosunda bir gün, İngiltere'de yayınlanan Daily Telegraph gazetesinde yer alan çapraz bulmacanın çözümü içerisinde bir kelime, Fransa'da bir liman kenti olan Dieppe idi. Birkaç gün sonra, 19 Ağustos'ta Müttefikler ağır bir bozguna uğradılar Dieppe muharebesinde. Bu rastlantı tabii ki İngiliz Savaş Bakanlığı'nın dikkatinden kaçmamıştı. Surrey'deki bir okulun müdürü Leonard Dawe tarafından hazırlanmıştı söz konusu bulmaca. İngiliz istihbaratının

Chaff (Saman) (İkinci Dünya Harbindeki kod adı "window") Radar alıcısını yanıltmak için kullanılan, sinyal yansıtıcı özelliğe sahip ince alüminyum şeritler.

yaptığı araştırma, bunun basit bir rastlantı olduğu şeklinde sonuçlanmıştı. 1944 mayısında -çıkarmanın planlanan tarihinden birkaç ay önce- yine aynı gazetede yer alan ve yine Leonard Dawe tarafından hazırlanmış olan bir bulmacanın cevapları içerisinde Utah vardı; birkaç gün sonrakinde de Omaha. Mayıs sona ermeden Overlord ve Mulberry de çıkmıştı. Haziranın ilk günü Neptune yer alınca bulmacada, beş gün sonra çıkarma yapmayı planlayan Müttefikler neredeyse iptal edeceklerdi harbin bu en önemli harekâtını. İki yıl önceki Dieppe rastlantısını hatırlayan İngiliz istihbaratı tarafından sorgulandı Leonard Dawe ama rastlantı ihtimalinin dışında herhangi bir bulgu elde edilemediği için serbest bırakıldı. Ancak yıllar sonra, kesin olmayan birtakım bağlantılar çıktı ortaya. İşte bu da başarısız bir harekât güvenliği (OPSEC) örneği...

°°°° Psikolojik Harekât (Psychological Operations - PSYOP)

Yabancı muhatapların duygularını, güdülerini, objektif muhakemelerini ve nihayetinde yabancı kişilerin, grupların, kurumların ve hükümetlerin davranışlarını etkilemek için yapılan operasyonlar olarak tanımlanır psikolojik harekât (PSYOP). Yabancıların davranışlarını harekâtı yürüten tarafın menfaatine olacak şekilde yönlendirmektir amaç.

Diğer tanımlardan farklı olarak, psikolojik harekât (PSYOP) tanımında özellikle yabancı vurgusu yapılıyor olması dikkatli okurun dikkatinden kaçmamıştır, muhakkak. 1996 tarihli bu dokümanda açıkça belirtmeden ima edilse de daha sonraki tarihlerde yayınlanan IO doktrinlerinde özellikle belirtilmektedir ki ABD silahlı kuvvetleri ABD toprağında ve ABD vatandaşlarına karşı psikolojik harekât uygulayamaz, kesinlikle. Devletin kendi vatandaşına gösterdiği saygıdır bu.

Psikolojik harekât unsurları diğer C^2W unsurlarıyla ve PA stratejistleriyle yakın çalışmalı.

Gerek C^2-taarruz, gerekse C^2-koruma operasyonlarında yanıltma ve psikolojik harekâta sık başvurulur. C^2-korumada PSYOP sayesinde düşmanın Amerikan kuvvetlerine karşı yürüttüğü dezenformasyon ve olumsuz propagandanın etkisi azaltılır. Öte yandan, PSYOP sayesinde Amerika'nın teknolojik üstünlüğü, imajı büyütülür.

1991-1996 yılları arasında ABD ve müttefiklerinin Türkiye'nin güneydoğusu ve Irak'ın kuzeyinde yürüttüğü Huzur Harekâtı (Operation Provide Comfort) süresince beş milyondan fazla psikolojik harekât (PSYOP) ürünü kullanılmış olduğunu belirtmiştir, General Shalikashvili.

Hazır yemek ve süt dağıtarak imaj yaratmayı anlıyorum ama Türkiye'de ve bölgede, hatta tüm dünyada meydana gelen hemen her şeyin altında Amerika'yı aramak adeti de acaba böylesi bir psikolojik harekât sonucu mu gelişti diye düşünmeden edemiyorum. Bölgemizde çok yaygındır her olumsuzluğun ardında Amerika Birleşik Devletleri veya İsrail ilişkisi aramak. Aslında tarih ve güncel durum bunu destekler; hatta böylesi ilişki ipuçları bulunabilir de. Bu algının sonucu olarak bu ülkeler bilinçli veya bilinçsiz birçok saldırının hedefi olmaktalar. Nihayetinde, bu durum bir başka çok önemli algı daha yaratmaktadır kamuoyunda ABD ve İsrail lehine: sanki her şeye muktedirlermiş gibi. Kendine karşı olanların söylemlerinden faydalanarak kendi lehine psikolojik harekât yürütmek de akıllıca bir yöntem olsa gerek. Ne var ki bilmeden

-veya bilerek- bu psikolojik harekâtın aleti olup, gerçekte olmayan güç ve beceriyi öne çıkaranlar hayli fazladır.

Psikolojik harekât hemen her seviyede komutan veya liderle komuta ettikleri askerler veya halk arasında -tabir yerindeyse- bir oduncu kaması gibi kullanılabilir. Lidere olan güveni azaltacak propaganda sayesinde liderin etkinliği azaltılarak komuta-kontrol veya yönetim bağı kopartılır.

°°°° Elektronik Harp - EH (Electronic Warfare - EW)

Elektromanyetik ve yönlendirilmiş enerji vasıtasıyla elektromanyetik tayfı denetlemek veya düşmana saldırmak olarak tanımlanmaktadır elektronik harp (EW). Elektronik taarruz (EA), elektronik savunma (EP) ve elektronik harp desteği (ES), elektronik harbin temel alt kırılımlarıdır.

-- Elektronik Taarruz (Electronic Attack - EA), karıştırma, elektronik yanıltma, yönlendirilmiş enerji kullanarak düşmanın elektromanyetik tayfı (EMS) kullanmasını engeller veya zayıflatır. Elektronik taarruz, düşmana karşı taktik formasyondan ulusal altyapıya kadar her seviyede uygulanabilir.

-- Elektronik Koruma (Electronic Protection- EP), dost kuvvetlerin elektromanyetik tayfı kullanmasını temin eder. Düşmanın hedef tespitini ve angajmanını zorlaştırarak dost kuvvetlerin zarar görmesini engeller. Bu bağlamda, elektronik koruma (EP) yaşamsaldır.

-- Elektronik Harp Desteği (Electronic Warfare Support - ES), tehditleri algılayabilmek için istemli veya istem dışı elektromanyetik radyasyon kaynaklarını arama, kestirme, belirleme ve yerini bulma faaliyetlerini içerir.

°°°° Fiziki İmha (Physical Destruction)

Düşman kuvvetlerini veya tesislerini etkisiz kılmak için uygulanan muharebe gücü -kara, deniz hava saldırıları ve özel kuvvetler- vasıtasıyla fiziki imha gerçekleştirilir.

Düşmanın C^2 hedeflerinin imhası, komuta ve kontrol becerisinin bir süreliğine zayıflatılması veya gerekiyorsa tamamen ortadan kaldırılması anlamına gelir. Fiziki imha yöntemine ancak kapsamlı bir değerlendirmeden sonra başvurmak gerekir.

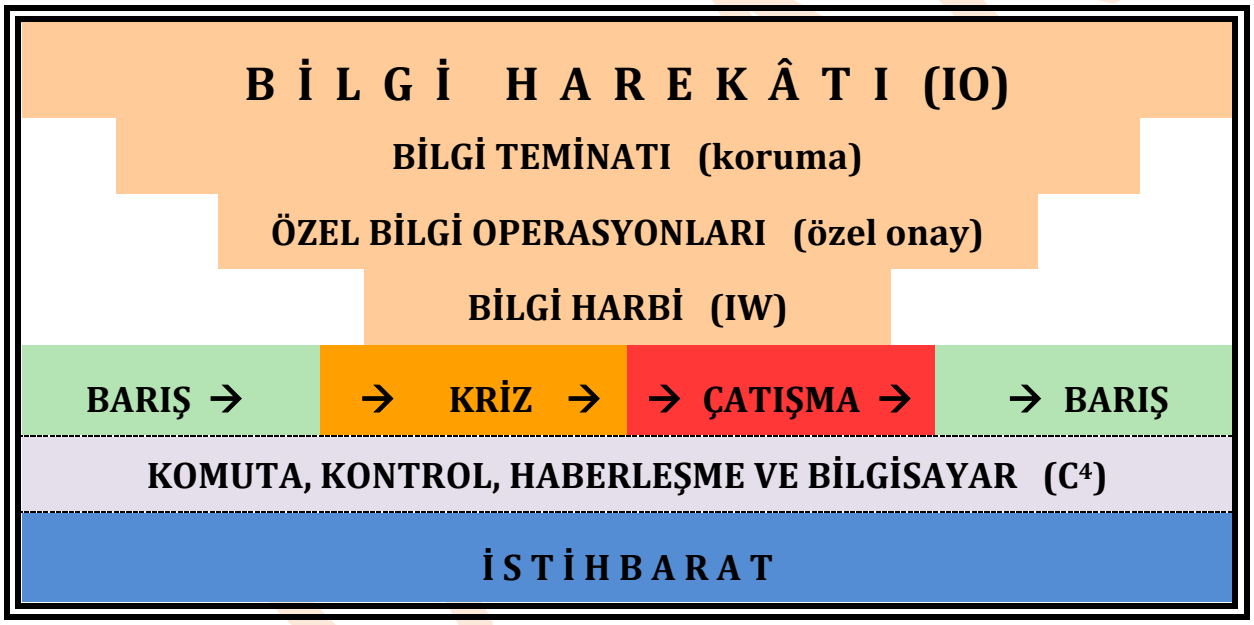
> 14 Nisan 1943 günü ABD istihbaratı, Japon deniz kuvvetleri baş komutanı Amiral Isoroku Yamamoto'nun dört gün sonra Pasifik'teki Bougainville adasına uçacağı haberini aldı. Askeri yeteneklerinin yanı sıra Amiral Yamamoto'nun bilinen bir özelliği, dakikliğe önem vermesi ve kendisinin de çok dakik olmasıydı. Bu yüzden, Müttefik harekât planlamacıları emindiler Yamamoto'nun uçağının 18 Nisan günü, saat 16:39'da Bougainville semalarında olacağından. Guadalcanal'daki ABD üssünden havalanan on altı adet P-38 için kolay bir avdı Amiral Yamamoto'nun uçağı. Böylece, Japon deniz kuvvetlerinin komuta ve kontrol merkezi tam kalbinden, hatta beyninden vurulmuş oldu. İşte, rutin davranışın, dakikliğin, düzenin istihbarat toplayan için ne denli kıymetli olduğunun örneği…

1998 - ABD MÜŞTEREK IO DOKTRİNİ

1996 tarihli ABD Kara Kuvvetleri sahra talimnamesi FM 100-6 Information Operations başlığıyla yayınlanan ABD bilgi harekâtı doktrini, 1998'de ABD Genelkurmayı'nın ortak yayını, Joint Pub 3-13 Joint Doctrine for Information Operations, yani Müşterek Bilgi Harekâtı Doktrini başlığıyla yayınlanmıştır. Önsözünde dönemin ABD Genelkurmay Başkanı, tüm kuvvetlerin ortak bilgi harekâtından bahisle, bu dokümanın bir ortak doktrin olduğunu ifade etmektedir.

° Esaslar

Bilgi Harekâtı (IO) ve Bilgi Harbi (IW) -daha önceki 1996 doktrininde olduğu gibi- kendi bilgi ve bilgi sistemlerini korurken düşmanın bilgi ve bilgi sistemlerini etkilemek olarak tanımlanmaktadır. Özellikle kriz ve çatışma döneminde etkin olarak uygulanan bilgi harekâtı (IO) eylemleri ise bilgi harbi (IW) olarak adlandırılmaktadır.



Bilgi harekâtının (IO) başarısı için haberleşme ve istihbarat desteğinin gerekliliği, özellikle istihbaratın önemi vurgulanmaktadır.

Bilgi harekâtı, **taarruz amaçlı (offensive)** ve **müdafaa amaçlı (defensive)** olmak üzere temelde ikiye ayrılmakla birlikte her ikisinin de koordineli bir şekilde kullanılması gereği vurgulanmakta; müdafaa amaçlı bilgi harekâtının her zaman, taarruz amaçlı bilgi harekâtının ise -taktik veya stratejik- savaşın her seviyesinde kullanılabileceği belirtilmektedir.

Bilgi harekâtı uygulamalarının karmaşık hukuk ve politika meseleleri içerebileceği, dolayısıyla, ulusal seviyede koordinasyon ve onay gerektirdiği hatırlatılmaktadır. Muharip komutanların uygulamalarının bölgesel istikrara veya ABD'nin ulusal

çıkarlarına, hatta güvenliğine zarar verebileceği ihtimali göz önünde bulundurulmalıdır. Bilgi harekâtı uygulamalarında yerel ve uluslararası sulh ve ceza hukuku ve uluslararası anlaşmaların yanı sıra ABD istihbarat kuruluşları ile resmi ve gayri resmi diğer kuruluşlar arasındaki ilişkiler de dikkate alınmalıdır.

> 1998 doktrininde bilgi harekâtı (IO), askeri amaçların ötesine, milli strateji seviyesine taşınmıştır.

Stratejik bağlamda bilgi harekâtı (IO), milli amaçlar uğruna muhtelif becerilerin ve eylemlerin entegre edilmesini gerektirir; dolayısıyla, diğer devlet kurumları ile yakın koordinasyon içerisinde yürütülmek durumundadır.

Barışta veya krizin erken döneminde bilgi harekâtının caydırıcı, hatta krizi tamamen giderici etkisi olabilir.

Müdafaa amaçlı (defensive) bilgi harekâtı her zaman, uygulanmak durumundadır; taarruz amaçlı (offensive) bilgi harekâtı ise görevin gerektirdiği durumlarda uygulanır.

> Tabii ki görevin tanımına göre durumlar esnek olabilir; zira doktrinin taarruz amaçlı bilgi harekâtı ile ilgili bölümünün girişinde şöyle deniyor:
>
> "**İlk vur; sert vur; hep vur.**" Amiral Sir John Fisher

1998 tarihli doktrinde bilgi harekâtını yürüten çeşitli kurumların liderlerinin -tasnif dışı- görev tanımları verilmektedir. Bunlar: Genelkurmay Başkanı, muharip komutanlar, kuvvet komutanları, Özel Kuvvetler Komutanı, Ulusal Güvenlik Ajansı (NSA) Direktörü, Savunma İstihbarat Ajansı (DIA) Direktörü, Savunma Bilgi Sistemleri Ajansı (DISA) Direktörü, Müşterek Komuta ve Kontrol Harbi Merkezi (JC2WC) Direktörü, Müşterek Harp Merkezi Direktörü, tüm Savunma Bakanlığı (DoD) unsurları.

> Bu kadar farklı kurum, kuruluş, teşkilat, ajans, komutan, direktör, lider, sorumlu, kısaltma, harf grubu… Sonuç, muazzam bir karmaşa!.. Yine de çok bilinen bir harf grubu eksik. Her ne kadar stratejik seviyeye taşınmış olsa da bilgi harekâtı uygulayan kuruluşlar arasında Merkezi Haberalma Teşkilatı (CIA) yer almamaktadır. İnandırıcı mı? Değil. Herhalde, doktrini hazırlayan askeri otorite araya mesafe koymak istemiş olsa gerek. Kozmetik bir çaba...

Gittikçe karmaşıklaşan bilgi sistemleri muharip kuvvetlere entegre edilmektedir; ancak, bu sistemler özde hayli kırılgandırlar. Sistemler ucuzladıkça ve yaygınlaştıkça daha çok kullanılmakta; dolayısıyla, kırılganlık da yaygınlaşmaktadır. Bu sebeple, gelişmiş bilgi sistemleri çift taraflı bıçak gibidir. Amerika'nın bilgi ve bilgi sistemlerine olan ileri derece bağımlılığı onu çok geniş yelpazede tehditlere maruz bırakmaktadır.

> Bilgi harbini sadece Amerika'ya özgü bir avantaj olarak görmek doğru olmaz.

Tutarlı bir bilgi harekâtı (IO) stratejisi için birçok farklı beceri uyumlu şekilde, birlikte kullanılmalıdır. Bilgi harekâtının ileri düzeyde uzmanlık gerektiren beceriler içerdiği düşünülebilir; ancak geçtiğimiz yarım yüzyılı aşkın sürede görüldü ki kullanılan araçların teknik özelliklerindeki gelişme insan becerisini gittikçe geri plana atmaktadır.

Bu sayede, on altı yaşında bir genç, askeri ve sivil bilgi sistemlerinin içinde cirit atabilmekte, çok tehlikeli sonuçlara yol açabilmektedir. Geçmişte oldu; gelecekte de olacak. Kaçınılmaz; ancak, tedbir alınabilir...

° Taarruz Amaçlı Bilgi Harekâtı

Savaşın her aşamasında, görev hedeflerine ulaşabilmek için taarruz amaçlı bilgi harekâtı kullanılabilir.

Görevin hedefi, görevin gereği ve benzer gerekçeler olduğu sürece bu tanım pek anlam ifade etmemektedir. Nihayetinde, görev gereği bahanesiyle her zaman, her fırsatta saldırı amaçlı bilgi harekâtı uygulanabilir.

°° Prensipler

Karar verici kişilerin karar mekanizması, taarruz amaçlı bilgi harekâtı için en üst hedeftir.

Harbin hedefi komutanının zihnidir, askerlerin bedenleri değil.

Sir Basil Liddell Hart

Taarruz amaçlı bilgi harekâtı esas harekât olabileceği gibi bir başka harekâtı desteklemek amacıyla da yürütülebilir veya Savunma Bakanlığı haricinde birimler tarafından planlanabilir veya uygulanabilir.

Yöntemlerin seçimi ve uygulanması, mevcut durum ve ABD'nin amaçlarıyla uyumlu; eylemler, ulusal ve uluslararası kanunlar ve askeri kurallara uygun olmalı ve gerekli müsaadeler mutlaka alınmalı.

Taarruz amaçlı bilgi harekâtının amaçları önceden belirlenmiş olmalı, amaçlara ulaşmak için hedefler belirlenmeli, en etkin yöntemler seçilmeli, belli bir güvenilirlikle olası sonuçlar tahmin edilmeli, harekât icra edildikten sonra sonuçlar değerlendirilmeli.

°° Beceriler

Taarruz amaçlı bilgi harekâtı, OPSEC, PSYOP, MILDEC gibi algıda yanıltı yaratacak eylemlerin yanı sıra bilgi sistemlerine yönelik EW ve fiziki imha eylemlerini de içermektedir

Becerinin gerektiği yerde kuvvete yer yoktur. Herodot

Harekât güvenliği (OPSEC) sayesinde niyet ve hazırlık eylemleri hakkında düşmanın bilgi edinmesi engellenir. Dolayısıyla, çok erken aşamalardan itibaren uygulanması gerekir.

Psikolojik harekât (PSYOP) ile yabancı muhataplara, onların hislerini, muhakemelerini, güdü ve davranışlarını etkileyecek seçilmiş bilgi ve işaretler aktarılır. Düşmanın geri çekilmesini veya teslim olmasını sağlamak amacıyla operasyonel

seviyede televizyon ve radyo yayınları, sesli anonslar veya broşürler vasıtasıyla uygulanan PSYOP, stratejik seviyede ise politik ve diplomatik mesajlarla uygulanır. PSYOP elemanları bire bir görüşmeler yoluyla da arzu edilen etkiyi sağlayabilir.

Askeri yanıltma (MILDEC) ile düşmanın istihbarat toplama, değerlendirme ve dağıtma sürecinden faydalanarak onun komuta ve karar verme mekanizması hedeflenir ve yanıltılır. Düşmanı yanıltmanın, kesin olmayan bilgi ile doğru karar vermesini zorlaştırmanın ötesinde esas amaç onu arzu edilen davranışa yönlendirmek olmalıdır. MILDEC eylemlerine destek amacıyla PSYOP ve istihbarattan yararlanılabilir. Bu denli önemli olan MILDEC çok iyi planlanmalı, özenle uygulanmalı ve inandırıcı olmalı.

> Savaş, tamamen yanıltma üzerine inşa edilir. Sun Tzu

Elektronik harp (EW), hem taarruz hem de savunma amaçlı bilgi harekâtına katkıda bulunmaktadır. Elektronik harp, üç ayrı şekilde uygulanabilir:

-- Elektronik taarruz (EA), elektromanyetik tayfın düşman tarafından etkin şekilde kullanmasını engellemek için yürütülen eylemlerdir.

Elektronik koruma (EP), dost veya düşman kuvvetlerin uygulamakta olduğu elektronik harp yöntemlerinin dost kuvvetlerin savaş yeteneğine zarar vermesini engellemek amacıyla yürütülen kendini koruma (self protection), karıştırma (jamming), veya yayın denetimi (emission control) eylemlerini içermektedir.

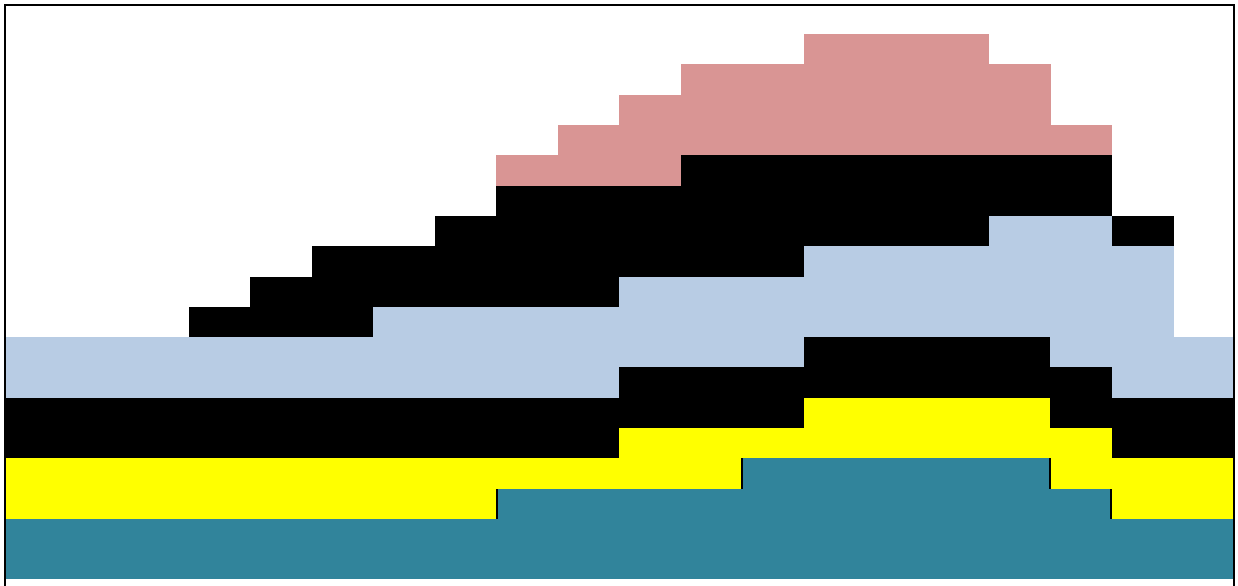
> Yayın Denetimi (Emissions Control - EMCON), aynı zamanda elektromanyetik sessizlik veya radyo suskunluğu olarak da bilinir.
>
> Japon uçaklarının Honolulu'daki bir yerel radyo istasyonunun yayınını izleyerek Pearl Harbor baskınını gerçekleştirdikleri hatıra getirildiğinde önemi daha da anlaşılır...

Elektronik harp desteği (ES), bilerek veya bilmeyerek yayınlanan elektromanyetik enerjinin algılanması sayesinde tehditlerin tanımlanması ve yerlerinin belirlenmesidir.

Elektronik ortamda dost kuvvetlerin zarar görmemesi için, komuta kademesi, EW ile diğer IO istihbarat ve haberleşme destek aktiviteleri arasında azami koordinasyonu sağlamalıdır. Bu koordinasyon, aynı zamanda olası duplikasyonu da önler.

Fiziki imha, belirlenmiş hedeflere karşı uygulanan vurucu, imha edici, öldürücü eylemlerdir.

Savaş sürecinde, bilgi harekâtında uygulanan becerilerin zaman içerisinde kullanımı şöyle gösterilebilir:



→ BARIŞ	→ KRİZ →	→ ÇATIŞMA →	→ BARIŞ

İ S T İ H B A R A T

KOMUTA, KONTROL, HABERLEŞME VE BİLGİSAYAR (C⁴)

	OPSEC ve MILDEC			Fiziki taarruz ve imha
	Diğer beceriler			EW
	Bilgi teminatı			PSYOP

Taarruz amaçlı bilgi harekâtının icrasında OPSEC, PSYOP, MILDEC, EW ve fiziki imza gibi beş temel beceriye ilaveten, PA ve CA gibi destekleyici becerilerden de yararlanılır.

PA sayesinde doğru ve zamanında bilgi iç ve dış muhataplara aktarılır, kendilerini ilgilendiren önemli gelişmelerden haberdar edilirler.

CA ise, dost veya tarafsız veya düşman bölgedeki komutanın, kendi kuvvetleri ile sivil otorite, kurumlar ve halk arasındaki ilişkiyi tesis etmesi amacıyla yürütülen eylemlerdir. Sivil-Askeri Operasyonlar (CMO) çerçevesinde CA ve PSYOP eylemleri birbirini destekler.

> 1998 tarihli ABD Bilgi Harekâtı (IO) doktrininde yer alan, 'Other classified capabilities are outlined in Appendix A, "Supplemental Information Operations Guidance" (published separately)' ifadesinden anlaşılmaktadır ki ABD bilgi harekâtının yürütülmesinde, "gizlilik dereceli" başka becerilere de başvurulmaktadır.

°° İstihbarat ve Bilgi Sistemleri Desteği

°°° İstihbarat Desteği

Taarruz amaçlı bilgi harekâtı için geniş tabanlı, özel istihbarat gerekir. İstihbarat oldukça uzun zaman alan bir faaliyet olduğundan, potansiyel kaynaklar mümkün olduğunca önceden geliştirilmiş olmalı. Bunlar, gizli olabileceği gibi, yerel şahıslar, akademik camia, iş dünyası, medya gibi açık kaynaklar da olabilir. Gerektiğinde, internet, radyo, televizyon veya basılı yayınlardan da yararlanılır.

Taarruz amaçlı bilgi harekâtı için istihbarat hazırlığı yaparken şu hususlar göz önüne alınmalı:

-- Geniş yelpazede, tüm bilgi sistemlerinin özellikleri.
-- Politik, ekonomik, kültürel ve sosyal etkiler.
-- Düşman veya olası düşmanın karar süreci.
-- Liderlerin, karar vericilerin, danışmanların özgeçmişleri.

°°° Bilgi Sistemleri Desteği

Taarruz amaçlı bilgi harekâtını destekleyecek bilginin toplanması, aktarılması, işlenmesi, dağıtılması ve görünür hale gelmesi bilgi sistemleri sayesinde gerçekleştirilir. Ayrıca, komuta kademesinin küresel bilgi altyapısına (GII) erişimi de bilgi sistemleri vasıtasıyla mümkün olur.

° Müdafaa Amaçlı Bilgi Harekâtı

Müdafaa amaçlı bilgi harekâtı, sahip olunan bilgi ve bilgi sistemlerinin (INFOSYS) korunmasını birbiriyle yakın alakalı dört eylem yardımıyla sağlar. Bunlar: bilgi ortamının korunması, taarruzun tespiti, zarar gören becerinin onarılması ve mukabil taarruz olarak tanımlanabilir.

Bilginin ve bilgi sistemlerinin korunması amacıyla politikaların, prosedürlerin, operasyonların, personelin ve teknolojinin birbiriyle entegrasyonunu sağlayan müdafaa amaçlı bilgi harekâtı; bilgi teminatı (IA), bilgi güvenliği (INFOSEC), harekât güvenliği (OPSEC), elektronik harp (EW), yanıltmaya karşı koyma, istihbarata karşı koyma (CI), karşı propaganda, fiziki güvenlik ve özel bilgi harekâtı (SIO) yöntemleri vasıtasıyla yürütülür ve istihbarat tarafından desteklenir.

> [Arzu edenler, harekât yerine operasyon, müdafaa yerine savunma, muhafaza yerine koruma, taarruz yerine saldırı, mukabil taarruz yerine karşı saldırı, teminat yerine güvence, tedbir yerine önlem, tespit yerine saptama veya belirleme kelimelerini kullanmayı tercih edebilirler veya yeğleyebilirler.]

Burada -bazılarını tekrarlamak pahasına- terimlerin tanımlarını vermek yerinde olur:

Bilgi Teminatı (Information Assurance - IA), bilginin ve bilgi sistemlerinin kullanılabilirliğini (erişilebilirliğini), hakikiliğini (sahihliğini), gizliliğini, bütünlüğünü ve

inkâr edilemezliğini sağlayan; koruma, tespit etme ve tepki gösterme eylemlerini içeren bilgi operasyonlarıdır.

-- **Erişilebilirlik (Availability)**: Yetkili kullanıcıların erişimine açık.

-- **Hakikilik (Authenticity)**: Kaynağı doğrulanabilir.

-- **Gizlilik (Confidentiality)**: Yetkisiz ifşaya karşı korunmuş.

-- **Bütünlük (Integrity)**: Yetkisiz değişikliğe karşı korunmuş.

-- **İnkâr edilemezlik (Non-Repudiation)**: Katkının reddedilemeyişi.

Bilgi Güvenliği (Information Security - INFOSEC), bilginin ve bilgi sistemlerinin, depolama, iletim ve işleme aşamalarında yetkisiz erişim veya değiştirmeye karşı korunması; öte yandan, yetkili erişimin devamlılığının sağlanması amacıyla yürütülen tespit etme, kaydetme ve karşı koyma eylemlerini içerir.

Harekât Güvenliği (Operations Security - OPSEC), kritik önemde bilgiyi tanımlamak, düşman istihbaratı tarafından yürütülebilecek eylemleri saptamak, düşman tarafından anlaşılabilecek veya zaman içerisinde parça parça elde edilerek anlamlı hale getirilebilecek işaretleri belirlemek, düşmanın kötü niyetle faydalanmasına karşı dost kuvvetlerin zaaflarını tespit etmek amacıyla yürütülen bilgi harekâtı şeklidir.

İstihbarata Karşı Koyma - İKK (Counterintelligence - CI), yabancı ülkeler adına veya onların elemanları ve/veya yabancı organizasyonlar, şahıslar veya uluslararası terör örgütleri tarafından yürütülen casusluk, sabotaj, suikast ve benzeri eylemlere karşı bilgi toplama ve önlem alma faaliyetini kapsar.

Elektronik Harp - EH (Electronic Warfare - EW), elektromanyetik ve yönlendirilmiş enerji kullanarak elektromanyetik tayfı kontrol etmek veya düşmana saldırmak amacıyla yürütülen askeri eylemleri içerir.

Fiziki Güvenlik (Physical Security), kişileri ve/veya ekipmanı, dokümanları, tesisleri suikast, sabotaj, hırsızlık, casusluk ve benzeri zarar verici eylemlere karşı korumak amacıyla alınan fiziki önlemleri içerir.

Özel Bilgi Harekâtı (Special Information Operations - SIO), güvenlik gereksinimleri, olası etkileri veya ABD'nin ulusal güvenliğini tehlikeye atma ihtimali gibi hassasiyet içeren ve özel inceleme veya onay süreci gerektiren bilgi harekâtı uygulamalarını tanımlar.

°° Taarruz Amaçlı Bilgi Harekâtı İle Entegrasyon

Dost kuvvetlerin sahip olduğu bilgi ve bilgi sistemlerine yönelik varlığı saptanmış veya olası tehditlere zamanında karşı koyabilmek ve cevap verebilmek için, müdafaa amaçlı bilgi harekâtı ile taarruz amaçlı bilgi harekâtı birbiriyle entegre edilmeli.

°° Diğer Kuvvetlerle Entegrasyon

Müdafaa amaçlı bilgi harekâtının koruma, tespit, onarım ve tepki unsurları arasındaki ilişkinin anlaşılması ve gerektiği şekilde uygulanması için, genelkurmay bünyesinde diğer kuvvetlerle entegrasyonu ve gerektiğinde en uygun kuvvet veya kuvvetlerce harekâtın yürütülmesi sağlanmalı.

°° Çokuluslu Kuvvetlerle Entegrasyon

Çokuluslu harekâtlarda silah sistemleri, bilgi tabanlı teknolojiler ve diğer beceriler genellikle diğer ulusların kuvvetleriyle paylaşılmak ve entegre edilmek durumundadır. Ancak bu durum, harekâtın başarısına destek olduğu kadar zaafa da yol açabilir.

°° Bilgi Ortamının Korunması

Bilgi sistemleri, tesisler ve istihbaratın toplaması, analizi, üretimi, dağıtımı gibi süreçler korunmuş bilgi ortamını meydana getirir. Bilgi ortamı, bilginin içeriği ve koruma standartları ile alakalıdır.

> Savaşta müdafaa, rahat taarruz edebilmek için yapılır.
>
> Tümamiral Alfred Thayer Mahan

Becerilerin tekrar yerine konması ve karşı taarruz için düşmanın bilgi harekât taarruzunun erkenden tespiti elzemdir. Dost kuvvetlerin becerilerinin yenilenmesi ve karşı taarruz için düşmanın -elektronik harp veya askeri yanıltma gibi- becerilerinin tespit edilmesi, anlaşılması ve dost bilgi sistemleri üzerindeki etkisinin değerlendirilmesi gerekir. Bu amaçla, şu bilgi harekâtı unsurlarından yararlanılır:

°°° Elektronik Harp Merkezleri

Elektronik harp merkezleri, bilgi harekâtı taarruzu ile ilgili erken bilgi elde eder, uyarıda bulunur, önleyici ve hasar giderici tedbirleri belirler ve durumu raporlar.

°°° Bilgi Sistemleri Geliştiricileri

Bilgi sistemlerini geliştirenler, bu sistemleri -özellikle otomatik bilgi sistemlerini- teknik veya kullanım zaaflarını giderecek şekilde tasarlamalı. Otomatik bilgi sistemleri (AIS) otomatik tespit, hasarı azaltma ve durumu raporlama özelliklerine sahip olmalı.

°°° Bilgi Sistemleri Tedarikçileri ve Sistem Yöneticileri

Gittikçe gelişen bilgi taarruzu tekniklerine karşı bilgi sistemleri tedarikçileri ve sistem yöneticileri sistemin çalışmasındaki anormallikleri tespit edebilmeli, gereken önlemi alabilmeli, hasarı azaltabilmeli ve durumu raporlamalı. Ayrıca, periyodik olarak risk değerlendirme, tespit ve hasar giderme ile ilgili güncellemeler yapmasını sağlayan bir rutin oluşturmalı.

°°° Bilgi ve Bilgi Sistemleri Kullanıcıları

Kullanıcılar, potansiyel tehditlerin ve bilgi sistemlerindeki zaafların bilincinde ve farkında olmalı; sistemin çalışmasındaki anormallikleri, bilgi içeriğindeki açıklanamaz değişiklikleri fark etmeli, raporlamalı ve gerekli tedbirleri almalı.

°°° Kolluk

Bilgi sistemlerine yönelik saldırılar veya tehlike içeren girişimler askeri kolluk ve karşı istihbarata bildirilmeli. Yapılacak soruşturmanın sonucundan istihbarat camiası, bilgi sistemleri tasarımcıları, sistem yöneticileri ve ilgili kullanıcılar gerektiği şekilde haberdar edilmeli. Adli ve istihbarata karşı soruşturma yürütülürken, sistemin ve içerdiği bilginin bütünlüğü ve güvenirliğinin yanı sıra kişisel mahremiyet hakkı da gözetilmeli.

°°° İstihbarat

İstihbarat, düşmanın faaliyetini değerlendirerek ve gerekli uyarıda bulunarak, bilgi harekâtı taarruzunun tespitine yardımcı olur. İlgili ve gerekli bilginin zamanında paylaşılabilmesi için, istihbarat ile karşı istihbarat, kolluk ve sistem tasarımcıları, yöneticileri ve kullanıcıları arasında yakın işbirliği olmalı.

°° Karşı Tepki

ABD Bilgi Harekâtı (IO) doktrininde bilgi harekâtının önemli oyuncuları şöyle gösterilmektedir: Beyaz Saray'ın koordinasyonunda; Savunma Bakanlığı, istihbarat kurumları, kolluk kuvvetleri ve endüstri.

Bilgi harekâtı taarruzu tespit edildiğinde, hasar giderici ve taarruzun etkili olmasına karşı tedbirlerin yanı sıra, kimi zaman tepki de vermek gerekebilir. Bu tepkinin etkinliği, taarruzun tespiti ve değerlendirilmesi becerilerinin etkinliğine bağlıdır. Tepki, mevcut taarruza karşı olabileceği gibi gelecekteki taarruzları caydırıcı amaçlı da olabilir.

Bilgi harekâtı taarruzuna karşı tepki vermede kolluk kuvvetleri, diplomatik girişimler, ekonomik yaptırımlar ve hatta askeri güç kullanımı söz konusu olabilir.

2003 - ABD IO DOKTRİNİ

ABD ordusunun Kasım 2003 tarihli Bilgi Harekâtı (IO) doktrini, *Information Operations: Doctrine, Tactics, Techniques, and Procedures* dokümanı daha öncekilerle benzerlik göstermektedir. Amaç, her halükârda bilgi üstünlüğünü elde etmek ve korumaktır.

Bilgi harekâtı (IO), temel olarak savunma amaçlı ve saldırı amaçlı olarak ikiye ayrılmakta ve etkinliği ancak her ikisinin birlikte uygulanması ve halkla ilişkiler veya sivil-askeri operasyonlar gibi ilgili becerilerin entegre edilmesiyle mümkün olmaktadır.

Küresel bilgi ortamı kavramı içerisindeki Küresel Bilgi Altyapısı (GII) deyiminin yerini Küresel Bilgi Şebekesi (Global Information Grid – GIG) almıştır.

Ordu, artık ticari haberleşme omurgası ve ekipmanını kullanmaktadır ki bunlar aynı zamanda düşmanın kullanımına da açıktır. Dolayısıyla, savunma amaçlı IO becerileri hemen her harekât için önemli olmaktadır.

° Tehditler

Muharebe veya hazırlık konumundaki birliklere yönelik bilgi harekâtı beklenen bir durumdur; dolayısıyla komutan, düşmanın çeşitli yöntemler kullanarak uyguladığı bilgi harekâtına karşı hazırlıklıdır. Ancak, yaygın bilgi ortamında, farklı askeri, siyasi, sosyal, kültürel, etnik, dini veya şahsi sebeplerle kişilerin, organizasyonların veya devletlerin yönlendirmekte olduğu başka tehditler de bulunmaktadır. Komutan, bu tehditlere karşı da hazırlıklı olmalı, algılamalı ve gerektiğinde mukabil bilgi harekâtı uygulayabilmeli.

°° Tehdit Seviyeleri

Bilgi ortamındaki tehditler, uygulayıcıların yetkinliği bakımından çeşitli seviyelerde olabilir:

Birinci seviye: Tek başına veya küçük gruplar halinde çalışan, ciddi desteğe sahip olmayan, pek sofistike olmayan, bilinen hacking yöntemlerini kullanan amatörler.

İkinci seviye: Bilinen hacking yöntemlerini sofistike şekilde uygulayan, ticari şirketler veya suç örgütleri tarafından desteklenen kişiler, küçük gruplar veya uluslararası topluluklar. Bu kişi veya gruplar genellikle keşif, bilgi toplama, bilgi hırsızlığı, ağ haritalama veya casusluk amaçlı faaliyette bulunurlar.

Üçüncü seviye: Devletlerle ilintili kurumlar tarafından desteklenen ve karmaşık yöntemler uygulayan, kişiler veya küçük gruplar.

Dördüncü seviye: Son teknoloji araçlar ve gizli tekniklerden yararlanarak özellikle bilgisayar ağlarına saldırı amaçlı, devlet destekli ve askeri harekâtla koordineli yürütülen bilgi harekâtı.

°° Tehdit Kaynakları

Tehditlerin kaynakları çok çeşitli olabilir:

Hackerlar: Genellikle sistemin açıklarından yararlanarak kendi beceri sınırlarını denemek güdüsüyle komuta ve kontrol (C^2) veya bilgi sistemlerine (INFOSYS) yetkisiz erişim sağlamaya çalışan tehdit unsurlarıdırlar.

Bilgi sistemlerinin, özellikle İnternet'in yaygınlaşmasıyla çok sayıda hacker'ın birlikte, genellikle politik nedenlerle saldırı düzenlemesi sıklıkla görülen bir durumdur. Ülke sınırlarını aşan böylesi toplu saldırılar hedef sistemin içerisine erişemese de sistemi

aşırı yükleyerek yetkili kullanıcıların sisteme erişimini, dolayısıyla sistemin etkin kullanımını engellemektedir.

İçerdekiler: Bilgi sistemine erişim yetkisi olanlar en sık rastlanan ve en çok zarar veren tehdit unsurlarıdırlar.

Devlet Harici Eylemci Örgütler: Yaygın bilgi ortamının avantajlarından yararlanan, sivil direniş örgütlerinden uyuşturucu kartellerine uzanan yelpazede yer alan bu tehdit unsurları oldukça maliyet etkin yöntemlerle ve dokunulmazlık perdesi ardından, uzaktan saldırılar gerçekleştirebilir ve medya vasıtasıyla dünya kamuoyunu etkileyebilirler.

Teröristler: Terörist eylemler, komuta ve kontrol sistemlerine yetkisiz erişimden komutanlara veya karar vericilere suikast düzenlemeye kadar varan farklı şekillerde olabilir.

Yabancı IO Faaliyetleri: Barışta, kriz veya çatışma ortamında yabancı devletler C^2 ve INFOSYS'e yönelik bilgi harekâtı (IO) faaliyeti yürütebilirler. Yabancı devletlerin bilgi harekâtı taarruzu basit hacker veya sivil direniş örgütü eylemlerine benziyor olabilir. Ayrıca, bilgi ortamını kendi lehlerine manipüle etmek için de kullanabilirler.

Bilgi kaynaklarının veya erişim sahiplerinin bilerek veya bilmeyerek yardım etmelerinin sağlanması, şantaj veya başka yöntemlerle manipüle edilmeleri de yabancı IO faaliyetleri içerisinde yer almaktadır.

"Dost Ateşi": Dost kuvvetlerin yürütmekte olduğu bilgi harekâtının sonucu veya yan etkisi olarak bilgi sistemleri olumsuz etkilenebilir. Örneğin, düşmanın haberleşmesini karıştırmak amacıyla uygulanan "jamming"den dost kuvvetlerin haberleşmesi de olumsuz etkilenebilir. Veya hedef ülkedeki yerel lideri düşmanca görüşler ifade eden uluslararası bir kuruluşla çalışmak yanlış algıya sebep olabilir.

Bunların yanı sıra, propaganda veya yanıltıcı yayın, elektromanyetik karıştırma (jamming) veya elektromanyetik darbe (Electromagnetic Pulse – EMP) vasıtasıyla komuta kontrol ve bilgi sistemleri çalışamaz hale getirilebilir.

Dikkat edilmesi gereken bir husus da şudur ki tehditlerin gerçekte -gerek kaynakları gerekse yetkinlik seviyeleri bakımından- algılanandan, tespit edilenden farklı olma ihtimali vardır. Birinci seviye bir hacker saldırısı gibi algılanan tehdit aslında düşman devletin uyguladığı üçüncü seviye bir tehdit olabilir; veya tersi.

°° Tehdit Yöntemleri

Yetkisiz Erişim: Komuta ve kontrol (C^2) sistemlerinden bilgi elde etmek, bilgi zerk etmek, bilgiyi değiştirmek veya silmek amacıyla yapılan yetkisiz müdahale.

Yetkisiz kişiler İnternet üzerinden askeri şebekelere, mesela yerel alan ağlarına bağlanabilirler. Bunu engellemek için (firewall) güvenlik duvarı kullanılır; ancak, eğer firewall aşılırsa C^2 sistemine de erişilir.

Yetkisiz erişimin internet ve firewall üzerinden yapılması şart değil; C^2 sistemine bağlı bir terminal üzerinden, yani içeriden de yapılabilir.

Zararlı Yazılım: Bilgi sisteminin beklenenden farklı şekilde çalışmasına yol açan yazılım.

Elektromanyetik Yanıltma: Düşmana yanıltıcı bilgi vermek, onu yanıltmak ve bu sayede muharebe yeteneğini ortadan kaldırmak amacıyla elektromanyetik enerjinin yayınlanması, yansıtılması, değiştirilmesi, bastırılması, kuvvetlendirilmesi.

> Örneğin, düşmanın telsiz çevrimine girip onun operatörünü taklit etmek veya taarruz hazırlığı yaparken radarları (search) arama modunda tutmak gibi…

Elektronik Taarruz (EA): Elektromanyetik enerji veya yönlendirilmiş enerji veya anti radyasyon silahları vasıtasıyla personel, teçhizat veya tesislere yönelik taarruz.

Bilgisayar Ağı Taarruz (CNA): Elektronik yöntemler vasıtasıyla bilgisayar ağlarına yönelik saldırı. CNA sayesinde bilgisayar ağı, dolayısıyla sistem çalışamaz hale getirilir. Bilgisayar ağına sürekli ve çok sayıda başvuru yaparak sistemi doygunluğa eriştirmek ve işlevini yapamaz duruma getirmek de (Denial of Service - DoS) CNA yöntemlerinden biridir.

Algı Yönetimi: Yabancı muhatapların hissiyatını, güdüsünü, muhakemesini; istihbarat sistemlerinin ve liderlerin tahmin ve karar yetisini etkilemek ve bu sayede onların arzu edilen şekilde davranmalarını sağlamak amacıyla seçili bilgi ve işaretleri değiştirmek veya aktarmak.

Sivil medya yayınlarından özel kuvvetler saldırılarına kadar çeşitli şekillerde yürütülebilen algı yönetimi, gerektiğinde dost kuvvetlere de yönelik olabilir, taarruz veya direnme şevkini artırmak için.

Propaganda: Düşmanın kontrolünde olan bilgi ortamını şekillendirmek. Dost kuvvetlerin harekâtını etkileyebilecek düşman davranışlarını yönlendirmek amacıyla uygulanır.

Yanıltma: Topluluklardan ziyade karar vericilere yönelik olarak bilgi ortamını şekillendirmek.
Yanıltma operasyonunda gerçeğin yanıltıcı bir görüntüsü sunulur muhataba.

Fiziki İmha: Komuta ve kontrol (C^2) sistemlerini zayıflatmaya, bozmaya veya imha etmeye yönelik fiziki eylemler.

> Seyir füzeleri, hassas güdümlü füzeler, insansız araçlar, yön bulma ve görüntü işleme sistemlerindeki gelişmeler bu beceriyi oldukça ileri düzeye taşımaktadır.

° Hukuki Durum

Bilgi sistemlerine müdahale ile ilgili ulusal ve uluslararası hukuki düzenlemeler sıklıkla değişmekte olduğundan, bilgi harekâtı uygulamalarında komutanlar hayli karmaşık

hukuki yükümlülükler ve yaptırımlarla karşı karşıya kalabilirler. Bu yüzden, böylesi uygulamalarla ilgili hukuki danışmanlık desteği gerekli olabilir.

° Bilgi Harekâtının Unsurları (Beceriler)

Komutanlar, harekâtın etkinliğini artırmak için gerek müdafaa gerekse taarruz amaçlı bilgi harekâtı unsurlarını birlikte kullanmak durumundadırlar. Bu unsurlar:

Temel (Çekirdek) Beceriler	Destekleyici Beceriler	İlgili Beceriler
Harekât Güvenliği (OPSEC)	Fiziki İmha	Halkla İlişkiler (PA)
Askeri Yanıltma (~~MILDEC~~) (MD)	Fiziki Emniyet	Sivil-Askeri Operasyonlar (CMO)
Psikolojik Harekât (PSYOP)	Bilgi Teminatı (IA)	
Elektronik Harp (EW)	İstihbarata Karşı Koyma (İKK) (CI)	
Bilgisayar Ağı Operasyonları (CNO)	Yanıltmaya Karşı Koyma	
Bilgisayar Ağı Taarruz (CNA)	Propagandaya Karşı Koyma	
Bilgisayar Ağı Savunma (CND)		
Bilgisayar Ağı İstismar (CNE)		

1996 tarihli doktrinden bu yana OPSEC, PSYOP, MILDEC ve EW temel (çekirdek) beceriler içerisindeki yerlerini korumuşlardır. Askeri yanıltma (MILDEC), bu doktrinde MD şeklinde kısaltılmıştır.

Bilgisayar ağları ile alakalı beceriler haricinde pratikte pek bir şey değişmemiştir.

[Psikolojik harekât (PSYOP) konusu özel olarak incelenmeyi hak ediyor.]

°° Temel (Çekirdek) Beceriler

Bilgi harekâtının temel (çekirdek) becerileri, harekât güvenliği (OPSEC), askeri yanıltma (MD), psikolojik harekât (PSYOP), elektronik harp (EW) ve bilgisayar ağı operasyonları (CNO) olarak tanımlanmaktadır.

°°° Harekât Güvenliği (OPSEC)

Görevin, harekâtın başarıyla yürütülmesi ve sonuçlanmasını engelleyecek, zorlaştıracak her türlü bilgi akışına karşı önlemler ve eylemler.

ABD ordusu için harekât güvenliği (OPSEC) şöyle tanımlanmaktadır:

-- Düşman istihbaratı tarafından izlenebilecek, dost kuvvetlere ait bilginin esas unsurlarını (EEFI) ve aktiviteleri belirlemek.

-- Düşman istihbaratı tarafından izlenebilen ve bir araya getirildiğinde dost kuvvetlere ait bilginin esas unsurlarının (EEFI) anlaşılabileceği işaretleri belirlemek.

-- Düşmanın faydalanmasına açık zaafları bertaraf edecek veya kabul edilebilir seviyeye indirecek tedbirleri belirlemek ve uygulamak.

> Ordu doktrininde dost kuvvetlere ait bilginin esas unsurları (EEFI) olarak tanımlanan bilgi, müşterek doktrinde kritik bilgi olarak tanımlanmaktadır.

°°° Askeri Yanıltma (MD)

Dost kuvvetlerin askeri becerileri ve imkânları hakkında düşmanın karar vericilerini yanıltmaya ve bu sayede dost kuvvetler harekâtının başarı ihtimalini artırmaya yönelik önlemler ve eylemler.

Düşmanın karar mekanizmasını yanıltmada iki farklı temel yöntem kullanılır:

-- Dost kuvvetlerin niyeti ile ilgili belirsizliği artırmak.

-- Dost kuvvetlerin niyeti ile ilgili kesinliği artırmak.

Askeri yanıltma (MD) sayesinde dost kuvvetlerin yürüttüğü harekât karşısında düşman daha savunmasız hale gelir.

°°° Psikolojik Harekât (PSYOP)

Daha önce, 1996 tarihli doktrinde de tanımlandığı üzere, yabancıların davranışlarını harekâtı yürüten tarafın menfaatine olacak şekilde yönlendirmek amacıyla yabancı muhatapların duygularını, güdülerini, objektif muhakemelerini ve nihayetinde yabancı kişilerin, grupların, kurumların ve hükümetlerin davranışlarını etkilemek için yapılan operasyonlar olarak tanımlanır psikolojik harekât (PSYOP).

> Düşman değil yabancı vurgusu dikkat çekiyor, yine. Çünkü, ABD ülkesi içerisinde veya ABD vatandaşlarına karşı -düşman dahi olsalar- psikolojik harp uygulamak kanuna aykırıdır.

°°°° Sınırlamalar

Psikolojik harekât planlanırken ve yürütülürken birtakım sınırlamalara riayet etmek gerekmektedir:

-- Psikolojik harekât (PSYOP), ABD topraklarındaki ve sahip olduğu yerlerdeki muhataplara ve ABD vatandaşlarına yönelik uygulanamaz.

-- Özellikle saldırı amaçlı uygulandığında, ABD kanunlarına, uluslararası hukuk ve sözleşmelere riayet edilmeli.

-- Ayrıntılar için 1948 tarihli Smith-Mundt yasası ve 1998 tarihli başkanlık direktifi (PDD-68) yol göstericidir.

> Smith-Mundt Act of 1948 diye bilinen, asıl başlığı United States Information and Educational Exchange Act of 1948 olan, 1948 tarihli ABD Bilgi ve Eğitim Değişimi yasasının amacı dünya halkları arasında Amerika Birleşik Devletleri'nin daha iyi anlaşılmasını sağlamak ve uluslararası ilişkilerde iş birliğini geliştirmek olarak

belirtilmiştir. Bu amaçla, bir zamanlar Ankara'da da Amerikan Haberler Merkezi adıyla faaliyet gösteren United States Information Agency - USIA) ve Amerika'nın Sesi radyosu (Voice of America - VOA) ve daha birçok ajans kurulmuş ve mevcut kuruluşlar bu yasa çerçevesinde faaliyet sürdürmüşlerdir.

Söz konusu yasa, diğer ülkeler nezdinde Amerika'nın daha iyi anlaşılmasını ve Amerikan halkı ile diğer ülkelerin halklarının birbirlerini daha iyi anlamalarını desteklemek amacıyla ABD Kongresi'nden geçirilmiştir. Böylece, Amerika ve Amerikan halkı ve politikaları ile ilgili olarak diğer ülkelerin halklarının bilgilendirilmesi ve diğer ülkelerle Amerika arasında olagelen teknik hizmetler, eğitim, sanat ve bilim alanındaki bilgi, beceri ve personel değişimi yasal bir temele dayandırılmıştır. ABD yasalarına göre suç teşkil eden veya ABD'nin güvenliği ile çelişen bilgi bu yasa çerçevesinde yayınlanamaz. Yabancı ülkelere yönelik yürütülen bilgilendirmenin bir devlet tekeli vasıtasıyla yapılmaması; gerektiği durumlarda, özel basın, yayın, radyo, sinema ve diğer ajansların kullanılması tavsiye edilmektedir. *Buraya kadar her şey çok iyi, çok hoş...*

Peki, böylesi bir eğitim, bilim, teknoloji, sanat ve kültürel değişim ve bilgilendirme programının yönetimi niçin eğitim, kültür, bilim, teknoloji, sanat veya kültürle alakalı bir bakanlığa değil de Dışişleri Bakanlığı'na bırakılmış? Yani ABD vatandaşı bir profesör veya teknik uzman veya tiyatro eğitmeni veya orkestra şefi bir başka ülkeye, mesela Türkiye'ye gidecekse bunun ABD çıkarları için yararlı ve gerekli olup olmadığına ABD Dışişleri Bakanlığı karar veriyor. *Bu denli farklı bakanlıklar arasında koordinasyon zor olur; iyisi mi hepsinden ayrı tek bir bakanlığa bırakalım demiş olsalar gerek.* Peki ya bu programda görev alacak -devlet memuru veya değil- tüm Amerikan vatandaşlarının FBI tarafından incelenmiş ve onaylanmış olması mecburiyeti niye? *Herhalde, diğer ülkelerle ve onların halklarıyla, kültürleriyle, teknolojileriyle temas eden Amerikalıların çok etkilenip raydan çıkmalarından, kendi ülkeleri aleyhine faaliyet göstermelerinden çekindikleri için olsa gerek.* (FBI tarafından soruşturulma koşulu 1979'da yasadan çıkarılmıştır.)

Her ne kadar dönemin koşulları, mücadele ettikleri Sovyet tarzı yapılanmayı örnek almalarına sebep olmuşsa da, şaka bir yana, bu yasa ABD'nin psikolojik harekât (PSYOP) uygulamalarının temelini oluşturur ki elli beş sene sonra yayınlanan Bilgi Harekâtı (IO) doktrininde bile bu yasaya referans veriliyor olması şaşırtıcıdır. *Özgür bilim, özgür sanat, özgür basın,* bir yere kadar…

Bu yasa çerçevesinde değişim programlarıyla yabancı ülkelere gönderilen ABD vatandaşı uzmanlar, bilim ve sanat adamları/kadınları, çalıştıkları ülke veya kurum onları bu ülkeye sadakat yemini etmeye mecbur bırakmadıkça gittikleri ülkenin resmi kurumlarında görev yapabilirler. *Acaba bu değişim programında yer alan diğer ülkeler de kendi vatandaşları için böyle bir koşul koymuşlar mı? Araştırmaya değer...*

Kaçınılmaz saçmalıktan kaçınmak mümkün olmuyor, tabii ki… Hem kendi vatandaşlarına yönelik psikolojik harekâtı yasaklayacak, hem de yabancı ülkelere yönelik propaganda amaçlı yayın yapacaksın. Nasıl olacak? Özellikle İnternet'in yaygınlaşmasıyla günümüzde hemen herkesi kapsar hale gelen bilgi ortamında yabancılara yönelik yapılan yayının aynı zamanda Amerikan halkını da etkilememesi mümkün değil. Bu sebeple olsa gerek, Smith-Mundt yasasında 2012'de yapılan

düzenlemeyle yabancı ülkelere yönelik yapılan yayının Amerikan halkına ulaşmaması koşulu kaldırılmıştır.

2000'li yıllarda, stratejik seviyedeki psikolojik harekât uygulamaları Uluslararası Kamuoyu Enformasyon Programı (International Public Information Program - IPIP) ile uyumlu olmak durumundadır. Sınırları dışında, yabancı muhataplara yönelik yapılan ABD'nin dış politikası ile ilgili bilgi yayınını IPIP koordine etmektedir.

Kosova ve Haiti operasyonlarında görüldü ki herhangi bir kurum ya da kuruluş, yabancı bir ülkedeki ABD aleyhine olumsuz yayınlara karşı koymak, ABD politikalarını savunmakla görevli değil. Bunun üzerine, "düşmanı yenmek için ABD hükümetine yardım" gerekçesiyle, 1999 yılında ABD Başkanı Clinton'ın PDD-68 numaralı direktifiyle savunma, dışişleri, adalet, ticaret ve hazine bakanlıklarından, CIA ve FBI'dan üst düzey yetkililerin katılımıyla IPI Grubu oluşturulmuştur. Grubun tüzüğünde, ABD'yi hedef alan yabancı propaganda ve yanıltmalara karşı istihbarat teşkilatlarının etkin rol alacağı belirtilmiştir. ABD'nin düşmanları tarafından yapılan olumsuz propagandaya karşı yabancı muhatapları etkilemek, ABD'nin güvenliğini güçlendirmek, ekonomik refahını desteklemek ve demokrasiyi yaymak için oluşturulan bu program, tıpkı PSYOP tanımındaki gibi, yabancı muhatapların duygularını, güdülerini, muhakemelerini ve nihayetinde kişilerin, grupların, kurumların, hükümetlerin davranışlarını etkilemeyi amaçlamaktadır. Öte yandan, IPI operasyonları gizli değil, açık yürütülmek ve başkanlık direktifi gereği "yabancı muhatapları yanıltmamak", "gerçeği yansıtmak" zorundadır. Amerikan halkına yönelik psikolojik harekât uygulamak kanuna aykırı olduğu için, IPI operasyonlarında bu kurala riayet edilir. Dahası, dışarıya yönelik bir operasyonların günümüz bilgi ortamında ABD kamuoyunu da etkilemesi söz konusu olduğundan, IPI operasyonları iyi hesaplanmalı ve koordine edilmelidir.

Okuyucunun dikkatini çekmiştir; ABD'nin güvenliği ve refahı ile demokrasinin yayılması birlikte değerlendirilmekte. Her ne kadar ABD içerisinde veya Amerikan halkına yönelik psikolojik harekât kanunen yasak olsa da direktifin kaleme alınışında dahi psikolojik harekât unsurları açıkça kendini gösteriyor. (Bir nevi, "kendim için istiyorsam namerdim" durumu…)

Aşikârdır ki her ne kadar içeriye yönelik psikolojik harp kanunen yasaklanmış olsa da içeriyi etkilememesi mümkün değil. Bunda, bilgi ortamını oluşturan medya, İnternet ve diğer unsurların yaygınlığı önemli rol oynamaktadır.

Zaman zaman yöneticilerin veya uygulayıcıların ihmali veya suiistimaliyle olan içeriye yönelik psikolojik harekât örnekleri vardır. Özellikle PA ile PSYOP arasındaki sınırı belirlemek veya belirlenmiş sınırı aşmamak oldukça zordur. Örneğin, İkinci Körfez Savaşında Laura Bush ve Cherie Blair'in birkaç gün arayla medya önünde yaptıkları konuşmalarda, benzer cümlelerle, Afganistan'da oje süren kadınların tırnaklarının söküldüğünü dile getirmeleri masum bir yakınma mı, PA mı, PSYOP mu; kim bilebilir?

Nihayetinde, uygulamada zorluklar yaşansa da, zaman zaman uygulayanların ihmali veya suiistimali olsa da, ***psikolojik harekâtın kendi ülkesinde ve kendi vatandaşları üzerinde uygulanmasını kanunla yasaklamak o ülke yönetimi için erdemli bir duruştur.***

Psikolojik harekât (PSYOP), stratejik, operasyon ve taktik seviyede yabancı muhatapları etkilemede ABD hükümetinin başlıca dayanağıdır. Bu bağlamda PSYOP:

-- Askeri yanıltmanın (MILDEC) etkisini artıran;

-- Dost kuvvetlerin operasyonlarıyla ilgili olarak düşmandaki algıyı şekillendiren;

-- Liderlik kademesi hakkında düşmanda kuşku yaratan;

-- ABD'nin üstünlüğü imajını yansıtan;

-- Toplulukların davranışını etkileyecek bilgi yayınlayan;

-- Askeri harekâtın en az zayiatla gerçekleştirilmesine, ABD ile müttefiklerinin yararına sonuçlanmasına yardımcı olan bir kuvvet çarpanı olarak değerlendirilebilir.

Psikolojik harekât:

-- Düşmanın bilgi toplama becerilerini ve yöntemlerini belirlemek;

-- İstenen algıyı kuvvetlendirmek için düşmana aktarılacak veya ondan esirgenecek bilgi ve emareleri belirlemek;

-- Belirli amaçlar için vurgulanacak veya görmezden gelinecek konuları belirlemek;

-- Düşmanın davranışlarını yönlendirebilmek için yüz yüze görüşmeler, etkili konuşmacılar ve medya unsurlarından yararlanmak;

-- Düşmanın istenmeyen bir eylemde bulunmasını engellemek için ona eylemin olası sonuçlarını göstermek gibi teknikler içermektedir. Bu teknikler siyasi, kültürel, etnik, dinsel bölgesel, ulusal, demografik ve coğrafi değerlendirmeler esas alınarak geliştirilir ve uygulanır.

Taarruz amaçlı bilgi harekâtında olduğu gibi psikolojik harekâtta da düşmanın moralini ve komutanın etkinliğini zayıflatıcı haberler yayılır. Bu amaçla:

– ABD kuvvetlerinin operasyonları ile ilgili olumlu imaj yaratılır;

– Hedef muhataplara ulaşabilmek için haberleşme güçlüğü, okuryazarlık azlığı, sansür gibi engelleri aşmak için önlemler alınır;

– Düşmanın morali, direnme azmi kırılır; çatışmayı sürdürme isteğine karşı alternatifler sunulur;

– Düşman, bazı etkili silahları kullanmaktan caydırılır;

– Etnik, kültürel, dinsel veya ekonomik farklılıklar istismar edilir;

– Risklere karşı, sivil unsurlarla alakalı istihbarat sağlanır;

– Düşmanın içerisindeki direniş güçlerinin morali güçlendirilir, onlara destek sağlanır.

°°° Elektronik Harp (EH) (EW)

Düşmanı etkisizleştirmek amacıyla elektromanyetik ve yönlendirilmiş enerji vasıtasıyla elektromanyetik tayfı denetim altına alarak yürütülen harp şeklidir, Elektronik Harp.

Elektronik Harp (EH) (Electronic Warfare - EW), kendi içerisinde -kimi zaman tek başına, kimi zaman birlikte kullanılan- üç temel bileşenden oluşur: Elektronik Savunma (Electronic Protection - EP), Elektronik Taarruz (Electronic Attack - EA) ve Elektronik Harp Destek (Electronic Warfare Support - ES).

[Daha önceki -ve sonraki- doktrinlerdekinden farklı olmadığı için elektronik harp ve alt bileşenleri konusunda ayrıntıya girilmemiştir.]

°°° Bilgisayar Ağı Operasyonları (CNO)

Bilgi harekâtının temel becerilerinden olan Bilgisayar Ağı Operasyonları (Computer Network Operations - CNO) genellikle taktik seviyede değil, daha üst seviyelerde yürütülür. Bilgisayar Ağı Taarruz (CNA) daha ziyade üst seviyede uygulanırken, Bilgisayar Ağı Savunma (CND) hemen her seviyede uygulanmalıdır. Bilgisayar Ağı İstismar (CNE) ise genellikle kolordu ve üstü seviyelerde yürütülen bir istihbarat faaliyeti olarak değerlendirilir.

°°° Bilgisayar Ağı Taarruz (CNA)

Bilgisayar Ağı Taarruz (Computer Network Attack - CNA), aslında taarruz amaçlı bilgi harekâtının bir parçasıdır; ancak, düşmanın taarruz amaçlı bilgi harekâtını yürüteceği kaynaklara yönelik yapılanı ise müdafaa amaçlı bilgi harekâtının parçası olarak kabul edilir.

°°° Bilgisayar Ağı Savunma (CND)

Bilgisayar Ağı Savunma (Computer Network Defense - CND) sayesinde bilgisayar ağları, düşmanın veya yetkisiz kişi ve kuruluşların eylemlerine karşı -mümkünse- tamamen veya kısmen korunur. Bu amaçla;

- Bilgisayar ağları üzerinde koruyucu ve yetkisiz eylemlerin faillerinin yakalanması ve cezalandırılmasını sağlayıcı tedbirler alınır;
- Tehditlere karşı farkındalığı artırıcı eğitimler düzenlenir.
- Bilgisayar ağına yönelik saldırıları tespit amaçlı yazılım ve firewall kullanılır;

°°° Bilgisayar Ağı İstismar (CNE)

Bilgisayar Ağı İstismar (Computer Network Exploitation - CNE) vasıtasıyla düşmanın bilgisayar ağlarından veya otomatik sistemlerinden istifade ederek (doğrusu, istismar ederek) bilgi elde edilir veya operasyon yürütülür.

°° Destekleyici Beceriler

Fiziki imha, fiziki emniyet, Bilgi Teminatı (Information Assurance - IA), İstihbarata Karşı Koyma (İKK) (Counterintelligence - CI), yanıltmaya karşı koyma ve propagandaya karşı koyma, bilgi harekâtının destekleyici becerilerini oluşturmaktadır. 2003 doktrini ile fiziki imha, bir temel beceri olmaktan çıkmış, destekleyici beceriler arasında yer almıştır.

°°° Fiziki İmha

Her ne kadar bir Bilgi Harekâtı (IO) becerisi olarak ele alınsa da, fiziki imha vasıtasıyla hedef ortadan kaldırıldığında hem bilgi harekâtı hem de geleneksel amaçlar elde edilmiş olur.

°°° Fiziki Emniyet

Fiziki emniyet, personeli korumak; tesise, ekipmana, malzeme ve dokümanlara yetkisiz erişimi engellemek ve casusluğa, sabotaja, çalınmaya ve hasara karşı alınan tedbirlerdir.

°°° Bilgi Teminatı (IA)

Bilginin ve bilgi sistemlerinin erişilebilirliğini, hakikiliğini, gizliliğini, bütünlüğünü ve inkâr edilemezliğini sağlayan koruyucu bilgi operasyonları, bilgi teminatının esasını teşkil eder.

Erişilebilirlik: Yetkili kullanıcıların erişimine açık.

Hakikilik: Kaynağı ve doğrulanabilir.

Gizlilik: Yetkisiz ifşaya karşı korunmuş.

Bütünlük: Yetkisiz değişikliğe (silinme dahil) karşı korunmuş.

İnkâr edilemezlik: Mesajın alındığının veya gönderenin kimliğinin reddedilemeyişi ki bu sayede iki taraf da mesaj üzerinde işlem yapmış olma ihtimalini inkâr edemez.

Bilgi Teminatı (Information Assurance - IA) aynı zamanda bilgisayar ağı savunma (CND) tedbirlerini de içerir.

°°° İstihbarata Karşı Koyma (İKK) (CI)

Yabancı devletler veya onların unsurları kurumlar, şahıslar veya uluslararası terörist örgütler tarafından yürütülen casusluk ve diğer istihbarat eylemlerine, sabotaja ve suikasta karşı koymak üzere toplanan bilgi ve yürütülen faaliyet İstihbarata Karşı Koyma (İKK) (Counterintelligence - CI) olarak tanımlanır.

İstihbarata karşı koymanın esası, eldeki bilgiyi korumak için tedbirli olmak ve düşmanın istihbarat toplamasını engellemek için açıkları kapatmak ve zaafları gidermek olarak tanımlanabilir. Bu amaçla, OPSEC ve MILDEC becerilerinden da yararlanılır.

°°° Yanıltmaya Karşı Koyma

Yanıltmaya karşı koyma faaliyeti, düşmanın uygulamakta olduğu yanıltma operasyonlarının etkisini gidermek ya da azaltmak veya bu operasyondan fayda sağlayarak avantaj elde etmek amacıyla yürütülür. (Yanıltma operasyonunu ortaya çıkarmak amacıyla yürütülen istihbarat faaliyetini bu tanımın dışında tutmak doğru olur.)

Yanıltmaya karşı koyma faaliyetlerinin başarısı için, düşmanın daha önce uygulamış olduğu yanıltma yöntemleri hakkında bilgi sahibi olmakta yarar vardır. Başarılı bir yanıltmaya karşı koyma operasyonunda düşman genellikle yanıltmanın anlaşıldığının farkına varmaz ve yanıltma operasyonunu sürdürür; daha doğrusu, sürdürdüğünü zanneder.

°°° Propagandaya Karşı Koyma

Düşmanın yürüttüğü psikolojik harekâtın parçası olan propagandanın zararlı etkisini azaltmak amacıyla propagandaya karşı koyma programı yürütülür. Dost kuvvetlerin operasyonlarını olumsuz etkileyen her türlü mesaj, söylenti, görüntü şeklindeki propagandaya karşı, tüm çatışma süresince ve hatta öncesi ve sonrasında bu faaliyeti sürdürmek gerekebilir.

Bu bağlamda, bazı kavramları gözden geçirmekte yarar var:

°°°° Propaganda

Propagandayı yürüten tarafın menfaati doğrultusunda muhatap grubun görüşünü, düşüncesini, hissiyatını ve davranışını etkilemek amacıyla yapılan her türlü haber veya bilgi yayma faaliyeti.

Propaganda kampanyası ile düşmanın karşı koyma azmi, direnci kırılır. Propagandada gerçekle yalan öyle karıştırılır ki muhatap farkı anlayamaz.

°°°° Yanlış Bilgi

Herhangi bir kaynaktan yayınlanan veya bir talebe cevap olarak gönderilen yanlış bilgi.

Yanlış bilgiye karşı en iyi önlem, dikkate almamak veya yanlış bilgilendirmeye karşı doğru bilgi sağlamaktır. Bazı durumlarda askeri bilgi kaynağının güvenilirliği saygın bir haber ajansınınkiyle karşı karşıya gelir. Böylesi durumlarda, açık olmak ve doğru bilgiyi yayınlayarak yanlış bilgiyi bertaraf etmek en doğru hareket tarzıdır. Halkla ilişkiler (PA) personeli ve medya arasında açık, güvenilir, yakın ilişki olması yanlış bilginin olumsuz etkisini en aza indirmekte yardımcı olur.

°°°° Uydurma Bilgi (Dezenformasyon)

Dezenformasyon, genellikle istihbarat teşkilatları veya diğer gizli kuruluşlar tarafından yayılan, dost kuvvetlerin ve müttefiklerin karar mekanizmasını etkilemeye yönelik, gerçeği çarpıtan, yanıltıcı bilgidir.

Dezenformasyon vasıtasıyla tarihten gelen etnik, dini veya ırksal ayrılıklar gündeme getirilerek müttefikler arasındaki ittifak ve uyumu bozmanın fırsatları aranır. Taktik seviyede dezenformasyon, kuvvetlerin olmayan tehdide, yani yanlış hedefe yoğunlaşmasına sebep olabilir.

°°°° Karşı Bilgi

Karşı görüşteki kaynaklardan bilerek veya bilmeyerek yayınlanan doğru bilgi. Genellikle propagandanın etkisini bertaraf etmek için karşı bilgiden yararlanılır.

°° İlgili Beceriler

Daha önceleri destekleyici beceriler olarak tanımlanan Sivil İşler (Civil Affairs - CA) ve Halkla İlişkiler (Public Affairs - PA) bu doktrinde ilgili beceriler olarak sınıflandırılmıştır.

Bilgi Harekâtı (IO) ile ilgili beceriler temelde halkla ilişkiler (PA) ve sivil-askeri operasyonlarla (Civil-Military Operations - CMO) olarak tanımlansa da sadece bunlarla sınırlı değildir; mesela, diplomatik çabaları destelemek amacıyla yürütülen özel kuvvetler harekâtı da bilgi harekâtı ile ilgili sayılabilir.

°°° Halkla İlişkiler (PA)

İç ve dış kamuoyuna yönelik, doğru, güvenilir ve zamanında bilgilendirme.

> 2003 tarihli bu doküman ABD Kara Kuvvetleri (Ordu) IO doktrini olduğu için ifadeler genellikle ordu ile alakalı yazılmıştır.

Halkla ilişkilerin (PA) başlıca görevi, barışta ve kriz veya savaş halinde ABD halkını ve ordusunu bilgilendirmek ve bu sayede kamuoyunun orduya olan güvenini korumaktır.

Halkla İlişkiler (Public Affairs - PA) prensipleri:

-- Gerçek önemlidir. Başarılı halkla ilişkiler güvene ve güvenilirliğe dayalıdır. (Gerçeği yansıtmamak, halkla ilişkilerde güvenilirliği zedelemenin en kolay yoludur.) ABD ve uluslararası kamuoyunun yanıltılmadığından, yanlış algıya sebep olunmadığından emin olmak gerekir.

-- Haber çıktıysa çıkmıştır. Haber (bilgi) yayıldıktan sonra ulaşma imkânı olan herkes tarafından ulaşıldığı kabul edilir ve ona göre davranılır. ABD Savunma Bakanlığı'nın politikası, eleştiriden kaçınmak için veya utanç kaygısıyla bilginin tutulması veya gizlenmesini men eder.

> Bunlara inanmakta zorlanıyor insan; acaba bu IO doktrinleri özellikle IO materyali olarak mı yayınlanmış diye düşünmekten alamıyor kendini. Yine de resmi politikanın bu şekilde tanımlanmış olması takdiri şayan olsa gerek.

-- Haberlere sansür uygulamak, teknik olarak mümkün olmadığı gibi, kabul edilebilir bir politika da değil günümüzde. Medya, olay henüz olmuşken olay yerine ulaşıyor; bu durumda, halkla ilişkiler (PA) unsurlarını erkenden sahaya göndermek gerekir.

-- Tek ses olmalı. Komutan, sadece sorumluluk alanlarına giren konularla alakalı konuşmaları, diğer konular hakkında spekülasyon yapmamaları hususunda eğitmeli altındakileri.

°°° Sivil-Askeri Operasyonlar (CMO)

Sivil-Askeri Operasyonlar (Civil-Military Operations - CMO), askerler ile resmi ve gayri resmi kuruluşlar ve yetkililer ve sivil toplum arasındaki ilişkileri kurmak, muhafaza etmek, etkilemek ve bundan faydalanmak amacıyla yürütülür.

Sivil-askeri operasyonlar (CMO) askeri harekâtın öncesinde, harekât süresince veya sonrasında, hatta hiçbir askeri harekât söz konusu değilken bile yürütülebilir. Sivil-askeri operasyonları yürütürken, operasyonun gidişatını ve sonucunu etkileme ihtimali bulunan yerel sivil toplumla ve yönetimle, sivil toplum örgütleriyle, uluslararası kuruluşlarla irtibatta bulunmak gereklidir. Sivil-askeri operasyonlar, tanımı gereği, askeri operasyonları desteklemek ve/veya sivil otoriteleri desteklemek şeklinde iki yönlü olabilir.

Sivil-askeri operasyonlar (CMO) ile halkla ilişkiler (PA) ve psikolojik harekât (PSYOP) birbiriyle koordineli şekilde planlanmak, yürütülmek, değerlendirilmek durumundadır.

> Kendi ülkesi içerisinde ve kendi vatandaşlarına yönelik psikolojik harekât uygulamama zorunluluğu bu koordinasyonu hayli önemli kılmaktadır.

° Bilgi Harekâtının Safhaları

Bilgi harekâtı, savaş veya kriz esnasında olduğu gibi öncesi veya sonrasında barış dönemlerinde de yürütülür. Ancak, yoğunluğu, hedefleri ve muhatapları farklı olabilir.

° Barışta

Komutanlar, kriz veya savaş zamanı için stratejik ortamı şekillendirmek amacıyla barış zamanında da bilgi harekâtı uygulayabilirler. Çabalarını odaklamak için ihtiyat planlarından yararlanmak suretiyle her bir bilgi harekâtı unsuru (becerisi) için -yeri ve zamanı geldiğinde kullanmak üzere- veritabanları hazırlarlar.

> Biz buna kısaca "fişleme" diyoruz.

Bu veritabanları her bir düşman unsuru ve diğer önemli şahsiyetler ve kurumlarla ilgili bilgi içerir. Örneğin:

-- Siyasi önderlik;

-- Askeri ve sivil haberleşme şebekeleri (yerli ve yabancı medya dahil) bilgi becerileri ve zayıflıkları;

-- Askeri operasyonlar, önderlik ve altyapıdaki stratejik ve taktik zaaflar;

-- Bir askeri harekâtı başlatabilme ve sürdürebilmeyi etkileyen etkenler; (Harekâtı sürdürebilecek ekonomik altyapının da dikkate alınması gerekir.)

-- Halkın süregiden harekâta desteği ve moral gücü;

-- Tarihi dostluklar veya düşmanlıkların, etnik ve ırksal farklılıkların sosyal etkileri.

Daha ayrıntılı örnekler vermek gerekirse:

-- Hükümet ve diğer önemli aktörler üzerinde nüfuz sahibi kişiler ve gruplar;

-- Hükümet ve diğer önemli aktörler içerisinde karar vericiler;
-- ABD'nin çıkarları ile uyumlu kişiler ve gruplar;
-- ABD'nin tesirine açık kişiler ve gruplar;
-- ABD'nin çıkarlarına karşı kişiler ve gruplar;
-- ABD'nin ekonomik veya askeri desteğini kabule eden veya etmeyen, resmi ve gayri resmi kişiler ve gruplar;
-- Belirli grupların ilgisini çeken temalar;
-- Yabancı ülkelerin istikrar -veya istikrarsızlık- unsurları;
-- Dini, etnik ve kültürel adetler, esaslar ve değerler;
-- Etnik gruplar arası ilişkilerin ve lisanların değerlendirilmesi;
-- Okuryazarlık oranı;
-- Haberleşme altyapısının değerlendirilmesi;
-- Askeri haberleşme ve komuta kontrol (C2) altyapısının değerlendirilmesi;
-- Askeri eğitim ve yetkinliklerin değerlendirilmesi;
-- Esirgeme (denial of service), askeri yanıltma ve psikolojik harekâta karşı dayanıklılık -veya duyarlılık- seviyesini tespiti.

Barış zamanı yürütülen bazı bilgi harekâtı eylemlerinin stratejik etkileri olabileceği için, komutanın stratejik seviyede onay alması gerekir. Yine de değerlendirme, planlama, hazırlık ve eğitim etkinlikleri ile kriz veya savaş durumunda yararlanabileceği bağlantılar kurabilir.

> Eğitim, kolayca yoğrulabilen yapısının sağladığı avantaj sayesinde oldukça yaygın bir bahane, bir araç olarak öne çıkıyor. "Eğitim mi?" "Öyleyse sorun yok."

°° Krizde

Kriz durumunda acil durum ya da kriz planları uygulanır. Krizde amaç, kriz ortamını barış ortamına çevirmek olmalıdır. Bu amaçla bilgi harekâtını daha incelikli, mahirane yöntemlerle uygulamak gerekir. Oldukça uzun süren ve farklı seviyeler içeren onay sürecinden geçen planlama ve hazırlık yapılır.

Bu aşamada olası düşmanlara yönelik, daha iyi odaklanmış istihbarat, gözetleme ve keşif (Intelligence, Surveillance and Reconnaissance - ISR) operasyonları yürütülür. Karar vermede yararlanmak amacıyla hedef gruplar, olası düşmanlar hakkında tüm kaynaklardan bilgi devşirilir. Düşmanın politik, ekonomik, sosyal veya askeri yapısı içerisinde yer alan aktörler etki altına alınır. Barışta bilgi ortamında oluşturulan koşullar ve ilişkiler sayesinde düşmanın karar vericilerinin krizi barışçıl yöntemlerle çözecek şekilde davranmaları sağlanır.

°° Savaşta

Savaşta komutan, muharebe gücünün bilgi unsurunu diğer unsurlarla senkronize eder ve bu sayede düşmanın sadece askeri gücünü değil, sivil karar mekanizmasını da felce uğratmayı amaçlar.

2006 - ABD MÜŞTEREK IO DOKTRİNİ

2006 tarihli müşterek doktrinde, bir önceki 1998 tarihli müşterek doktrine nazaran şu farklılıklar getirilmiştir, özet olarak:

-- 1998 tarihli Müşterek Bilgi Harekâtı Doktrini, 30 Ekim 2003 tarihli Savunma Bakanlığı Bilgi Harekâtı Yol Haritası dokümanı doğrultusunda yeniden değerlendirilmiştir.

-- Taarruz amaçlı bilgi harekâtı ve müdafaa amaçlı bilgi harekâtı deyimlerinin kullanılmasına son verilmiştir. Ancak, bilgi harekâtının hem taarruz hem de müdafaa amaçlı kullanılıyor olması kabul edilmektedir.

-- Bilgi harekâtının temel (çekirdek) becerileri, destekleyici becerileri ve ilgili becerileri yeniden tanımlanmıştır. OPSEC, PSYOP, MILDEC, EW, temel beceriler içerisinde kalırken, fiziki imha çıkarılmış, bilgisayar ağı operasyonları (CNO) eklenmiştir. (Bu değişiklik, 2003 tarihli Kara Kuvvetleri doktrininde yapılmıştı.)

-- Destekleyici beceriler, savaş kamerası (COMCAM), bilgi teminatı (IA), istihbarata karşı koyma (CI) ve fiziki taarruz, becerileri eklenerek yeniden düzenlenmiştir.

-- İlgili beceriler, halkla ilişkiler (PA), sivil askeri harekât (CMO), kamu diplomasisine savunma desteği (DSPD) şeklinde yeniden düzenlenmiştir. (1998 tarihli müşterek doktrinde halkla ilişkiler (PA) ve sivil işler (CA) destekleyici beceriler olarak yer alıyordu.)

-- Bilgi ortamı yeniden tanımlanarak bilgi harekâtı ve askeri harekât ile olan ilişkisi; istihbarat ve haberleşme sisteminin bilgi harekâtına olan desteği ve bilgi harekâtının çokuluslu yönleri tartışılmıştır.

-- Bilgi harbi deyimi, bilgi harekâtı doktrininden çıkarılmıştır.

(olumlu) bilgi ile (olumsuz) harp arasındaki bağlantı kopartılmış.

° Bilgi Ortamı

Bilgi, ulusal güvenlik bakımından hayati, stratejik bir kaynaktır.

Bilgiyi toplayan, işleyen ve dağıtan bireylerin, kuruluşların ve sistemlerin toplamı bilgi ortamını (information environment) oluşturur. Liderler, karar verenler, kişiler ve kurumlar bilgi ortamındaki aktörlerdir. Bilgiyi elde etmek, analiz etmek, uygulamaya koymak ve dağıtmak için gereken malzeme ve sistemler ise bilgi ortamının altyapısını (information infrastructure) oluşturur.

°° Bilgi Ortamının Boyutları

Birbiriyle ilişkili üç boyuttan meydana gelir bilgi ortamı: fiziki (physical), bilgisel (informational) ve bilişsel (cognitive).

°°° Fiziki Boyut (Physical)

Bilgi harekâtının yürütülmesini sağlayan komuta ve kontrol (C^2) sistemleri ve destek altyapısı bilgi ortamının fiziki boyutunu oluşturur. Haberleşme ağının üzerinde konuşlandığı platform, kullanılan teknoloji ve kullanan kişiler de bu boyutta yer alır. Bilgi ortamının fiziki boyutu nispeten daha kolay ölçülebildiğinden bilgi harekâtının savaş gücü genellikle bu boyutla değerlendirilir.

°°° Bilgisel Boyut (Informational)

Bilginin toplanması, işlenmesi, depolanması, dağıtılması, gösterilmesi ve korunması bilgi ortamının bilgisel boyutunu oluşturur. Bilgi akışı, içerik ve modern askeri komuta kontrol (C^2) bu boyutta yürütülür ve dolayısıyla korunması gerekir.

°°° Bilişsel Boyut (Cognitive)

Karar vericilerin ve muhatapların zihinleri bilişsel boyutu oluşturur. Kişiler bu boyutta düşünür, tahayyül eder, algılar ve karar verirler. Liderlik, verilen emirler, personelin eğitimi, tecrübesi, motivasyonu, morali, uyumu, zihinsel durumu, farkındalığı ve bunun yanı sıra medya, kamuoyu, halkın algısı ve söylentiler bu boyutta etkilidir.

Teknolojideki ilerleme, insan bilincinin algılayamayacağı, anlayamayacağı hız ve yoğunlukta bilginin toplanması, işlenmesi, depolanması, dağıtılması, gösterilmesi ve korunmasını gerektirmekte ve bunu mümkün kılmaktadır.

Bilgiyi elde etmek için sınırlı miktarda zaman ve kaynak olduğu göz önüne alınmalı. Kararlar, bilişsel veya otomatik yöntemlerle verilse dahi, bilginin kalitesini iyileştirmek için elde sınırlı zaman ve imkân olduğundan karar mekanizması çoğu zaman sübjektif manipülasyona müsaittir.

°° Bilgi Ortamında Kalite Kriterleri

Kaliteli bilginin bedeli yüksektir. Bilginin kalitesinin değerlendirilmesinde birçok kriter kullanılmaktadır. Hangi kriterin önemli olduğu bilginin kullanım amacına göre değişebilir.

Doğruluk (Accuracy) Gerçek durumu gösteriyor.

Alakalılık (Relevance) Görev veya durumla alakalı.

Zamanındalık (Timeliness) Karar vermeye imkân verecek kadar erken zamanda.

Kullanılabilirlik (Usability) Kolay anlaşılabilir şekilde.

Bütünlük (Completeness) Karar vermek için gereken tüm bilgi var.

Özlülük (Brevity) Sadece gereken ayrıntıda.

Güvenlilik (Security) Gerektiği gibi korunmuş, güvenli.

> 1996 tarihli IO doktrininin Alakalı Bilgi ve İstihbarat bölümünde de benzer kriterlerden söz edilmektedir. 2006 müşterek IO doktrininde ise hassasiyetin yerini özlülük almakta; bilginin gereken ayrıntıda olmasının ötesinde sadece gereken ayrıntıda olması vurgulanmaktadır. Bunda sanırım, geçen on sene içerisinde bilgi ortamında yaşanan gerekli, gereksiz, alakalı, alakasız bilgi artışının, daha doğrusu bilgi kirliliğinin etkisi olsa gerek.

° Bilgi Harekâtının Unsurları

> Muharebenin enstrümanları ancak kullanmayı bilen için değerlidir.
>
> Charles Ardant du Picq

Bilgi harekâtı yürütülürken temel, çekirdek beceriler ile destekleyici beceriler ve ilgili beceriler birbiriyle uyumlu şekilde uygulanır.

> [Bilgi harekâtı unsurlarının çoğu daha önceki IO doktrinlerinde ayrıntılı şekilde açıklanmıştır; dolayısıyla, sadece bu doktrinde yer alan unsurlar açıklanacaktır.]

°° Temel (Çekirdek) Beceriler

Temel beceriler: Psikolojik Harekât (Psychological Operations - PSYOP), Askeri Yanıltma (Military Deception - MILDEC), Harekât Güvenliği (Operations Security - OPSEC), Elektronik Harp (EH) (Electronic Warfare - EW), Bilgisayar Ağı Operasyonları (Computer Network Operations - CNO).

1998 tarihli müşterek IO doktrininde yer alan Fiziki İmha çıkarılmış, yerine 2003 tarihli ordu doktrininde olduğu gibi Bilgisayar Ağı Operasyonları (CNO) eklenmiş; ancak, Bilgisayar Ağı Taarruz (CNA), Bilgisayar Ağı Savunma (CNO) ve Bilgisayar Ağı İstismar (CNE) bunun alt kırılımları olarak gösterilmişti,r.

°° Destekleyici Beceriler

Destekleyici beceriler: Bilgi Teminatı (Information Assurance - IA), Fiziki Emniyet (Physical Security), Fiziki Taarruz (Physical Attack), İstihbarata Karşı Koyma (İKK) (Counterintelligence - CI), Savaş Kamerası (Combat Camera - COMCAM).

1998 tarihli müşterek doktrinde temel beceriler içerisinde yer alan Fiziki İmha (Physical Destruction), temel becerilerden çıkarılarak destekleyici beceriler arasına Fiziki Taarruz olarak dahil edilmiştir. Ayrıca, Fiziki Güvenlik, İstihbarata Karşı Koyma (CI) ve Savaş Kamerası (COMCAM) becerileri de eklenmiştir.

Destekleyici beceriler, temel becerilerle entegre ve koordineli şekilde uygulanmalı.

°°° Fiziki Taarruz

2003 tarihli ordu doktrininde yer alan fiziki imha becerisi bu doktrinde fizik taarruz olarak tanımlanmaktadır.

Askeri harekâtların temelinde bulunan taarruz, bilgi harekâtı için de geçerli bir kavramdır. İmha gücü ile düşmanın hedeflerine zarar vermeyi veya tamamen imha etmeyi içeren bir yöntemdir. Fiziki taarruz vasıtasıyla daha kolay faydalanılabilecek (istismar edilebilecek) bilgi sistemlerini kullanmaya zorlanabilir düşman. Düşmanın bilgi sistemlerinden faydalanmak, imha etmekten daha çok yarar sağlayabilir.

°°° Savaş Kamerası (COMCAM)

Savaş kamerası (Combat Camera - COMCAM) kimi zaman düşmanı etkilemek, kimi zaman dost kuvvetlerin komuta kademesini bilgilendirmek, kimi zamansa halkla ilişkiler (PA), sivil-askeri operasyonlar (CMO), askeri yanıltma (MILDEC) veya psikolojik harekâta (PSYOP) destek vermek amacıyla kullanılabilir. Savaş kamerası (COMCAM) kayıtları bazen müttefikler veya medya ile paylaşılabilir; ancak, harekât güvenliğine (OPSEC) halel gelmemesi için, dışarıya verilmeden önce denetlenmesi gerekir.

°° İlgili Beceriler

İlgili beceriler: Halkla İlişkiler (Public Affairs - PA), Sivil-Askeri Operasyonlar (Civil-Military Operations - CMO) ve Kamu Diplomasisine Savunma Desteği (Defense Support to Public Diplomacy - DSPD).

1998 tarihli müşterek doktrinde destekleyici beceriler olarak tanımlanan Halkla İlişkiler (PA), bu doktrinde ilgili beceriler içerisinde tanımlanmıştır. Sivil İşler (CA) ise Sivil Askeri Operasyonlar (CMO) olarak yeniden tanımlanarak ilgili becerilere dahil edilmiştir.

İlgili beceriler, temel ve destekleyici becerilerle entegre ve koordineli şekilde uygulanmalı.

°°° Kamu Diplomasisine Savunma Desteği (DSPD)

Kamu Diplomasisine Savunma Desteği (DSPD), hükümetin kamu diplomasisini desteklemek amacıyla Savunma Bakanlığı unsurlarının uyguladıkları, sadece bilgi harekâtı ile sınırlı olmayan eylem ve tedbirleri kapsar.

Yurt dışındaki Amerikan vatandaşları ve kurumları ile muhatapları arasındaki diyalog ortamını oluşturmak; yabancı toplum ve kanaat önderlerini anlamak, bilgilendirmek ve nüfuz altına almak vasıtasıyla ABD dış politikasının hayata geçirilmesine yardımcı olabilecek uluslararası açık bilgi aktivitelerinin uygulanmasına katkı sağlar. Onaylanması halinde, bu amaçla psikolojik harekât (PSYOP) unsurlarından da yararlanılabilir.

° Bilgi Harekâtının Prensipleri

Askeri harekâtın başarısı, gerekli bilgiyi elde etmek, değerlendirmek ve entegre etmek, öte yandan düşmanın bunu yapmasını engellemekle alakalıdır. Bu amaçla yürütülen taarruz veya müdafaa amaçlı bilgi harekâtı daha ziyade karar mekanizmalarını ve kararları etkilemeye yöneliktir. Kararlar genellikle o an mevcut bilgiye dayanarak alınır. Ancak, karar vericilerin kullanmakta olduğu bilgi ortamı psikolojik, elektronik veya fiziki yöntemlerle etkilenebilir. Mevcut bilginin hangi kalite kriterine göre kabul edilebilir olduğu ise kişilere, kurumlara, dinlere, kültürlere, coğrafyaya göre farklılık gösterebilir. Bilgi harekâtı karar verme mekanizmasında yer alan kişilere ve/veya otomatik sistemlere yönelik olabilir; ancak, otomatik sistemlere yönelik bilgi harekâtının etkinliği karar vericilerin bu sistemlere olan güveni ve bağımlılığı ile ilişkilidir. Her durumda, gerçek ya da olası düşmanı ABD menfaatlerine zarar verecek eylemlerden caydırmak bilgi harekâtının nihai hedefidir.

° Bilgi Harekâtına İstihbarat Desteği

Bilgi ortamı içerisinde askeri harekâtı planlamadan önce dinamik bilgi ortamının güncel durumu hakkında bilgi toplanmalı, analiz edilmeli ve değerlendirilerek komuta kademesine aktarılmalı. Bu sebeple, bilgi ortamının fiziki, bilgisel, bilişsel özelliklerine ve yürütülmekte olan bilgi harekâtının değerlendirilmesi ile ilgili istihbarata gerek duyulur.

°° Bilgi Harekâtının Planlanmasında İstihbarat

-- İstihbarat kaynakları sınırlıdır.

-- İstihbarat toplamanın hukuki sınırları vardır. İstihbarat, yasal yöntemlerle elde edilmiş olmalı. Ayrıca, kolluk kuvvetleri tarafından yasal yöntemlerle de sağlanabilir istihbarat.

-- Bilgi harekâtı istihbarat desteği uzun zaman alır. Özel kaynakların ve metotların yerleştirilmesi ve uygulanması için zamana ihtiyaç olabilir.

-- Bilgi ortamı dinamiktir, değişkendir. İstihbaratın elde edildiği -ve kullanıldığı- zamanla ilişkisi önemlidir.

Bilgi ortamının özellikleri istihbaratı etkiler. Fiziki ve elektronik bilgi nesnel bakımdan ölçülebilir; ancak, insan doğasının ve psikolojik profillerin öznelliği göz önüne alınmalıdır.

° Planlama ve Koordinasyon

> Teknikte ve mekanizmada uzmanlaş; sanatı ve işi iyi öğren ve ne zaman sapacağını bilecek kadar akıllı ol.
>
> Gen. Anthony Zinni

Erken safhalarda bilgi harekâtından yararlanmak, harekâtın daha ileriki safhalarını etkileyecektir. Bu yüzden, bilgi harekâtının planlanmasına topyekun harekâtın

planlanmasının erken safhasında başlamalı ve eklenti olarak değil, harekâtın bir parçası olarak değerlendirilmeli.

Planlama aşamasında, bir onay otoritesi ve bir de uygulama otoritesi belirlenmeli. ABD silahlı kuvvetleri, kendi topraklarında ve yabancı topraklarda harekât yürütürken mutlaka ABD anayasası, kanunları, ikili anlaşmalar ve uluslararası anlaşmalara riayet etmek durumundadır. Öte yandan, bir bilgi harekâtı uygulamasının yabancı ülkeler tarafından düşmanca bir eylem olarak görülebileceği hususu göz önünde bulundurulmalıdır. Bu yüzden, askeri harekât bünyesindeki herhangi bir bilgi harekâtı uygulamasının kanunlara uygunluğu mutlaka üst seviyede değerlendirilmiş ve onaylanmış olması gerekir.

° Çokuluslu Bilgi Harekâtı

> Kuvvetli bir ulusuz. Ancak, kendi kendimize kuvvetli kalamayız.
>
> George C. Marshall

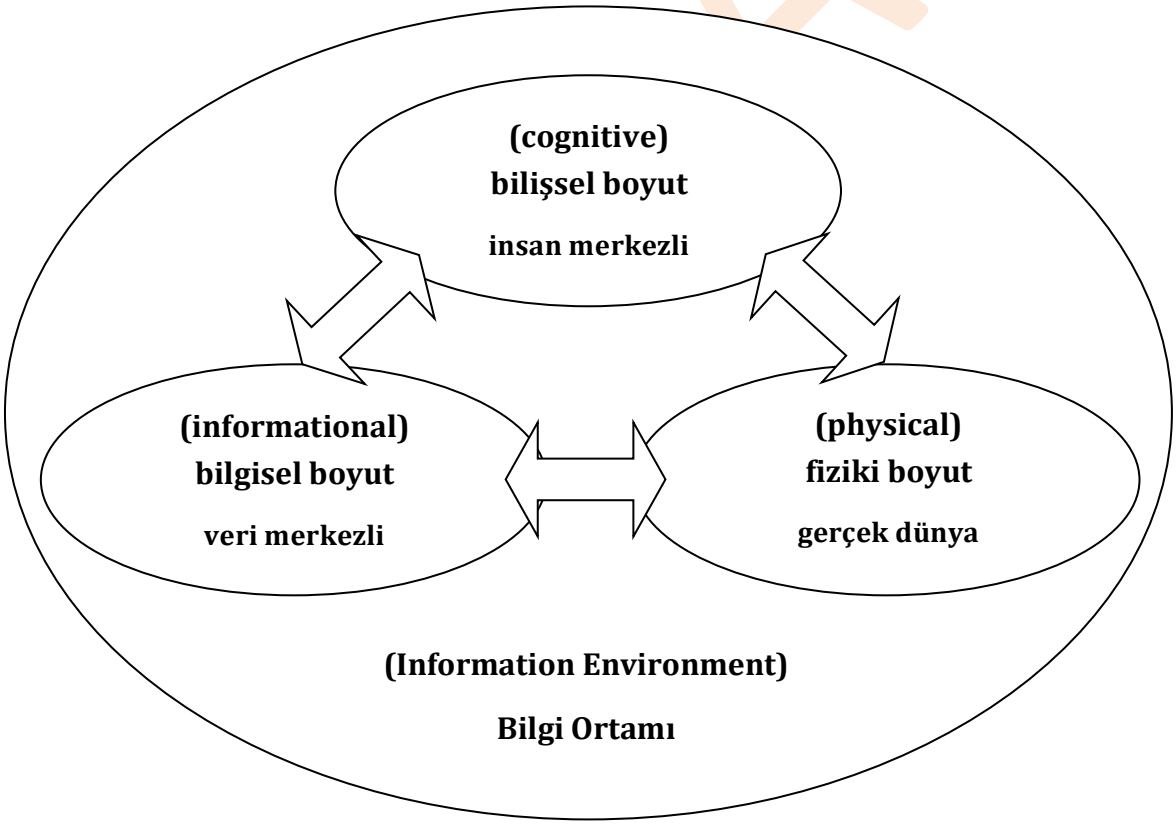
Müttefikler ve koalisyon ortakları farklı bilgi harekâtı kavramlarına itibar ediyor, bazıları çok kapsamlı, sofistike yöntemler kullanıyor olabilirler. Çokuluslu kuvvetlerin komutanı, koalisyondaki her ülkenin bilgi harekâtı programları ve hedefleri arasındaki çelişkileri gidermelidir. Bu çelişkileri gidermek, farklı bilgi harekâtı kavramları arasında entegrasyonu sağlamak için müttefiklerin bilgi harekâtı hedeflerini bilmek durumundadır. Bu amaçla, müttefik veya koalisyon ortaklarının doktrin, taktik, teknik ve prosedürlerinin askeri ve bilgi ortamı ile alakalı hukuki zorunlulukları ve bunun yanı sıra menfaat ve kaygıları, kültürel değerleri ve kurumları, etik ve ahlaki farklılıkları gibi konularda da bilgi sahibi olmak gerekir.

2012 - ABD MÜŞTEREK IO DOKTRİNİ

Ulusal gücün ekonomik, diplomatik, askeri ve bilgi enstrümanları ABD liderlerine dünyadaki krizlerle başa çıkma yollarını ve vasıtalarını sağlamaktadır. Bu vasıtaların bilgi ortamında kullanılması, nerdeyse gerçek zamanda bilginin emniyetli şekilde aktarılması, alınması, depolanması ve işlenmesi becerisini gerektirmektedir. Bu yeni teknolojinin farkında olan düşmanların da geleneksel askeri yöntemlerin yanı sıra, bilgi ortamını ele geçirmek amacıyla bilgi ile alakalı becerileri (Information Related Capability - IRC) kullanacakları aşikârdır. Bu sebepledir ki bilgi ortamı artık bir muharebe alanına dönüşmüştür.

° Bilgi Ortamı

Bilgiyi toplayan, işleyen, dağıtan ve kullanan bireyler, kuruluşlar ve sistemlerin toplamı bilgi ortamını oluşturur. Bu ortam, fiziksel, bilgisel ve bilişsel olmak üzere birbiriyle ilişkili üç boyuttan meydana gelir.



°°° Fiziki Boyut (Physical)

Bilgi harekâtının yürütülmesini sağlayan komuta ve kontrol (C^2) sistemleri ve destek altyapısı bilgi ortamının fiziki boyutunu oluşturur. Haberleşme ağının üzerinde konuşlandığı platform, kullanılan teknoloji, gazeteler, kitaplar, mikrodalga kuleleri, bilgisayarlar, tabletler, akıllı telefonlar, kullanan kişiler gibi ölçülebilen her türlü nesne fiziki boyut içerisinde yer alır. Bilgi ortamının fiziki boyutunu sadece askeri veya ulusal sınırlar içerisinde değil, ulusal, coğrafi ve ekonomik sınırların ötesinde değerlendirmek gerekir.

°°° Bilgisel Boyut (Informational)

Bilginin toplanması, işlenmesi, depolanması, dağıtılması, gösterilmesi ve korunması bilgi ortamının bilgisel boyutunu oluşturur. Modern askeri komuta kontrol (C^2) bu boyutta yürütülür ve bu boyutta yürütülen işlemler bilginin akışını ve içeriğini etkiler.

°°° Bilişsel Boyut (Cognitive)

Bilgiyi aktaran, alan ve işlem yapanların zihinleri bilişsel boyutu oluşturur. Bilişsel boyut, bireylerin veya grupların bilgiyi işleme, algılama, muhakeme ve karar süreçleri ile alakalıdır. Bireysel veya kültürel inançlar, normlar, zaaflar, güdüler, duygular, deneyimler, ideolojiler, töreler, kimlikler, eğitim, akıl sağlığı gibi faktörler bilişsel boyutun unsurlarını etkileyen etmenlerdir. Belirli bir ortamda bu etmenleri tanımlamak, karar vericilerin nasıl etkileneceğini ve en iyi sonucun alınacağını belirlemek bakımından oldukça önemlidir. Bu yüzdendir ki bilişsel boyut, bilgi ortamının en önemli bileşenidir.

° Bilgi Harekâtı

Bilgi harekâtının esası tekil becerilere sahip olmak değil, arzu edilen etkiyi elde etmek için bu becerileri bir kuvvet çarpanı olarak kullanabilmektir. Bilgi harekâtının yürütülmesine katkıda bulunan birçok askeri beceri vardır ki planlama aşamasında bunların dikkate alınıyor olması gerekir.

°° Bilgiyle Alakalı Beceriler (IRC)

Tüm olası seçenekleri kapsamasa da, bilgi harekâtının yürütülmesinde aşağıda belirtilen Bilgiyle Alakalı Beceriler (Information Related Capabilities - IRC) kullanılabilir:

> Daha önceki doktrinlerde temel (çekirdek) beceriler, destekleyici beceriler, ilgili beceriler diye ayrıntılı sınıflandırılan beceriler bu doktrinde tek bir sınıf altında toplanmıştır. Herhalde, doktrini hazırlayanlar bu becerileri sınıflandırmanın pek anlamlı olmadığını, yeri geldiğinde her becerinin bir diğeri kadar önemli olduğunu, bilgi harekâtı becerilerinin birbiriyle uyum içerisinde uygulanmasının lüzumunu anlamış olsalar gerek.

(1) Stratejik İletişim (Strategic Communication - SC)

Stratejik iletişim (SC) süreci, koordineli programlar, planlar, temalar, mesajlar ve ulusal gücün tüm enstrümanlarının eylemleri ile senkronize ürünler vasıtasıyla önemli muhatapları anlayarak ve onlarla temas kurarak, ulusal menfaatlerin, politikaların ve hedeflerin geliştirilmesi için uygun koşulların yaratılması, güçlendirilmesi ve korunması çabalarını kapsar.

> ABD'nin Ankara Büyükelçisinin doğu ve güneydoğu illerimizi kapsayan nabız yoklama gezisi stratejik iletişimin örneğidir.

(2) Kurumlar arası müşterek koordinasyon

Kurumlar arası koordinasyon, Savunma Bakanlığı (DoD) ile diğer resmi kurumlar, özel sektör, gayri resmi kuruluşlar ve kritik altyapı etkinlikleri arasında ulusal amaçlarla yürütülen koordinasyon faaliyetidir.

(3) Halkla İlişkiler (Public Affairs - PA)

Halkla ilişkiler (PA), Savunma Bakanlığı'nın operasyonları ile alakalı olarak gerek iç gerekse dış kamuoyuna yönelik bilgi aktarma ve ilişki kurma faaliyetidir.

(4) Sivil-Askeri Operasyonlar (Civil-Military Operations - CMO)

Sivil-askeri operasyonlar (CMO), ABD hedeflerine ulaşabilmek amacıyla dost, tarafsız veya düşman ortamlarda askeri kuvvetler ile resmi veya gayri resmi kuruluşlar ve sivil topluluklar arasındaki ilişkileri kurmak, sürdürmek, etkilemek ve onlardan faydalanmak şeklinde tanımlanabilir.

Bu faaliyetler, askeri harekât öncesinde, süresince veya sonrasında yürütülüyor olabilir. CMO personelin işlevi normalde yerel otorite veya hükümet tarafından sağlanan imkânlarla yürütülür ki bu da onları yerel sivil topluluklarla direkt temas halinde olmaları ve yerel toplulukların algılarını etkilemeleri sonucunu doğurur. Topluluklar içerisinde düşman unsurlar da bulunabileceğinden, yaratılan algı çok önemlidir.

Sivil-askeri operasyonlar (CMO) ile bilgi harekâtı (IO), birçok ortak noktaları olmasına rağmen tamamen farklı disiplinlerdir. Bilgi harekâtı açısından hedef kitle (Target Audience -TA) daha ziyade düşman olmakla beraber, uygulanan beceriler (IRC) dost veya tarafsızları da etkileyebilir. Benzer şekilde, CMO daha ziyade dost ve tarafsız topluluklara yönelik yürütülürken, potansiyel düşman kitle de etkileniyor olabilir.

(5) Siber (Siberuzay) Operasyonlar (Cyberspace Operations - CO)

Siberuzay, internet, haberleşme ağları, bilgisayar sistemleri, gömülü işlemciler ve denetleyiciler içeren birbiriyle bağlantılı bilgi teknolojisi altyapısı ve içerdiği verinin oluşturduğu bilgi ortamını bünyesinde barındıran bir küresel alandır. Siber operasyon becerisi, bilgi harekâtını desteklemek amacıyla kullanıldığında, belirli bir bilgi ortamını veya bir siber kimliği hedefleyerek düşmanın karar mekanizmasını manipüle eder veya çalışmaz hale getirir.

(6) Bilgi Teminatı (Information Assurance - IA)

Bilgi üstünlüğünü elde etmek için bilgi teminatı (IA) gereklidir. Ayrıca, siber operasyonlar ile bilgi teminatı, birbiriyle bağlantılı ve biri diğerine destek olması gereken becerilerdir.

(7) Uzay Operasyonları (Space Operations)

Uzay operasyonları, müşterek harekât çerçevesinde önemli bir kuvvet çarpanıdır. İstihbarat, keşif ve gözetleme, çevresel etkileri izleme, füze uyarı, uydu haberleşme, uzayda konuşlu yön bulma, konumlama ve zamanlama gibi işlevlerle bilgi harekâtına destek sağlar.

(8) Askeri Bilgi Destek Operasyonları (Military Information Support Operations - MISO)

Askeri bilgi destek operasyonları (MISO), yabancı muhataplara sadece seçili bilgi aktararak onların duygularını, objektif muhakeme yetilerini ve nihayetinde hükümetlerin, kurumların, grupların veya bireylerin davranışlarını etkilemeye yönelik planlı operasyonlardır.

(9) İstihbarat

İstihbarat, bilgi ortamını meydana getiren fiziki, bilgisel ve bilişsel boyutlar arasındaki ilişkiyi anlaşılır kılan ve bilgi harekâtını destekleyen, yaşamsal bir askeri beceridir.

> Söz konusu askeri doktrin olduğundan, askeri beceri olarak tanımlanmıştır, istihbarat. Esasında askeri tanımın ötesinde değerlendirmekte yarar vardır.

(10) Askeri Yanıltma (Military Deception - MILDEC)

Bilgiyle alakalı becerilerin en eskilerinden biri olan askeri yanıltma (MILDEC), dost kuvvetlerin başarısı için düşmanın karar vericilerini yanıltmayı amaçlar. Ancak, sadece yanıltmak yeterli değildir; dost kuvvetlere avantaj sağlayacak davranışlar göstermelerini sağlamak lazım gelir.

(11) Harekât Güvenliği (Operations Security - OPSEC)

Harekât güvenliği (OPSEC), düşmanın kritik bilgiye ve belirtiler ulaşmasını engelleyerek belirli zafiyet noktaları ile ilgili tehlikeyi azaltmak amacıyla yürütülen standart uygulamalardan oluşur.

(12) Özel Teknik Operasyonlar (Special Technical Operations - STO)

Bilgi harekâtı (IO) ile özel teknik operasyonlar (STO) senkronize edilmeli ve çatışması engellenmeli.

> Savunma Bakanlığı haricindeki CIA, NSA, Dışişleri Bakanlığı gibi kurumlara askeri operasyon desteği vermek üzere Soğuk Savaş günlerinde Pentagon bünyesinde

kurulmuş olan Özel Teknik Operasyonlar (STO) biriminin yöntemleri bilgi harekâtı (IO) ile benzer olduğundan olası çatışmaların engellenmesi gerekir.

(13) Müşterek Elektromanyetik Spektrum Operasyonları (Joint Electromagnetic Spectrum Operations - JEMSO)

Bilgi ile alakalı tüm görevler artık gittikçe elektromanyetik spektruma (EMS) bağımlı hale gelmekte. Elektronik harp (EW) ve müşterek elektromanyetik spektrum yönetiminden oluşan müşterek elektromanyetik spektrum operasyonları (JEMSO) becerisi elektromanyetik spektruma bağımlı operasyonların amaçlandığı şekilde yürütülmesini sağlar.

(14) Önemli Lider Teması (Key Leader Engagement - KLE)

Yabancı muhatapların önemli (anahtar) liderleriyle ABD askeri liderleri arasında sağlanan temas (angajman), politika değişikliği veya müşterek kuvvetler komutanının (JFC) hedeflerini desteklemek gibi tanımlı amaçlarla gerçekleştirilen kasti ve planlı bir temastır. Bu tür temaslar, yabancı liderleri veya karar vericileri stratejik, operasyonel, taktik seviyede etkilemek ve şekillendirmek amacıyla kullanılabilir veya ABD kuvvetlerine olan inanç ve güveni sağlamlaştırmak amacıyla akademik liderler, dini liderler ve aşiret liderleri gibi belirli gruplara yönlendirilebilir.

Daha önceki IO doktrinlerinde yer alan en temel becerilerden biri olan psikolojik harekât (PSYOP) bu doktrinde yer almamaktadır. İlginç...

° Hukuki Sorumluluk

Bilgi ortamındaki ABD askeri faaliyeti, diğer askeri operasyonlarda olduğu gibi, kanunlar ve kurallar çerçevesinde yürütülür. Müşterek bilgi harekâtı her zaman sadece yerel değil, ulusal seviyede koordinasyon ve onay gerektiren hukuki ve idari meseleler içerir. ABD Anayasası, kanunları, kuralları, politikaları ve uluslararası hukuk, bilgi harekâtı dahil olmak üzere tüm askeri faaliyetleri sınırlar. ABD kuvvetleri, ister ABD dışındaki yerlerde, ister sanal bilgi ortamında faaliyet gösteriyor olsun, ABD kanunlarına ve uluslararası harp hukukuna riayet etmekle yükümlüdürler.

Ülkemizin huzur ve refahı için sorumluluk üstlendiğinde, en cesur korkmalı ve en akıllı ürpermeli.

ABD Başkanı James K. Polk, 1845

[tam metin: Ülkemizin huzur ve refahı ve bir bakıma tüm insanlığın umudu ve mutluluğu için sorumluluk üstlendiğinde, ...]

Bilgi harekâtı planlamacıları çok çeşitli ve karmaşık hukuki değerlendirmelerle uğraşmak durumundadırlar. Hukuki yorumlar, zaman zaman, ilgili teknolojilerin karmaşıklığına veya etkilenen menfaatlerin önemine göre değişiklik gösterebilir ve hatta bilgi ile alakalı becerilerin (IRC) uygulama pratiği ve teknolojik değişimler mevcut kanunların güncellenmesini gerekli kılabilir. Öte yandan, kurallar, politikalar sürekli değişmekte, feshedilmekte veya yenisi eklenmekte. Dolayısıyla, bilgi harekâtı nihayetinde, çokuluslu operasyonlar ve her ülkenin kendi kanunları, politikaları ve onay

süreçleri ile daha da karmaşık hale gelen bir arenada yürütülmek durumundadır. Bu sebepledir ki müşterek bilgi harekâtı planlamacılarının uzman görüşü için hukuk müşavirine danışmaları gerekir.

Ancak, tüm bu derleme göstermektedir ki bilgi harekâtı veya bilgi harbi, layıkıyla uygulandığında, tespit edilmesi, engellenmesi veya hukuki tedbir veya müeyyide uygulanması hayli zor bir harp sanatıdır.

ABD SİBER OPERASYONLAR DOKTRİNİ

[Müşterek Siberuzay Operasyonlar Doktrini (JP 3-12 Joint Cyberspace Operations) 2013 başı itibariyle henüz yazım/onay aşamasında olduğundan bu başlık altında ABD Hava Kuvvetleri'nin AFDD 3-12 Cyberspace Operations doktrini incelenmiştir. Bilgi harekâtı konusunda olduğu gibi, bu konuda da müşterek doktrinin bu dokümanı temel alacağı kuvvetle muhtemeldir.]

° Tanımlar

Siberuzay İnternet, haberleşme ağları, bilgisayar sistemleri ve gömülü işlemciler ve denetleyiciler içeren, birbiriyle bağlantılı bilgi teknolojisi altyapısı.

Siber (siberuzay) operasyonlar Siberuzayda askeri hedefler elde etmek veya etki yaratmak amacıyla siber becerilerin uygulanması.

Siber (siberuzay) üstünlük Engellenmeden, herhangi bir zamanda ve herhangi alanda operasyon yürütecek şekilde siberuzayda avantaj elde etmek.

Siber üstünlük, zamanda ve mekânda sınırlı olabileceği gibi, geniş erimli ve uzun süreli de olabilir. Siber üstünlük kavramı, müşterek kuvvetlerin arzu ettikleri etkiyi elde etmelerini önleyecek şekilde düşman kuvvetlerden kaynaklanan girişimi engellemek üzerine inşa edilmiştir. [girişim: parazit, karıştırma, müdahale; (İng.) interference] Üstünlük, girişimin etkinliğine engel olur; ancak bu demek değildir ki girişim tamamen engellenebilir. Girişim söz konusu olsa da harekâtın sağlıklı yürütülmesine etkisi olmayabilir.

Arzu edilen tam üstünlük sağlamak olsa da, bu her zaman mümkün olmayabilir. Sadece görevle sınırlı veya yerel siber üstünlük dahi arzu edilen etkinin elde edilmesi için yeterli olabilir. Dolayısıyla komutan, görevi gerçekleştirebilecek kadar üstünlük sağlayacak çabayı göstermeli.

° Siberuzayı Anlamak

Bilgi harekâtı, siberuzayda veya başka alanlarda yürütülen operasyonlar kümesidir. Siberuzayda yürütülen operasyonlar direkt olarak bilgi harekâtını etkileyebilir; buna karşılık, siber özellikte olmayan bilgi harekâtı eylemleri de siberuzayı etkileyebilir.

Siberuzay, insan tarafından oluşturulmuş bir alandır; kara, deniz, hava, uzay alanlarına benzemez; varlığını sürdürebilmek için insanların devamlı ilgisine muhtaçtır.

Siberuzaydaki şebekeler birbirleriyle ilişkili ve birbirlerine bağımlı olsalar da bazı bölümleri ayrılmış ve yalıtılmıştır. Fiziksel ayırım, firewall'lar, protokoller ve şifreleme ile siberuzayda yalıtım, sağlanabilir. Şebekeler siberuzayda yalıtıldığında küresel ağlara kontrollü bağlantı sağlanmış olur.

Siberuzayın parçaları elektronik sistemler ve elektromanyetik spektrumun bölümleri vasıtasıyla birbirine bağlanmıştır ve yeni sistemler veya teknolojiler geliştirildikçe bu vasıtalar elektromanyetik spektrumun başka bölümlerini de kapsayabilir, daha büyük kapasitede ve daha hızlı olabilir, daha fazla bant genişliği içerebilir. Zamanla sistemlerin elektromanyetik spektrum içerisindeki yerleri (frekansları) değişebilir. Siberuzayda gerçekleştirilen bir fiziki manevradır bu.

Mantıki (logical) boyutta da manevralar gerçekleştirilebilir. Örneğin, güvenli bir sunucuya sızmak istendiğinde bu sunucuyu koruyan yazılımda bir mantık hatası aranır. Saldıran, bu hatayı ortaya çıkaracak kodu yazar; sunucuyu koruyan ise bunu tespit ettiğinde, onu etkisiz kılacak kodu yazar. Saldıran buna karşı bir başka kod yazar… İşte bu da mantık boyutunda yapılan manevradır. Siberuzayda yürütülen mücadele hem fiziki hem de mantıki manevralardan meydana gelir ki her ikisi de gereklidir.

> Bu aşamada Martin Libicki tarafından tanımlanan, siberuzayın üç kademesine kısa bir bakış atmak yararlı olabilir:
>
> Conquest in Cyberspace (Siberuzayda Fetih) adlı kitabında siberuzayı üç katmana ayırır Libicki: fiziki, sentaktik ve semantik. Bilginin aktarılmasını, depolanmasını ve anlaşılır hale gelmesini sağlayan donanım ve altyapı fiziki katmanı oluşturur. Sentaktik katman ise, fiziki katman içerisindeki bilginin formatlanması, aktarılması, depolanması, anlaşılır hale gelmesi için gereken algoritmalar, protokoller, yani yazılımdan oluşur. Semantik katmanda, artık, bilginin kendisi vardır.
>
> Bu katmanlar, bilgisayar ağlarını modellemek amacıyla ISO tarafından geliştirilmiş olan OSI modeli ile benzerlik göstermektedir.
>
> Bir başka modelde ise siberuzay; altyapı, fiziki, sentaktik, semantik olmak üzere, dört katmandan oluşmaktadır. Bu modelde, kablolama ve donanım altyapı katmanında yer alırken, fiziki katmanda bu altyapıya can veren elektromanyetik enerji, fotonlar, frekanslar yer almaktadır -ki bana göre gereksiz bir ayırım.

° Harekât Ortamı

Siberuzay, modern yaşamın her yönü için çok önemli işlemlerin yürütüldüğü bir mecradır, şimdilerde. Sivil toplum ve asker, gittikçe artan şekilde bağımlıdır siberuzaya. Modern toplum için siberuzay hem bir güç hem de zafiyet kaynağıdır. Siberuzayda yürütülen faaliyet, modern toplum için birçok imkân sağlamanın yanı sıra düşmanın faydalanabileceği veya saldırabileceği zaafları da içermektedir. Endüstriyel kontrol, elektrik, su, gaz şebekeleri, bankacılık sistemi, haberleşme ve ulusal güvenlik artık ağ tabanlı yapılar üzerindedir. Son otuz yıl içerisinde gerçekleşen bu gelişme sayesinde

toplum büyük fayda sağlamışken ciddi kırılganlıklar da ortaya çıkmıştır. Hasımlar, siber (siberuzayda) saldırılarla kritik altyapıyı imha edebilir, düzgün çalışmaz hale getirebilir veya ondan -kendi lehine- faydalanabilir ve bundan dost savaş sistemleri, hatta tüm ülke zarar görebilir.

Siberuzaydaki düşmanlar asgari teknoloji içeren yatırım ve düşük maliyetli, kolay erişilebilen kaynaklardan yararlanarak ciddi zarara yol açabilirler. Ticari (raftan alınabilen ticari, Commercial Off-The-Shelf - COTS) teknoloji onlara, askeri amaçlar için uyarlayabilecekleri oldukça kullanışlı ve ucuz teknolojik imkânlar sunmaktadır. Bu sayede, gittikçe daha gelişkin sistemler ve sofistike yöntemler kullanılmaktadır.

° Siberuzay Altyapı İlişkileri

(ABD) Hava Kuvvetleri, eğitim, nakliye ve normal operasyonları dahil, çoğu faaliyetini yürütürken ABD'nin kritik altyapısı ve kaynaklarına bağımlıdır. Bu altyapı ve kaynakların fiziki bakımdan korunması yeterli olmamaktadır artık; çünkü birçoğu endüstriyel kontrol sistemleri (Industrial Control System - ICS) tarafından yönetilmektedir.

Öte yandan, teknolojik ilerlemelerde özel sektör önemli rol oynadığı için askeriye gittikçe artan oranda COTS teknolojiye bağımlı hale gelmektedir. Üreticiler üzerinde yabancıların sahipliği ve denetimi veya küresel tedarik zincirinde meydana gelebilecek aksaklıklar sebebiyle bu bağımlılık bazı zaaflara yol açabilir: COTS üreticileri, servis sunucuları, tedarik zincirinin halkaları düşman tarafından etkilenebilir, ürünlerin içine güvenlik açığına yol açabilecek donanım veya yazılım yerleştirilebilir.

> Birinci bölümde bir nebze değindiğim paranoya burada da kendini gösteriyor. Bir miktar haklılık payı olsa da, unutmamalı ki eğer 1990'ların ortasında başlatılan COTS kullanımı geçen yirmi yılda bu denli yaygınlaşmasaydı, askeri teknoloji şimdilerde sivil teknolojinin çok gerisinde kalmış olurdu. Askeri teknoloji, COTS kullanmasa da zaten sivil teknolojiye her halükârda yenik düşecekti; hatta kullanmadığı o sivil teknolojinin nasıl çalıştığını dahi anlamadan.
>
> Tabii ki daha önce bahsi edilen Stuxnet ve benzeri örnekler bu paranoyayı destekliyor ama -COTS veya değil- güvenlikle ilgili her hususta olduğu gibi, mesele daima iyi yönetim meselesidir.
>
> Karar verirken konunun ticari boyutunu da göz ardı etmemek gerekir. Yeterli yetkinlikte olmayan bazı yerli üreticilerin bu paranoyayı gündeme getirerek ve iyi niyetli yetkililerin ağzından dillendirerek haksız kazanç elde etmeye çalıştıkları durumlar da söz konusu olabilir.
>
> Çözüm: -her işte olduğu gibi- dünyayı tanımak, teknolojiyi bilmek, ihtiyacı değerlendirmek, tedbir almak, denetlemek, iyi uygulamak; kısaca, iyi yönetmek.

° Ulusal Siberuzay Politikası

-- Tehditler ve zaaflarla ilgili farkındalık yaratarak günün acil tehditlerine karşı savunma cephesi oluşturmak.

-- İstihbarata karşı koyma becerilerini geliştirerek ve anahtar bilgi teknolojilerinde tedarik zincirinin güvenliğini artırarak tehditlere karşı korunmak.

-- Strateji belirleme ve geliştirme ile koordineli şekilde araştırma, geliştirme ve eğitime önem vermek.

> Birinci bölümde konu edilen, ABD Başkanı Barack Obama'nın konuşmasında siber güvenlik, ülkenin karşılaştığı en ciddi ekonomik ve ulusal mesele olarak kabul edilmekte ve bununla baş etmeye yeterince hazırlıklı olmadıklarının altı çizilmektedir. Göreve geldikten hemen sonra ABD Başkan'ı, bilgi ve haberleşme altyapısının ayrıntılı şekilde incelenmesi ve Amerika'nın siber güvenliğinin sağlanmasına yönelik kapsamlı bir geliştirme çalışması için talimat vermiştir. Bu amaçla, devlet ve özel sektörün tüm imkânlarını seferber ederek birlikte çalışması, ileri teknoloji yatırımı yapması, her alanda siber güvenlik farkındalığı yaratması, eğitimi geliştirmesi ve yirmi birinci yüzyılın sayısal işgücünü oluşturması önerilmekte ve tabii ki tüm bunlar yapılırken Amerikalılar tarafından kullanılan ve Anayasa ile garanti altına alınmış olan özgürlükler ve mahremiyet haklarının çiğnenmemesi gereği de vurgulanmaktadır.

Siberuzayı güvenlik altına alabilmek için geliştirilen ulusal strateji üç ana başlıktan oluşmaktadır:

-- Amerika'nın kritik altyapısına yönelik siber saldırıların engellenmesi;

-- Siber saldırılara karşı zafiyetin azaltılması;

-- Siber saldırıların zararlarının azaltılması ve kısa sürede toparlanma.

Esasta bu strateji, Amerikan vatandaşlarının kendi sahip oldukları, kullandıkları ve kontrol ettikleri siberuzayı güvenli kılmalarını sağlamayı amaçlamaktadır.

° Tehditler

Ülke güvenliğine yönelik diğer alanlardaki tehditler diğer ülkelerden veya ülkeleri aşan terörist gruplardan gelebilir; ancak bu oldukça büyük kaynak gerektirir. Halbuki siberuzay herkes için oldukça kolay elde edilebilen asimetrik avantajlar sağlar.

Siberuzay söz konusu olduğunda birçok tehdit dikkate alınmalıdır:

Ulus devletler Potansiyel olarak en tehlikeli tehdittir, çünkü devletler çok geniş kaynaklara sahip olabilirler. Bu tehdit, bilinen düşman devletlerden kaynaklanabileceği gibi, özellikle istihbarat söz konusu olduğunda dost devletlerden de kaynaklanabilir.

Uluslarötesi (transnational) aktörler Ulusal sınırlarla bağlı olmayan formal veya gayri formal yapılar, para toplamak, hedef muhataplarla haberleşebilmek, eleman

devşirmek, hükümete olan güveni bozmak, operasyonlar planlamak ve hatta doğrudan terörist saldırılar için siberuzaydan yararlanabilirler.

Suç Örgütleri Ulusal veya uluslarötesi suç örgütleri kendi kullanımları veya başkasına satmak için siberuzayda bilgi elde etmek isteyebilirler.

Kişiler veya Küçük Gruplar Daha ziyade hacker diye bilinen kişiler veya küçük gruplar bilgisayar ağlarına ve bilgisayarlara erişebilirler. Bazıları zarar verme niyetlisi değildir; sadece sistemlerin açıklarını bulmak veya becerilerini ispatlamak için yaparlar. Hatta sistemlerin sahiplerine yardım ettikleri de olur. Bazıları politik amaçlarla mesaj yaymak veya otoriteye karşı güçlü olduklarını göstermek için yaparlar. Bir kısmı ise finans veya devlet kurumlarının bilgi sistemlerine saldırarak karmaşa yaratmayı hedeflerler. Bazı durumlarda, suç örgütleri veya düşman organizasyonlar gibi kimliğini gizleyen başka tehditler de hacker'lardan yararlanıyor olabilirler.

Geleneksel Tehdit Geleneksel tehditler, bilinen askeri becerileri uygulayan düşman devletlerden kaynaklanabilir. Oldukça gelişkin ve karmaşık olan bu tehditler daha ziyade askeri hedeflere ve amaçlara yöneliktir.

Düzensiz Tehdit Düzensiz tehditler, geleneksel yöntemlerin dışında asimetrik yöntemlerle siberuzayı kullanan ve onun yararlarını ortadan kaldıran tehditlerdir. Örneğin, teröristler bir yandan finans ve endüstri kuruluşlarına saldırmak için siberuzaydan yararlanırken, öte yandan fiziki saldırılar da düzenleyebilirler. Suç unsurları veya politik ajanda yaratmak isteyenler kendi menfaatleri ya da amaçları doğrultusunda siberuzayı kullanırlar.

Katastrofik Tehdit Katastrofik tehditler, kitle imha silahlarının ele geçirilmesini ve kullanılmasını hedefler. Bu sayede meydan getirilecek bir elektromanyetik darbe (Elektromagnetic Pulse - EMP) vasıtasıyla siberuzayın büyük bir bölümü tamamen çalışmaz hale getirilebilir.

Yıkıcı Tehdit Savaş ortamlarında var olan ABD'nin halihazırdaki avantajlarını azaltacak veya ortadan kaldıracak derecede önemli teknolojik atılımlar yıkıcı tehdit oluşturabilir. Dünya çapında yürütülen araştırma, geliştirme, yatırım ve endüstriyel çalışmalar bu tür teknolojik atılımları mümkün kılan bir ortam yaratmaktadır. Siber teknolojilerin dünya çapında gittikçe yaygınlaşıyor olmasının yaratabileceği fırsatlara karşı Savunma Bakanlığı (DoD) hazırlıklı olmalıdır.

Doğal Tehdit Seller, kasırgalar, yıldırımlar, güneş fırtınaları gibi doğal olaylar ve afetler siberuzaya zarar verebilir. Bu tür olaylar, düşmanlar için de fırsatlar yaratabilir.

Tesadüfi (Kazaen) Tehdit Önceden öngörülemeyen, kazaen meydana gelen bu tür tehditler, kasıtsız da olsa, siberuzaydaki operasyonlara zarar verebilir.

> Kazaen de olsalar bu tür tehditlerin büyük oranda önlenebilmesi mümkündür; bu amaçla standart (iyi) çalışma yöntemleri belirlenmeli, mümkünse yönergeler hazırlanmalı ve ciddiyetle uygulanmalı; tesadüfün yıkıcı etkisine karşı tedbir alınmalı.

İç Tehdit İç tehditler, bilgi ağına, bilgi sistemlerine ve bilgiye erişim yetkisi olan, güvenilir olduğu kabul edilen kişilerdir.

> Askeri ortamlarda değil belki ama sivil ortamlardaki tehditlerin nicelik ve nitelik olarak en fazla zarar veren türü iç tehdittir.

ALGI YÖNETİMİ

Günümüz bilgi çağında algı yönetimi (Perception Management) gittikçe önemli olan ve oldukça yaygın kullanılan bir harp ve aynı zamanda barış vasıtasıdır.

> Bu bağlamda, yanlış algı yönetimi (misperception management) belki daha doğru bir tanım olabilirdi.
>
> 2001-2007 tarihli askeri tanımlar dokümanında algı yönetimi ve psikolojik harekât aynı şekilde tanımlanmıştır.* Bu durumda anlaşılmaktadır ki psikolojik harekât aslında algı (yanlış algı) yönetiminden başka bir şey değildir.
>
> (*) Bilahare, 2010-2013 tarihli dokümandan her ikisi de çıkarılmıştır. 2012 tarihli bilgi harekâtı (IO) doktrininde de psikolojik harekât becerisi yer almamaktadır. İlginç…

Algı yönetimi, özellikle barışta, mutlaka yanlış haber yaymak demek değildir. Amaç, bir algıyı pekiştirmek veya çatışmayı engellemek için bir ülkenin üst düzey yöneticilerini veya karar mercilerini etkilemektir. Genellikle, uzun zamana yayılan, karmaşık bir süreçtir bu.

Düşmanın yeteneklerini bilmek tabii ki önemlidir; ancak, etkili olabilmek için onun liderlerini, karar mekanizmasını, düşünce yapısını, kültür ve tarihini de anlamak gerekir.

° Temel Dayanaklar, Unsurlar

Algı yönetiminde başarılı olmaya yardımcı iki temel dayanak vardır: meşruiyet ve inandırıcılık. Hedef kitlenin ve uluslararası camianın desteğini sağlamada meşruiyet önemli rol oynar. İnandırıcılık ise, yapılacağı söylenenin yapılmasıdır. Düşman, ancak bu şekilde inanır söylenene.

> Bu iki dayanak, meşruiyet ve inandırıcılık algısı sağlandıktan sonra söylenenin veya yapılanın ne olduğu pek önemli değildir.

Moda tabirle küresel köy haline gelen günümüz dünyasında toplumlar manipülasyona açıktırlar; toplulukların algısının değiştirilmesi, hatta yaratılması mümkündür. Bunu mümkün kılan birçok unsur vardır: dünya medyası, fasılasız haber akışı, gerçek zamanda haber alma, kolay ve düşük maliyetli görüntülü haber imkânı ve tabii ki internet.

Tüm bunlar, algı yönetiminin en önemli unsuru olarak tek bir kelimeye indirgenebilir: medya.

° Prensipler

Birinci prensip: algı yönetimi, öncelikle planlı, koordine bir harekât olarak ele alınmalıdır.

İkinci önemli prensip, şartlandırmadır. Özellikle yerleşik inanç ve kanaate aykırı durumlar söz konusu olduğunda, muhatap kitle dobra bir ifadeyle önüne getirileni kabul etmeme eğilimindedir. Halbuki, zamana yayılmış olarak azar azar getirilen değişiklikler daha kolay kabul edilebilir.

Üçüncü prensip, manipülasyondur. Var olan inancı manipüle etmek veya onu işlemek, yanlış kanıtlar göstererek onu değiştirmekten daha kolaydır. Büyük toplulukların ve özellikle uluslararası kamuoyunun inançlarını değiştirmek çok zordur. Kanıt bulmaya ve göstermeye çalışmaktansa manipülasyon üzerine yoğunlaşmak daha etkili olur.

Sadece yanlış kanıtlar değil, doğru kanıtlar gösterilse dahi yerleşik inancı değiştirmek çoğu zaman kolay, hatta mümkün olmaz.

Algı yönetiminde olguların rolü çok azdır. (Adı üzerinde; algı yönetimi…)

Her ne kadar üçüncü prensibe aykırı gibi görünse de, bazen ve az miktarda gerçekten yararlanmak dördüncü prensip olarak değerlendirilebilir. İnançların aksine kanıtları doğrudan ve bir seferde ortaya koymaktansa, belirsiz zamanlarda, az miktarda doğruyu sunmak ve muhatap kitlenin aklını karıştırmak, yanlış kararlara yöneltmek daha etkin sonuçlar doğurabilir.

Beşinci prensip olarak olası yan etkilerin tahmin ve kontrol edilmesinden söz edilebilir. Özellikle, hedefe ulaşmada engel teşkil edebilecek, tehlikeli ve istenmeyen yan etkiler daha büyük sorunlara yol açmadan kontrol altına alınmalıdır.

Geri besleme, algı yönetiminde altıncı prensiptir. Hedefe ulaşmak için birtakım ayarlamalar, düzeltmeler yapmak gerekebilir ve bu amaçla yürütülen faaliyetin ölçülmesi ve değerlendirilmesi elzemdir.

Yüz muharebeye girip yüzünde de galip gelmek marifet değildir. Hiç savaşmadan düşmana boyun eğdirmektir mükemmeliyetin zirvesidir.

Sun Tzu

KISALTMALAR

Kısaltmalar mevzuu pek eğlencelidir. Bu furyayı başlatan Amerikalılar genellikle bilinen şeyleri süslü kelimelerle tanımlar ve sonra bu kelimelerin baş harflerini kullanarak bir jargon yaratırlar. Mesela, harekât güvenliği söz konusu olduğunda korunması gereken kritik bilgi yerine Essential Elements of Friendly Information deyimini icat eder; sonra bu kadar uzun yazamadıkları için EEFI der geçerler. Veya bir özel harekât eğitim merkezini USAJFKSWCS diye tanımlarlar. Fransızlarsa bir başka alemdirler; istedikleri kelimeleri alır, istemediklerini almazlar, sadece baş harfleri değil, ortadan veya sondan harfler de kullanırlar. Mesela, MINUGUA (Mission de vérification des Nations unies pour les droits de l'homme au Guatemala). United karşılığı Birleşmiş mi Birleşik mi diyeceğimize veya Ortadoğu mu yoksa Orta Doğu mu yazacağımıza henüz karar veremediğimiz için bizde kural pek belli değildir.

AES	Advanced Encryption Standard	Gelişkin Şifreleme Standardı
AIC	Availability-Integrity-Confidentiality	Erişilebilirlik-Bütünlük-Gizlilik
AIS	Automated Information Sytems	Otomatik Bilgi Sistemleri
ARPANET	Advanced Research Projects Agency Network	İleri Savunma Araştırmaları Dairesi Ağı
C^2	Command and Control	Komuta ve Kontrol
C^2W	Command and Control Warfare	Komuta ve Kontrol Harbi
C^4I	Command, Control, Communications, Computers and Intelligence	Komuta, Kontrol, Haberleşme, Bilgisayar ve İstihbarat
CESG	Communications-Electronics Security Group	(İngiltere) Haberleşme-Elektronik Güvenlik Grubu
CI	Counterintelligence	İstihbarata Karşı Koyma (İKK)
CIA	Central Intelligence Agency	Merkezi Haberalma Teşkilatı
CIA	Confidentiality-Integrity-Availability	Gizlilik-Bütünlük-Erişilebilirlik
CA	Civil Affairs	Sivil İşler
CMO	Civil Military Operations	Sivil-Askeri Operasyonlar
CMOC	Civil Military Operations Center	Sivil-Askeri Operasyon Merkezi
CNA	Computer Network Attack	Bilgisayar Ağı Taarruz
CND	Computer Network Defense	Bilgisayar Ağı Savunma
CNE	Computer Network Exploitation	Bilgisayar Ağı İstismar
CNO	Computer Network Operations	Bilgisayar Ağı Operasyonları
CMO	Civil-Military Operations	Sivil-Askeri Operasyonlar

CO	Cyberspace Operations	Siber (Siberuzay) Operasyonlar
COMCAM	Combat Camera	Savaş Kamerası
COMINT	Communications Intelligence	Haberleşme İstihbaratı
COMSEC	Communications Security	Haberleşme Güvenliği
DARPA	Defense Advanced Research Proects Agency	Savunma İleri Araştırma Proeleri Ajansı
DECT	Digital European Cordless Telecommunications	Sayısal Avrupa Kablosuz Haberleşme
	Digital Enhanced Cordless Telecommunications	Sayısal Geliştirilmiş Kablosuz Telefon
DCS	Distributed Control System	Dağınık (Dağıtılmış) Kontrol Sistemi
DES	Digital Encryption Standard	Sayısal Şifreleme Standardı
DES3	Triple DES	üçlü DES
DIA	Defense Intelligence Agency	Savunma İstihbarat Ajansı
DII	Defense Information Infrastructure	Savunma (Bakanlığı) Bilgi Altyapısı
DISA	Defense Information Systems Agency	Savunma Bilgi Sistemleri Ajansı
DoD	Department of Defense	Savunma Bakanlığı (ABD)
DSPD	Defense Support to Public Diplomacy	Kamu Diplomasisine savunma Desteği
EA	Electronic Attack	Elektronik Taarruz
ECCM	Electronic Counter Counter Measures	Elektronik Karşı Karşı Tedbirler (EKKT)
ECM	Electronic Counter Measures	Elektronik Karşı Tedbirler (EKT)
EEFI	Essential Elements of Friendly Information	Dost Bilgisinin Esas Unsurları
ELINT	Electronic Intelligence	Elektronik İstihbarat
EMCON	Emissions Control	Yayın Denetimi
EMP	Electromagnetic Pulse	Elektromanyetik Darbe
EMS	Electromagnetic Spectrum	elektromanyetik spektrum, ... tayf
EP	Electronic Protection	Elektronik Savunma
ES	Electronic Warfare Support	Elektronik Harp Desteği
ESM	Electronic Support Measures	Elektronik Destek Tedbirleri (EDT)
EW	Electronic Warfare	Elektronik Harp (EH)
FAPSI	(FAGCI) Federal Agency for Government Communications and Information	(Rusya) devlet haberleşme ve bilgi merkezi
FBI	Federal Bureau of Investigation	Federal Soruşturma Bürosu
FISINT	Foreign Instrumentation Intelligence	Yabancı Enstrümantasyon İstihbaratı
FM	Field Manuel	Sahra Talimnamesi (ST)
FSB	Federal Security Service	(Rusya) Federal Güvenlik Servisi

FSO	Federal Protective Service	(Rusya) Federal Koruma Servisi
GC&CS	Government Code and Cipher School	(İngiltere) devlet kodlama ve şifreleme okulu
GCHQ	Government Communications Headquarters	(İngiltere) devlet haberleşme merkezi
GIE	Global Information Environment	Küresel Bilgi Ortamı
GIG	Global Information Grid	Küresel Bilgi Şebekesi
GII	Global Information Infrastructure	Küresel Bilgi Altyapısı
GPS	Global Positioning System	Küresel Konumlama Sistemi
GSM	Groupe Spécial Mobile	mobil haberleşme için özel çalışma grubu
	Global System for Mobile communications	mobil haberleşme için küresel sistem
HUMINT	Human Intelligence	İnsan İstihbaratı
IA	Information Assurance	Bilgi Teminatı
IAEA	International Atomic Energy Agency	Uluslararası Atom Enerjisi Ajansı
ICS	Industrial Control System	Endüstriyel Kontrol Sistemi
IMINT	Imagery Intelligence	Görüntü İstihbaratı
INEW	Integrated Network-Electronic Warfare	(Çin) Entegre Ağ-Elektronik Harp
INFOSYS	Information Systems	Bilgi Sistemleri
INTERNET	Internetwork	internet
IO	Information Operations	Bilgi Harekâtı, Bilgi Operasyonu
IOCA	Interception of Communication Act	(İngiltere) haberleşmenin izlenmesi yasası
IPB	Intelligence Preparation of the Battlespace	muhabere alanında istihbari hazırlık
IPIP	International Public Information Program	Uluslararası Kamuoyu Enformasyon Programı
IRC	Information-Related Capability	Bilgiyle Alakalı Beceri
IS	Information Superiority	Bilgi Üstünlüğü
ISO	International Organization for Standardization	Uluslararası Standartlar Organizasyonu
ISP	Internet Service Provider	İnternet Servis Sağlayıcı (ISS)
ISR	Intelligence, Surveillance and Reconnaissance	İstihbarat, Gözetleme ve Keşif
IW	Information Warfare	Bilgi Harbi
İHA	(Unmanned Air Vehicle - UAV)	İnsansız Hava Aracı
JC2WC	Joint Command and Control Warfare Center	Müşterek Komuta ve Kontrol Harp Merkezi
JEMSO	Joint Electromagnetic Spectrum Operations	Müşterek Elekromanyetik Spektrum Operasyonları
JFC	Joint Force Commander	Müşterek Kuvvetler Komutanı
JP	Joint Publication	Ortak Yayın (ABD Genelkurmayı)

KGB	Committee for State Security	(SSCB) Devlet Güvenlik Komitesi (SSCB) istihbarat teşkilatı
KLE	Key Leader Engagement	Önemli Lider Teması
LAN	Local Area Network	Yerel Alan Ağı
MASINT	Measurement and Signature Intelligence	ölçüm ve iz sinyalleri istihbaratı
MIE	Military Information Environment	Askeri Bilgi Ortamı
MILDEC	Military Deception	Askeri Aldatma
MISO	Military Information Support Operations	Askeri Bilgi Destek Operasyonları
MIT	Massachusetts Institute of Technology	Massachusetts Teknoloji Enstitüsü
MTR	Military Technical Revolution	(Rusya) Askeri Teknik Devrim
NETINT	Network Intelligence	Network (Bilgisayar Ağı) İstihbaratı
NGO	Non-Government Organization	Sivil Toplum Kuruluşu
NII	National Information Infrastructure	Ulusal Bilgi Altyapısı
NLP	Neuro-Liguistic Programming	duyusal ve dilsel programlama
NSA	National Security Agency	Ulusal Güvenlik Ajansı (ABD)
NSFNET	National Science Foundation Network	Ulusal Bilim Vakfı Ağı (ABD)
NSL	National Security Letter	Ulusal Güvenlik Mektubu
NSPD	National Security Presidential Directive	Ulusal Güvenlik Başkanlık Direktifi
OODA	Observe, Orient, Decide, Act	izle, yönlendir, karar ver, hareket et
OOTW	Operations Other Than War	Savaş Harici Operasyonlar
OPSEC	Operations Security	Harekât Güvenliği (Emniyeti)
OSI	Open Systems Interconnection	Açık Sistemler Bağlantısı
OSINT	Open Source Intelligence	Açık Kaynak istihbaratı
OTP	One Time Pad	tek kullanımlık defter
PA	Public Affairs	Halkla İlişkiler, Kamu İşleri, Amme İşleri
PDD	Presidential Decision Directive	Başkanlık Karar Direktifi
PGP	Pretty Good Privacy	epey münasip mahremiyet
PLA	People's Liberation Army	(Çin) Halkın Kurtuluş Ordusu
PLC	Programmable Logic Controller	programlanabilir kontrol cihazı
PSYOP	Psychological Operations	Psikolojik Harekât
PTT		(Türkiye) Posta Telgraf Telefon (1995 öncesi)
PTT ARLA		(Türkiye) PTT Araştırma Laboratuarı
PVO	Private Voluntary Organization	Özel Gönüllü Kuruluş

RF	Radio Frequency	Radyo Frekansı
RF	Russian Federation	Rusya Federasyonu
RII	Relevant Information and Intelligence	Alakalı Bilgi ve İstihbarat
RIPA	Regulation of Investigatory Powers Act	(İngiltere) araştırma erkini düzenleyen yasa
RIP Bill	Regulation of Investigatory Powers Bill	(İngiltere) araştırma erkini düzenleyen yasa tasarısı
RMA	Revolution in Military Affairs	Askeri Konularda Devrim
RNG	Random Number Generator	Rastgele Sayı Üreteci
ROA	Rules of Engagement	Angajman Kuralları
RSA	Rivest Shamir Adlemaan	asimetrik kripto algoritması
SC	Strategic Communication	Stratejik İletişim
SCADA	Supervisory Control And Data Acquisition	denetleyici kontrol ve veri toplama
SIGINT	Signal Intelligence	Sinyal İstihbaratı
SIGSEC	Signal Security	Sinyal Güvenliği
SIO	Special Information Operations	Özel Bilgi Harekâtı
SIS	Secret Intelligence Service (MI6)	Gizli İstihbarat Servisi
SOF	Special Operations Forces	Özel Harekât Kuvvetleri
SORM	System of Operation Research Measures	(Rusya) internet trafiğinden bilgi elde etmek....
SMSG	School Mathematics Study Group	okul matematik çalışma grubu
SSCB		Sovyet Sosyalist Cumhuriyetler Birliği
STO	Special Technical Operations	Özel Teknik Operasyonlar
SVR	Foreign Intelligence Service	(Rusya) Yabancı İstihbarat Servisi
TA	Target Audience	Hedef Kitle, muhatap
TECHINT	Technical Intelligence	Teknik İstihbarat
TELINT	Telemetry Intelligence	Telemetri İstihbaratı
TRANSEC	Transmission Security	İletişim Güvenliği
UAV	Unmanned Air Vehicle	İnsansız Hava Aracı - İHA
USB	Universal Serial Bus	evrensel seri veriyolu
USIA	United States Information Agency	Amerikan Haberler Merkezi
USSR	Union of Soviet Socialist Republics	Sovyet Sosyalist Cumhuriyetler Birliği (SSCB)
VOA	Voice of America	Amerika'nın Sesi radyosu
VoIP	Voice over IP	İnternet Protokolü üzerinden ses iletişimi

KAYNAKÇA

Bu derlemede yararlanılan tüm kaynakların belirtilmesine azami özen gösterdim; sadece alıntı yapılanlar değil, benim bilgi dağarcığımı oluşturan kaynaklara da yer verdim kaynakçada. Ancak, kaynak göstermede ve kaynakçanın düzenlenmesinde bilimsel bir yayın için zorunlu olan kurallara riayet etmem pratikte mümkün olmadı. Çoğu zaman tek bir paragrafı hatta cümleyi bile birçok kaynaktan derlemek durumunda kaldım. Birkaç kaynakta yer alan cümleleri birleştirerek, düzenleyerek, sadeleştirerek tek bir cümle halinde sundum okuyucuya. Bu durumda, ilgili kaynakları ayrı ayrı belirtmem yazımın sürekliliğini bozacak ve okuyan için rahatsızlık yaratacaktı. Kaynakçada belirtilen kaynakların bazılarının başlıkları ortak olduğundan yazar değil eser adına göre sıralamayı ve bu sayede konu bütünlüğü korunmayı tercih ettim. Alıntı yapmadığım kaynaklara da yer verdim, konuya ilgi duyanların faydalanması için. Amacım, genel okuyucunun ilgi seviyesini artırmak ve araştırma yapmak isteyenler için faydalı olabilecek kaynaklar sunmaktır. Ayrıca, çok miktarda internet tabanlı kaynak belirtilmekte, bunların arasında wikipedia özel yer tutmaktadır. Birçokları bunu gereksiz bulabilir; nihayetinde, konu ne olursa olsun her isteyen wikipedia'ya başvurabilir, benim işaret etmeme gerek duymadan. Ama wikipedia gibi onca emekle oluşturulmuş bir bilgi kaynağı, hele de yararlanmışsam, saygıyı muhakkak hak ediyor. Nihayetinde, bu derleme bir bilimsel yayın değil; esasen genel okuyucuyu hedeflemektedir; dolayısıyla, bilimsel yayınlar için geçerli olan kaynak gösterme kurallarından sapmayı tercih ettim.

(A) Basılı kitap, dergi veya yazma formatında dokümanlar:

(1) *109 East Palace, Robert Oppenheimer and the Secret City of Los Alamos*, Jennet Conant, Simon & Schuster, 2005

(2) *21. Yüzyılın Şafağında Savaş ve Savaş Karşıtı Mücadele*, Alvin Toffler ve Heidi Toffler, Sabah Kitapları, 1994

(3) *Applied Cryptography*, Bruce Schneier, John Wiley & Sons, 1996

(4) *In Athena's Camp, Preparing for Conflict in the Information Age*, Edited by John Arquilla, David Ronfeldt, RAND National Defense Research Institute, 1997

(5) *Body of Secrets, Anatomy of the Ultra-Secret National Security Agency*, James Bamford, Doubleday, 2001

(6) *Break the Code, Crptography for Beginners*, Bud Johnson, Dover Publications, 1997

(7) *The Code Book*, Simon Singh, Fourth Estate, 1999

(8) *The Codebreakers,* David Kahn, Scribner, 1996

(9) *Codebreakers, The Inside Story of Bletchley Park*, edited by Sir F.Harry Hinsley and Alan Stripp, Oxford University Press, 1993

(10) *Conquest in Cyberspace: National Security and Information Warfare*, Martin C. Libicki, Copyright The RAND Corporation, Cambridge University Press, 2007

(11) *Cry Spy, True Stories of 20th Century Spies and Spy Catchers*, edited by Burke Wilkinson, Bradbury Press, 1969

(12) *Cryptanalysis, A Study of Ciphers and Their Solution*, Helen Fouché Gaines, Dover Publications, 1989 (1956) (1939)

(13) (*De la Cryptographie, essai sur les méthodes de déchiffrement*, P. Valerio)

(14) *Cryptography in an Algebraic Alphabet*, Lester S.Hill, The American Mathematical Monthly, Vol. 36, No. 6 (Jun. - Jul. 1929), pp. 306-312

(15) *The Current Revolution in Military Affairs and its Impact on Asia-Pasific Security*, Wang Baocun, China Military Science, April 2000

(16) *Cyber Power, and National Security*, Edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, Center for Technology and National Security Policy, National Defense University Press, Potomac Books, Inc, Washington D.C., 2009

(17) *Elementary Cryptanalysis, A Mathematical Approach*, Abraham Sinkov, The Mathematical Association of America, New Mathematical Library, 1980 (1966)

(18) *On Information Warfare Stratagems*, Niun Li, Li Jiangzhou, Xu Dehui, Zhogguo Junshi Kexue, Beijing , January 2001, translated and download from Foreign Broadcast Information Service (FBIS)

(19) *Innovating and Developing Views on Information Operations*, Qingmin Dai, Zhogguo Junshi Kexue, Beijing , August 2000, translated and download from Foreign Broadcast Information Service (FBIS), November 2000

(20) *Inside Cyber Warfare*, Jeffrey Carr, O'Reilly Media, 2012

(21) *An Introduction to the Formal Theory of Information Warfare*, S.P. Rastorguyev, Moscow, 2003

(22) *Bir Matematikçinin Savunması*, G.H. Hardy, (çev. Nermin Arık), TÜBİTAK Popüler Bilim Kitapları, 1997

(23) *Mathematical Recreations and Essays*, W.W. Rouse Ball, (rev. by H.S.M. Coxeter), The MacMillan Co., New York, 1960, p. 396

(24) *A Preliminary Analysis of IW*, Wang Baocun, Zhogguo Junshi Kexue, Beijing , November 1997, translated and download from Foreign Broadcast Information Service (FBIS)

(25) *The Puzzle Palace, Inside the National Security Agency, America's Most Secret Intelligence Organization*, James Bamford, Penguin Books, 1983

(26) *Risale fi istihraç el muamma,* Ebu Yusuf Yakub ibn-i İshak el Kindi, Süleymaniye Kütüphanesi Ayasofya Koleksiyonu No. 4832 sayfa 211 - 217

(27) *Secrets and Lies, Digital Security in a Networked World*, Bruce Schneier, John Wiley & Sons, 2000

(B) İnternet ortamında .pdf formatında yayınlanmış dokümanlar:

(1) *America's Cyber Future, Security and Prosperity in the Information Age, Volume I, VolumeII*, Edited by Kristin M. Lord, Travis Sharp, CNAS, Center for a New American Security, June 2011

(2) *The Arabic Origins of Cryptology, Book One: al Kindi's Treatise on Cryptanalysis*, Dr Mohammed Mrayati et al. KFCRIS & KACST, 2002

(3) *China's Electronic Strategies*, Timothy L. Thomas, Foreign Military Studies Office, Fort Lavenworth, KS, 2001

(4) *Codes and Ciphers, Julius Caesar, The Enigma and the Internet*, Robert Churchhouse, Cambridge University Press, 2002

(5) *Compendium of Key Joint Doctrine Publications*, Deputy Directorate, Joint Staff, J-7, Joint and Coalition Warfighting, Joint Doctrine Support Division, January 2013

(6) *Comparing US, Russian, and Chinese Information Operations*, Timothy L. Thomas, Foreign Military Sudies, Office, Fort Leavenworth, 2004

(7) *Cyber OODA: Towards a Conceptual Cyberspace Framework*, Major Christian L. Basballe Sorensen, School of Advanced Air and Space Studies, Air University, Maxwell Air Force Base, Alabama, June 2010

(8) *The Cyber Security Management System, A Conceptual Mapping*, John H. Dexter, The SANS Institute, 2002

(9) *Cyberdeterrence and Cyberwar*, Martin C. Libicki, Project Air Force, RAND Corporation, 2009

(10) *Cyberspace Operations*, Air Force Doctrine Document 3-12, 15 July 2010, incorporating change 1, 30 November 2011

(11) *Deciphering Cyberpower, Strategic Purpose in Peace and War*, John B. Sheldon, Strategic Studies Quarterly, Summer 2011

(12) *Driving Technological Surprise: DARPA's Mission in a Changing World*, Defense Advanced Research Projects Agency, April 2013

(13) *Electronic Warfare and Radar Systems Engineering Handbook*, Naval Air Systems Command Avionics Department AIR-4.5, 1999

(14) *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, Roland Heickerö, FOI, Swedish Defence Research Agency, Division of Defence Analysis, Stockholm, 2010

(15) *Field Manual 100-6 Information Operations*, Headquarters, Department of the Army, August 1996

(16) *Field Manual 3-13 (100-6) Information Operations: Doctrine, Tactics, Techniques, and Procedures*, Headquarters, Department of the Army, November 2003

(17) *How to Use the 36 Chinese Stratagems to Win*, Kenrick E. Clevelandand Influence Marketing LLC, 1997

(18) *Information Age Anthology: The Information Age Military, Volume III*, Edited by David S. Alberts, Daniel S. Papp, CCRP, DpD C4ISR Cooperative Research Program, 2001

(19) *Information Operations: Warfare and the Hard Reality of Soft Power*, *A textbook produced in conjunction with the Joint Forces Staff College and the National Security Agency*, Leigh Armistead, Potomac Books, 2004

(20) *Information Operations Roadmap*, U.S. Department of Defense, 2003

(21) *Information Warfare, A Fundamental Paradigm of Infowar*, Dr Carlo Kopp, 2005

(22) *Information Warfare and Information Operations (IW/IO): A Bibliography*, Greta E. Marlatt, Dudley Knox Library, Naval Post Graduate School, 2008

(23) *Information Warfare, An Introduction*, Reto E. Haeni, The George Washington University Cyberspace Policy Institute, 1997

(24) *Information Warfare Principles and Operations*, Edward Waltz, Artech House, 1998

(25) *Introduction to Modern Cryptography*, Mihir Bellare, Phillip Rogaway, UCSD, UCDAVIS, 2005

(26) *Introduction to Modern Symmetric Key Ciphers*, BESU Bengal Engineering and Science University, ISS-12-05.pdf

(27) *Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms*, Joint Chiefs of Staff, April 2001 (as amended through 13 June 2007)

(28) *Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms*, Joint Chiefs of Staff, November 2010 (as amended through 15 April 2013)

(29) *Joint Pub 3-13 Joint Doctrine for Information Operations*, Joint Chiefs of Staff, October 1998

(30) *Joint Publication 3-13 Information Operations*, Joint Chiefs of Staff, February 2006

(31) *Joint Publication 3-13 Information Operations*, Joint Chiefs of Staff, November 2012

(32) *Joint Publication 3-13.1 Electronic Warfare*, Joint Chiefs of Staff, 2007

(33) *Joint Publication 3-13.4 (JP 3-58) Military Deception*, Joint Chiefs of Staff, 2006

(34) *Joint Publication 3-53 Doctrine for Joint Psychological Operations*, Joint Chiefs of Staff, 2003

(35) *Joint Publication 3-57.1 Joint Doctrine for Civil Affairs*, Joint Chiefs of Staff, 2003

(36) *Joint Publication 3-61 Public Affairs*, Joint Chiefs of Staff, 2005

(37) *New Comparative Study Between DES, 3DES and AES Within Nine Factors*, Hamdan O. Alanazi et al. Journal of Computing, Vol 2, No. 3 March 2010

(38) *New Directions in Cryptography*, Whitfield Diffie, Martin E. Hellman, IEEE Transactions on Information Theory, Vol. IT-22, No. 6 Nov 1976

(39) *New Directions in Cryptography: Twenty Some Years Later*, Shafi Goldwasser, MIT Laboratory for Computer Science, 1997

(40) *Perception Management: A Core IO Capability*, Khyber Zaman, Naval Postgraduate School, Monterey, California, 2007

(41) *Principles of Information Operations: A Recommended Addition to U.S. Army Doctrine*, LTC Gerald V. Burton, Jr, School of Advanced Military Studies United States Army Command and General Staff College, 2003

(42) *Protection of freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA)*, Published by the Home Office, 2012

(43) *Recommendation for Block Cipher Modes of Operation, Methods and Techniques*, Morris Dworkin, NIST Special Publication 800-38A, 2001

(44) *Secrecy, Authentication, and Public Key Systems Technical Report No. 1979-1*, Ralph Charles Merkle, Information Systems Laboratory, Stanford Electronics Laboratories, Department of Electrical Engineering, Stanford University, 1979

(45) *Security Engineering: A Guide to Building Dependable Distributed Systems*, Ross Anderson, Wiley, 2001

(46) *Security Engineering: A Guide to Building Dependable Distributed Systems*, Second Edition, Ross Anderson, Wiley, 2008

(47) *Strategic Impact of Cyber Warfare Rules for the United States*, Paul A. Matus, Center for Strategic Leadership U.S. Army War College, 2010

(48) *Strategic Plan*, Defense Advanced Research Projects Agency, 2009

(49) *Summary of Surveillance Powers Under RIPA*, Liberty, Protecting Civil Liberties Promoting Human Rights

(50) *Thumping the Hive: Russian Neocortical Warfare in Chechnya*, Scott E. McIntosh, Naval Post Graduate School, Monterey, CA, September 2004

(51) *Truth from These Podia, Summary of a Study of Strategic Influence, Perception Management, Strategic Information Warfare and Strategic Psychological Operations in Gulf II*, Sam Gardiner, Col. USAF (Ret.), October 2003

(52) *Understanding Information Age Warfare*, David S. Alberts et al., CCRP, 2001

(53) *United States Information and Educational Exchange Act of 1948, aka Smith-Mundt Act of 1948.*

(54) *Unveiling World War II's Greatest Spyr*, David Kahn, MHQ Military History Quarterly, Autumn 2007

(55) *What Is Information Warfare?* Center for Advanced and Technology, Martin C. Libicki, Institute for National Strategic Studies, National Defense University, August 1995

(C) İnternet ortamında yayınlanmış olan Wikipedia kaynakları:

(1) http://en.wikipedia.org/wiki/Arthur_Scherbius

(2) http://en.wikipedia.org/wiki/Bletchley_Park

(3) http://en.wikipedia.org/wiki/Block_cipher

(4) http://en.wikipedia.org/wiki/Bomba_(cryptography)

(5) http://en.wikipedia.org/wiki/Bombe

(6) http://en.wikipedia.org/wiki/Chinese_Information_Operations_and_Information_Warfare

(7) http://en.wikipedia.org/wiki/Colossus_computer

(8) http://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma

(9) http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

(10) http://en.wikipedia.org/wiki/Enigma_machine
(11) http://en.wikipedia.org/wiki/Enigma_rotor_details
(12) http://en.wikipedia.org/wiki/FAPSI
(13) http://en.wikipedia.org/wiki/Federal_Protective_Service_of_Russia
(14) http://en.wikipedia.org/wiki/Federal_Security_Service
(15) http://en.wikipedia.org/wiki/Foreign_Intelligence_Service_(Russia)
(16) http://en.wikipedia.org/wiki/G._H._Hardy
(17) http://en.wikipedia.org/wiki/George_Orwell
(18) http://en.wikipedia.org/wiki/Gilbert_Vernam
(19) http://en.wikipedia.org/wiki/Glavnoye_Razvedyvatel%27noye_Upravleniye
(20) http://en.wikipedia.org/wiki/Hans-Thilo_Schmidt
(21) http://en.wikipedia.org/wiki/Hedy_Lamarr
(22) http://en.wikipedia.org/wiki/Henryk_Zygalski
(23) http://en.wikipedia.org/wiki/James_H._Ellis
(24) http://en.wikipedia.org/wiki/Joseph_Mauborgne
(25) http://en.wikipedia.org/wiki/Jerzy_R%C3%B3%C5%BCycki
(26) http://en.wikipedia.org/wiki/KGB
(27) http://en.wikipedia.org/wiki/Lockheed_F-117_Nighthawk
(28) http://en.wikipedia.org/wiki/Lorenz_cipher
(29) http://en.wikipedia.org/wiki/Marian_Rejewski
(30) http://en.wikipedia.org/wiki/Max_Newman
(31) http://en.wikipedia.org/wiki/National_security_letter
(32) http://en.wikipedia.org/wiki/Neocortex
(33) http://en.wikipedia.org/wiki/One-time_pad
(34) http://en.wikipedia.org/wiki/Polish_Cipher_Bureau
(35) http://en.wikipedia.org/wiki/Rest_in_peace
(36) http://en.wikipedia.org/wiki/Revolution_in_Military_Affairs
(37) http://en.wikipedia.org/wiki/RSA_(algorithm)
(38) http://en.wikipedia.org/wiki/Rubber-hose_cryptanalysis
(39) http://en.wikipedia.org/wiki/School_Mathematics_Study_Group
(40) http://en.wikipedia.org/wiki/Scrambler
(41) http://en.wikipedia.org/wiki/Stanis%C5%82aw_Le%C5%9Bniewski
(42) http://en.wikipedia.org/wiki/Stefan_Mazurkiewicz
(43) http://en.wikipedia.org/wiki/Substitution-permutation_network
(44) http://en.wikipedia.org/wiki/Thirty-Six_Stratagems

(45) http://en.wikipedia.org/wiki/Tommy_Flowers

(46) http://en.wikipedia.org/wiki/W._T._Tutte

(47) http://en.wikipedia.org/wiki/Wac%C5%82aw_Sierpi%C5%84ski

(D) İnternet ortamında yayınlanmış diğer dokümanlar:

(1) http://crypto.stackexchange.com/questions/596/is-modern-encryption-needlessly-complicated?rq=1

(2) http://cryptome.org/ukpk-alt.htm

(3) http://cs.ucsb.edu/~koc/ac/notes/onetime.pdf

(4) http://ed-thelen.org/comp-hist/NSA-Comb.html

(5) http://fmso.leavenworth.army.mil/documents/dialect.htm

(6) http://home.comcast.net/~dhhamer/downloads/rotors1.pdf

(7) http://minttwist.org/2011/03/01/my-technology-hero-tommy-flowers-%E2%80%93-the-father-of-the-digital-age/

(8) http://mountainrunner.us/smith-mundt/#.UVgc3RDMjSh

(9) http://mountainrunner.us/smith-mundt/smith-mundt-u-s-code/#.UVgcGxDMjSh

(10) http://notthelittlethings.blogspot.com/2012/04/letter-frequencies-in-turkish.html

(11) http://notthelittlethings.blogspot.com/2012/05/change-in-letter-frequencies-in-turkish.html

(12) http://plus.maths.org/content/exploring-enigma

(13) http://primes.utm.edu/largest.html#intro

(14) http://privacyink.org/pdf/maa.pdf

(15) http://publicdiplomacycouncil.org/commentaries/05-31-12/when-do-we-start-honest-debate-over-modernization-act

(16) http://sergematovic.tripod.com/rsa1.html

(17) https://tao.truststc.org/courseware?domain=Network Security

(18) http://users.telenet.be/d.rijmenants/en/enigma.htm

(19) http://users.telenet.be/d.rijmenants/en/enigmatech.htm

(20) http://www.au.af.mil/au/awc/awcgate/crs/95-1170.htm

(21) http://www.au.af.mil/au/awc/awcgate/milreview/neocortical.pdf

(22) http://www.au.af.mil/au/awc/awcgate/milreview/thomas_china_iw.pdf

(23) http://www.bletchleypark.org.uk/edu/archives/machines.rhtm

(24) http://www.bletchleypark.org.uk/content/archive/index/august1939.rhtm

(25) http://www.bletchleypark.org.uk/content/hist/history/polish.rhtm
(26) http://www.bordc.org/nsl/nsl-history.pdf
(27) http://www.budiansky.com/ARTICLES_ARCHIVE_files/colossus.pdf
(28) http://www.cimt.plymouth.ac.uk/resources/codes/default.htm
(29) http://www.ciphersbyritter.com/
(30) http://www.ciphersbyritter.com/GLOSSARY.HTM
(31) http://www.ciphersbyritter.com/LEARNING.HTM
(32) http://www.cl.cam.ac.uk/~rja14/
(33) http://www.cl.cam.ac.uk/~rja14/Papers/
(34) http://www.codesandciphers.org.uk/enigma/index.htm
(35) http://www.codesandciphers.org.uk/lorenz/fish.htm
(36) http://www.colossus-computer.com
(37) http://www.controlglobal.com/articles/2013/boyes-beltway-cybersecurity.html
(38) http://www.cryptomuseum.com/crypto/enigma/working.htm
(39) http://www.cryptomuseum.com/crypto/enigma/d/index.htm
(40) http://www.cryptomuseum.com/crypto/enigma/g/index.htm
(41) http://www.cryptomuseum.com/crypto/enigma/m3/index.htm
(42) http://www.cryptomuseum.com/crypto/enigma/m4/index.htm
(43) http://www.cryptomuseum.com/crypto/bombe/index.htm
(44) http://www.cybersummits.com/eu/pdf/day1/Red-Dragon-part-2.pdf
(45) http://darpa.mil
(46) http://www.ellsbury.com/enigmabombe.htm
(47) http://www.exp-math.uni-essen.de/~vinck/crypto/script-crypto-pdf/add-to-2.pdf
(48) http://www.fas.org/irp/offdocs/nspd/
(49) http://www.fas.org/irp/offdocs/pdd/pdd-68.htm
(50) http://www.fipr.org/rip/
(51) https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa
(52) https://www.gov.uk/surveillance-and-counter-terrorism
(53) http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/
(54) http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/06_nspd_16.pdf
(55) http://www.hedylamarr.org/hedystory5.html
(56) http://www.history.navy.mil/faqs/faq61-2.htm
(57) http://www.history.navy.mil/library/online/infoops_cyberwar.htm
(58) http://www.ieeeghn.org/wiki/images/b/bb/Wesolkowski.pdf
(59) http://www.interhack.net/people/cmcurtin/snake-oil-faq.html

(60) http://www.iwar.org.uk/
(61) http://www.iwar.org.uk/rma/resources/nato/ar299stc-e.html
(62) http://www.khanacademy.org/math/applied-math/crypt/v/diffie-hellman-key-exchange
(63) http://www.legislation.gov.uk/ukpga/2000/23/contents
(64) http://www.liberty-human-rights.org.uk/materials/introduction-to-ripa-august-2010.pdf
(65) http://www.matematiksider.dk/enigma_eng.html
(66) http://www.math.ualberta.ca/~mss/misc/A%20Mathematician's%20Apology.pdf
(67) http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html
(68) http://www.ndu.edu/press/cyber-operations.html
(69) http://www.nku.edu/~christensen/1102cscmat483.htm
(70) http://www.nvi.gov.tr/Files/File/Sayisalimza/HuseyinEROL_BBG.pdf
(71) http://www.nsa.gov/about/_files/cryptologic_heritage/publications/misc/tiltman.pdf
(72) http://www.nytimes.com/2013/08/18/magazine/laura-poitras-snowden.html
(73) http://www.pgpi.org/doc/pgpintro/
(74) https://www.privacyinternational.org/blog/lawful-interception-the-russian-approach
(75) http://www.psywar.org/psywar/reproductions/PSYOP_ProvideComfort.pdf
(76) http://www.rutherfordjournal.org/article030108.html
(77) http://www.slideshare.net/cjgroeneveld/presd1-17
(78) http://www.state.gov/documents/organization/177574.pdf
(79) http://www.statewatch.org/news/jun00/rip1.htm
(80) http://www.statewatch.org/news/jun00/rip2.htm
(81) http://www.strategicstudiesinstitute.army.mil/pubs/summary.cfm?q=236
(82) http://www.systems-thinking.org/dikw/dikw.htm
(83) http://www.theguardian.com/world/2013/jun/16/g20-surveillance-turkey-targeted-gchq
(84) http://www.theguardian.com/world/2013/jun/17/turkey-russia-g20-spying-gchq?guni=Network%20front:network-front%20main-3%20Main%20trailblock:Network%20front%20-%20main%20trailblock:Position3
(85) http://www.tsk.tr/8_tarihten_kesitler/8_4_turk_tarihinde_onemli_gunler/sakarya_meydan_muharebesi/sakarya_meydan_muharebesi.htm
(86) http://www.washingtonpost.com/wp-dyn/content/article/2007/03/22/AR2007032201882.html
(87) http://www.washingtonpost.com/wp-srv/national/dotmil/arkin011899.htm
(88) http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure
(89) http://www.wired.com/dangerroom/2012/12/russias-hand/all/8