Sayı : 28

DÜŞÜNCE

DÜNYA'DAN BİR HABER

KILIÇTAN KODA

SIBER SAVAŞ

ÖZEL DOSYA

LEBANON PAGER EXPLOSİONS

İÇİNDEKİLER

YORUM

Savaş, insanlığın en eski pratiğidir. Kılıçlarla başlayan bu serüven, tüfeklerle, toplarla, tanklarla devam etti; nükleer çağda gökyüzünü karartan mantar bulutlarına kadar ulaştı. Ancak 21. yüzyıl, savaşın en görünmez ama en yıkıcı evresine tanıklık ediyor: siber savaş çağı. Artık topraklar değil, veriler; sınırlar değil, ağlar; kaleler değil, algoritmalar kuşatılıyor.

Bu sayıda, insanlığın kılıçtan koda uzanan yolculuğunu takip ediyor. Antik çağda Pisagor'un gizli bilgeliğinden Hasan Sabbah'ın fedailerine; Soğuk Savaş'ta Enigma makinesinden ECHELON sistemine; internetin doğuşunda Morris Worm'dan küresel krizi tetikleyen NotPetya'ya; ve nihayet yapay zekâ ile otonom saldırıların gündelik hayatı tehdit ettiği günümüze kadar tüm kırılma noktalarını ele alıyor. Bu yolculuk bize, savaşın yalnızca silahlarla değil, aynı zamanda bilgi, algı ve kod üzerinden yürütüldüğünü hatırlatıyor.

Bugün geldiğimiz noktada, siber savaş artık yalnızca devletlerarası bir hesaplaşma değildir. Kimi zaman bir lise öğrencisi (Mafiaboy), küresel ticaret devlerini dizüstü bilgisayarından çökertmiştir. Kimi zaman devletler (ABD–İsrail'in Stuxnet operasyonu), görünmez bir virüsle İran'ın nükleer santrallerini felce uğratmıştır. Kimi zaman da bir cihaz, masum bir çocuğun elinde patlayan bir pager gibi, savaşın ahlaki sınırlarını paramparça etmiştir.

Siber savaşın en tehlikeli boyutu, gerçeğin önemsizleşmesidir. Büyük veri çağında bilgi bolluğu, hakikati değil, algıyı kutsamaktadır. Deepfake teknolojileri, sahte haberler, bot orduları ile toplumlar artık neyin doğru olduğuna değil, neyin doğru olduğuna ikna edildiklerine inanmaktadır. Bu, insanlığın en büyük krizidir: bilgiye ulaşım çağında hakikatin kaybı.

Uluslararası güçler bu teknolojileri çoğu zaman fütursuzca, etik ve vicdani sınırları hiçe sayarak kullanmaktadır. Hukuk geriden gelmekte, uluslararası mekanizmalar ya yetersiz kalmakta ya da büyük devletlerin çıkarlarına teslim olmaktadır. Tallinn Manual gibi girişimler yalnızca tavsiye düzeyinde kalmış; Cenevre hukukunun "sivillerin korunması" ilkesi, patlayan cihazların, çöken altyapıların ve manipüle edilen toplumların gerçeği karşısında işlevsiz kalmıştır.

Burada sorulması gereken sorular ağırdır:

Yapay zekâ ve büyük veri, insanlığı özgürleştirecek mi, yoksa dijital bir kafese mi hapsedecek?

Uluslararası hukuk, siber saldırıları caydırabilecek mi, yoksa güçlü devletlerin cezasızlığına mı göz yumacak?

Gerçeğin değil algının hüküm sürdüğü bir dünyada, insan vicdanı nasıl bir direnç gösterecek?

Bu çalışma, yalnızca siber savaşların teknik tarihini değil, aynı zamanda insanlığın karşı karşıya olduğu etik, ahlaki ve vicdani sınavı tartışmaktadır. Çünkü mesele yalnızca ağların güvenliği değil; demokrasilerin, özgürlüklerin, bireysel hakların ve nihayetinde insan olmanın korunmasıdır.

Bugün geldiğimiz yol ayrımında iki ihtimal vardır:

Ya teknoloji, insan vicdanı ile birleşerek barışın temeli olacak; ya da kontrolsüz güçlerin elinde uygarlığı kendi dijital kıyametine sürükleyecektir.

Yavuz KAYA

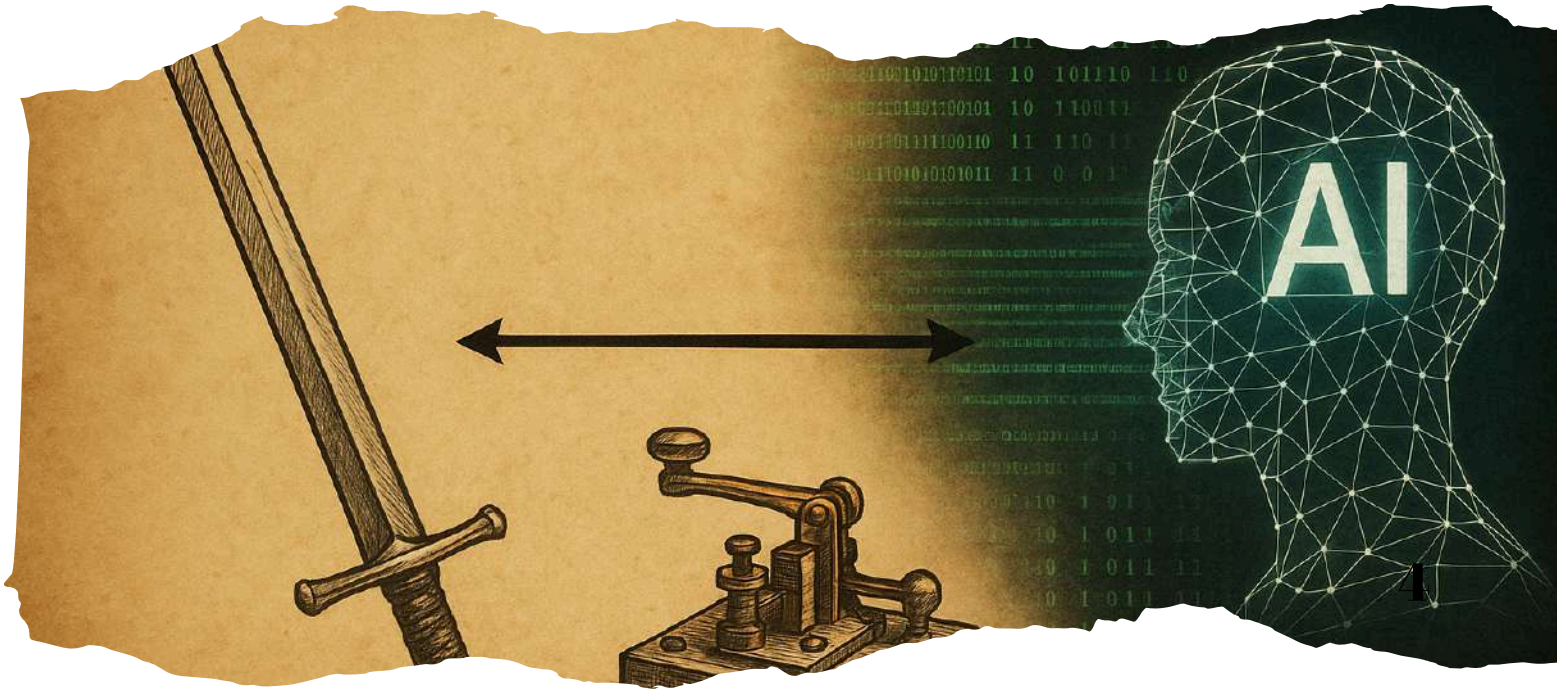
Tarihsel Süreçte Siber Savaşın Doğuşu

İnsanlık tarihi boyunca savaş kavramı, teknolojik gelişmelerin gölgesinde sürekli evrilmiştir. Kılıcın, barutun ve ateşli silahların yerini zamanla mekanik makineler, ardından uçaklar ve nükleer silahlar almıştır. Ancak 20. yüzyılın sonlarından itibaren savaşın doğası, fiziksel cephelerden görünmez ve sınır tanımaz dijital ortamlara taşınmaya başlamıştır. Bu yeni dönemin adı, literatürde "siber savaş" olarak anılmaktadır (Rid, 2013).

Siber savaş, yalnızca teknik bir olgu değil; aynı zamanda uluslararası güvenlik, hukuk ve strateji açısından köklü dönüşümlerin habercisidir. Zira artık devletler, güç gösterilerini sadece askeri birlikleriyle değil; bilgisayar ağları üzerinden yönlendirilen zararlı kodlarla, kritik altyapılara yönelik saldırılarla ve kamuoyunu manipüle eden dezenformasyon kampanyalarıyla da sergilemektedir (Clarke & Knake, 2010).
Bu süreçte tarihin sürekliliğini görmek mümkündür: Antik çağlarda casusluk ve gizli yazışmalar ne kadar stratejikse, günümüzde de şifreleme, veri koruma ve siber istihbarat o denli kritik hale gelmiştir. Nitekim "bilgiye sahip olanın güç sahibi olacağı" düşüncesi, günümüzde çok daha görünür bir hâl kazanmıştır. Çünkü artık savaş meydanları dijital ağlardır; tankların yerini kod satırları, kalelerin yerini güvenlik duvarları almıştır.

Siber savaşın doğuşu, yalnızca bir teknoloji meselesi olarak değil, aynı zamanda insanlık tarihinin en önemli kırılma noktalarından biri olarak değerlendirilmelidir. Bu kırılma, askeri stratejilerin ötesinde toplumsal yaşamı, ekonomik ilişkileri ve devletler arası hukuku yeniden tanımlamaktadır. Günümüzde kritik enerji altyapılarından seçim güvenliğine, bankacılık sistemlerinden sağlık ağlarına kadar geniş bir yelpazede dijital tehditler gündemin merkezindedir (Nye, 2017).

Takdim yazımız, bu dönüşümün tarihsel bağlamda anlaşılması gerektiğini vurgulamak için kaleme alınmıştır. Siber savaşın doğuşunu anlamak, yalnızca bilgisayar korsanlarının saldırılarını değil; binlerce yıllık bilgi mücadelesinin yeni bir evresini çözümlemek anlamına gelmektedir. Bu bağlamda, çalışmanın ilerleyen bölümleri savaşın evrimsel çizgisini kılıçtan koda, geleneksel cepheden sanal alana uzanan bir perspektifle ele alacaktır.



Savaşın Evrimi: Kılıçtan Koda

Savaş, insanlık tarihinin en eski pratiği olmakla birlikte, her dönemde teknolojik gelişmelerin ve zihinsel stratejilerin gölgesinde yeniden tanımlanmıştır. Başlangıçta savaş, bireysel güç, kılıç ustalığı ve taktiksel cesaret üzerinden yürütülürken; zamanla bilginin, gizliliğin ve psikolojik etkinin en az silahlar kadar belirleyici olduğu görülmüştür (Keegan, 1993).

Sessiz Bilginin Gücü: Pisagorcular

M.Ö. 6. yüzyılda ortaya çıkan Pisagorcular, yalnızca matematiğin değil, bilginin gizliliğinin de stratejik bir silah olduğunu göstermiştir. Bu topluluk, öğretilerini kapalı bir çevrede, "sessizlik yemini" ile muhafaza ederek bilginin gücünü korumayı amaçlamıştı. Onlara göre savaşta üstünlük yalnızca fiziksel kuvvetten değil, bilgiye erişim ve bu bilgiyi gizleme yetisinden doğuyordu (Burkert, 1972). Pisagorcuların bu tavrı, modern kriptoloji ve istihbarat disiplinlerinin entelektüel köklerini oluşturmuştur.

Psikolojik Harbin Öncüsü: Hasan Sabbah ve Alamut Fedaileri

11. yüzyılda Hasan Sabbah'ın önderliğinde Alamut Kalesi'nde örgütlenen Nizârî İsmailîler, savaş tarihine farklı bir boyut katmıştır. Sabbah'ın stratejisi, doğrudan cephe savaşından çok "asimetrik psikolojik üstünlük" üzerine kuruluydu. Fedailer, seçilmiş hedeflere yönelik suikastlarla büyük ordulara korku salmış; bu yöntem, düşman ordularını savaşmadan sindirme taktiği olarak tarihe geçmiştir (Daftary, 2007). Bu yönüyle Hasan Sabbah, günümüz "psikolojik harp" ve "asimetrik tehdit" doktrinlerinin erken bir örneğini temsil eder.

Sanayi ve Kod Çağına Geçiş

15. ve 16. yüzyıllarda ateşli silahların yaygınlaşmasıyla savaşın ölçeği büyümüş; top ve tüfek, ortaçağ savunma sistemlerini geçersiz kılmıştır (Black, 2011). 19. yüzyılda ise sanayi devrimi, demiryolları ve telgraf gibi yeniliklerle lojistiği ve iletişimi dönüştürmüş; bilgi güvenliği savaşın kaderini belirleyen bir unsur haline gelmiştir (Howard, 2002).

16. yüzyılda Enigma makineleri ve Alan Turing'in çözümlemeleri, kodun savaşın kaderini belirlediği ilk büyük kırılma noktasıdır (Copeland, 2006). Soğuk Savaş döneminde elektronik casusluk, uydu istihbaratı ve bilgisayar ağları üzerinden yürütülen çatışmalar, savaşın "görünmez bilgi savaşı" niteliğini daha da pekiştirmiştir.

Kılıçtan Koda: Bir Evrim

Bugün savaşın evrimi, iki eksende okunabilir: silah teknolojisinin dönüşümü (kılıç → tüfek → tank → nükleer → kod) ve bilginin stratejik araç haline gelişi (gizli bilgi → algı yönetimi → dijital kod). Kılıç, bireysel gücü ve yakın temas savaşını sembolize ederken; kod, küresel ölçekte görünmez, sınır tanımaz ve algoritmik bir savaş biçimini temsil etmektedir.
Bu perspektifle bakıldığında, Pisagorcuların sessiz bilgi kontrolünden Hasan Sabbah'ın psikolojik üstünlüğüne ve günümüz siber saldırılarına kadar uzanan çizgi, aslında savaşın özünde değişmeyen bir gerçeği gösterir: güç, bilgiyi kontrol edenin elindedir.

Tarihsel Kırılma Noktaları

M.Ö. 6. yüzyılda Güney İtalya'nın Kroton şehrinde, Pisagor'un etrafında toplanan gizli topluluk vardı. Onlar matematiği sadece bilim değil, sır ve güç kaynağı olarak gördüler.

Tarikata girenler "sessizlik yemini" ediyor, öğrendiklerini dışarı sızdırmıyordu. Sayılar kutsaldı; örneğin "10", evrenin bütünlüğünü temsil ediyordu. Bu gizlilik sayesinde bilgi, onları sıradan halktan ayıran bir silaha dönüştü.

Pisagorcular

- Dönem: M.Ö. 6. yy
- Yer: Kroton (Güney İtalya)
- Yöntem: Sessizlik yemini, gizli semboller
- Modern Bağlantı: Kriptografi & erişim sınırlaması

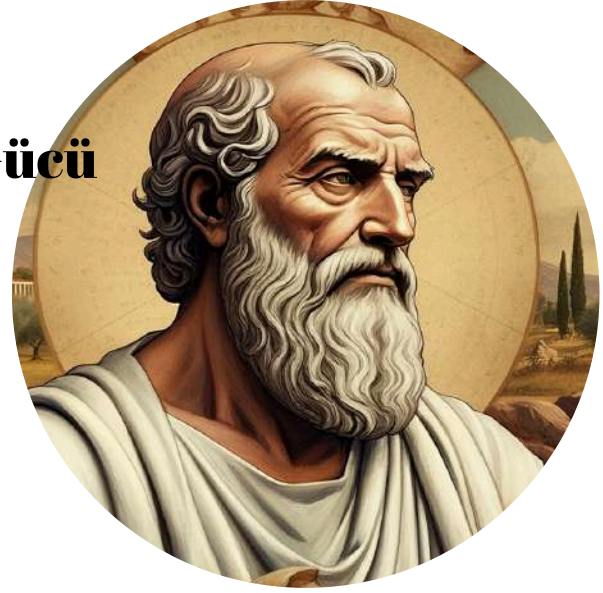
11. yüzyılda İran'ın sarp kayalıkları üzerinde yükselen Alamut Kalesi, tarihe korku ve hayranlıkla geçti. Hasan Sabbah'ın fedaileri, hedeflerinin yanına hizmetçi ya da dost kılığında sızar, yıllarca sessizce beklerdi.

Sonra bir gün, tek hamlede imparatorları, vezirleri devre dışı bırakırlardı. 1092'de Selçuklu Veziri Nizamülmülk'ün suikastı, bu stratejinin en çarpıcı örneğiydi.

Haşhaşiler

- Dönem: 11.–12. yy
- Yer: Alamut, İran
- Yöntem: Uzun vadeli istihbarat, uyuyan hücreler
- Modern Bağlantı: APT saldırıları (uzun vadeli siber casusluk)

Pisagorcular: Sessiz Bilginin Gücü



Tarihsel Arka Plan

M.Ö. 6. yüzyılda Güney İtalya'daki Kroton şehrinde Pisagor'un çevresinde toplanan topluluk, sadece matematik ve felsefe öğretisiyle değil, gizlilik ve örgütlü yapısıyla da dikkat çekti. Pisagorcular bir tür "bilgi tarikatı" gibiydi:

- Bilgi, herkese açık değildi.
- Öğretiler sıradan halka aktarılmıyor, sadece inisiyeler arasında paylaşılıyordu.
- Matematik ve astronomi, bir kozmik düzenin şifreleri olarak görülüyordu.

Yöntem ve Uygulamalar

- Kapalı Ağ Mantığı: Tarikata yeni katılanlar yıllarca "sessizlik yemini" etmek zorundaydı. Bu, bilginin dışarı sızmamasını sağlıyordu.
- Sembolik Kodlama: Pisagorcular, sayıları sembolik anlamlarla yükleyerek bir tür "kriptografi" sistemi kurdular. Örneğin "10 sayısı" kutsaldı ve evrenin bütünlüğünü temsil ediyordu.
- Bilgi–İktidar İlişkisi: Matematiksel bilgiyi yalnızca kendilerinde tutarak toplum üzerinde manevi ve politik etki kurdular.

Tarihsel Sonuçlar

- Kroton'da bir süre şehir yönetiminde etkin oldular; gizli yapıları nedeniyle düşman topluluklar tarafından baskılandılar.
- Bilginin "korunması gereken bir güç" olduğu anlayışı ilk kez sistematik hale geldi.
- "Bilgi kimin elindeyse, iktidar ondadır" anlayışı, felsefi düzeyde pratikleşti.

Siber Savaş Bağlantısı

- Modern siber güvenlikte "erişim sınırlaması" ve "kriptografi" ne ise, Pisagorcularda ritüel ve sembol gizliliği oydu.
- Onlar için bilgi, toplumdan saklandığında güç getiriyordu → Bugün de veriler, şifreleme ve erişim denetimiyle korunduğunda stratejik üstünlük sağlıyor.
- Pisagorcular'ın "sessizlik yemini" = günümüzde gizlilik protokolleri ve güvenlik izinleri.

Stratejik Çıkarım

Siber savaşın temeli, bilgiyi koruma sanatıdır. Pisagorcular, bilginin saklanması gerektiğini ilk kez kurumsallaştırarak bugünkü siber güvenlik mantığının kültürel atası oldular.

Hasan Sabbah ve Alamut Fedaileri

Tarihsel Arka Plan

yüzyılda Selçuklu İmparatorluğu'nun doğusunda, Alamut Kalesi Hasan Sabbah'ın yönetiminde bir merkez haline geldi. Nizârî-İsmailî topluluk, tarihte "**Haşhaşîler**" olarak bilindi.

Selçuklu veziri Nizamülmülk ve pek çok siyasi figür, onların suikastlarının hedefi oldu.

Örgüt yapısı, doğrudan askerî güce değil, gizlilik, istihbarat ve seçilmiş suikastlara dayanıyordu.

Yöntem ve Uygulamalar

Uzun Vadeli İstihbarat: Hedefler yıllarca gözlendi. Fedailer, onların evlerine hizmetçi veya yakın çevresine dost olarak sokuldu.

Uyuyan Hücreler: Bazen fedai, harekete geçmek için 5–10 yıl beklerdi.

Psikolojik Etki: Suikastlar genellikle kalabalık yerlerde yapıldı; amaç yalnızca öldürmek değil, korku yaymaktı.

Tarihsel Vakalar

1092 – Nizamülmülk Suikastı: Selçuklu veziri, Sabbah'ın fedaileri tarafından öldürüldü. Bu olay, Haşhaşîlerin adını tüm İslam coğrafyasına duyurdu.

1113 – Halep Emiri'nin Öldürülmesi: Fedailer sarayın içine kadar sızmıştı.

1176 – Sultan Selahaddin Eyyubi'ye Suikast Girişimi: Başarısız olsa da Sabbah'ın örgütünün gücünü gösterdi.

görülebilir.

Hasan Sabbah'ın örgütü, doğrudan ordularla değil, bilgi ve sabırla yürütülen operasyonlarla siyasal dengeleri değiştirdi. Bu, "klasik savaş"ın dışındaki yöntemlerle devletlerin diz çöktürülebileceğinin kanıtıydı.

Siber Savaş Bağlantısı

Günümüzdeki APT saldırıları (Advanced Persistent Threats) Sabbah'ın yöntemini birebir yansıtıyor:

Sisteme sız → içeride kal → doğru zamanı bekle → tek vuruşla etki yarat.

Tıpkı Sabbah'ın fedaileri gibi, zararlı yazılımlar da yıllarca sistem içinde uyur, iz bırakmadan veri toplar ve kritik anda harekete geçer.

"Psikolojik etki" de aynı: Suikastlar halkı korkuttu; modern siber saldırılar da güven duygusunu yıkar. (Örneğin, bankacılık sisteminin çökmesi → toplumsal panik).

Stratejik Çıkarım

Siber savaş yalnızca teknolojik değil, aynı zamanda sabır savaşıdır. En yıkıcı saldırılar, anlık hamlelerden değil, yıllar süren gizli hazırlıklardan doğar. Hasan Sabbah'ın stratejisi, modern siber operasyonların tarihsel öncüsü olarak

Tarihsel Bağlam ve Kriptolojinin Evrimi

Modern Şifreleme Çağına Giriş

Kriptoloji, insanlık tarihinin en eski güvenlik araçlarından biridir. İlk örneklerine Mısır hiyerogliflerinde, Mezopotamya tabletlerinde ve Roma İmparatorluğu dönemindeki Caesar Şifrelemesi gibi yöntemlerde rastlanır. Bu erken dönem teknikler, genellikle basit yer değiştirme (substitution) ve kaydırma (transposition) algoritmalarına dayanıyordu. Ancak bu yöntemler, sınırlı yazı sistemi ve iletişim teknolojisi sebebiyle nispeten güvenli sayılabiliyordu.

Orta Çağ boyunca diplomatik yazışmalar ve dini metinlerde şifreleme, daha çok "kriptoanaliz" bilimi ile yarışan bir zanaat hâline geldi. Al-Kindi'nin (801–873) "Kriptoanaliz Üzerine Risale"si, frekans analizi yöntemini geliştirerek kriptolojinin bilimsel temellerini atan en önemli eserlerden biri kabul edilir. Rönesans ve sonrasında Avrupa krallarının saraylarında, diplomasi ve istihbarat ağlarının gelişmesiyle şifreleme sistemleri daha da karmaşık bir hâl aldı.

Endüstri Devrimi ve Mekanik Şifreleme Araçlarının Ortaya Çıkışı

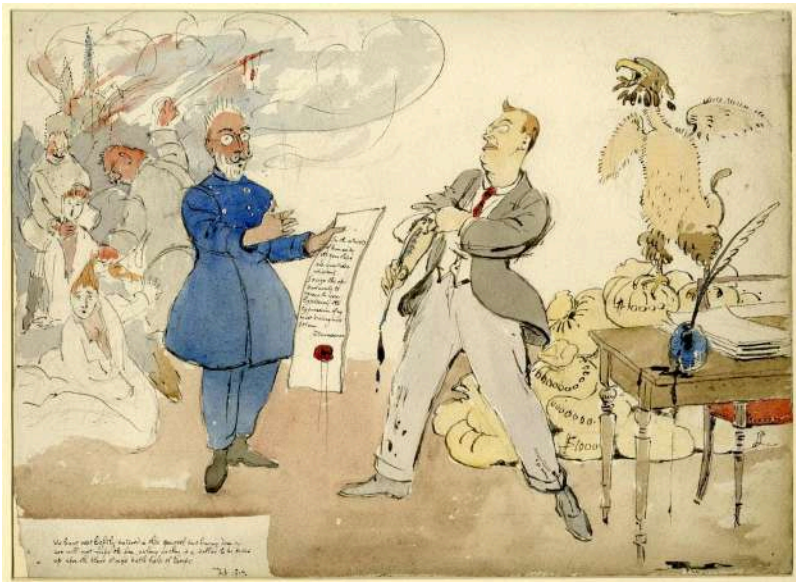
18. ve 19. yüzyıllarda telgrafın icadı, uzun mesafeli haberleşmeyi hızlandırırken aynı zamanda bilgi güvenliği ihtiyacını artırdı. Bu dönem, manuel şifreleme tekniklerinden mekanik şifreleme cihazlarına geçişin başlangıcı oldu. 19. yüzyılda geliştirilen Jefferson Disk ve Wheatstone'un Playfair Şifresi, daha sistematik ve çoklu alfabelere dayanan yöntemler ortaya koydu. Bu gelişmeler, modern kriptolojinin matematiksel temellere kaymasının habercisiydi.

Telgraf ağlarının uluslararası ticarette, diplomasi ve askeri harekâtta kullanılmaya başlanmasıyla, şifreli iletişim bir devlet politikası haline geldi. Bu, 20. yüzyılın başında şifreleme alanında ilk büyük kurumsallaşmanın önünü açtı.

Telgraf, Şifreler ve Enigma Makinesi
Alan Turing ve Kodların Çözülüşü

Bilgi Savaşının Yükselişi: 20. Yüzyıl ve Kod Çözücülerin Önemi

I. Dünya Savaşı, kriptolojiyi stratejik bir silaha dönüştürdü. Almanların kullandığı Zimmermann Telgrafı'nın 1917'de İngilizler tarafından çözülmesi, ABD'nin savaşa katılımında belirleyici rol oynadı. Bu olay, kriptolojinin artık yalnızca gizlilik değil, savaşların seyrini değiştirecek bir "bilgi silahı" olduğunun somut kanıtıydı.



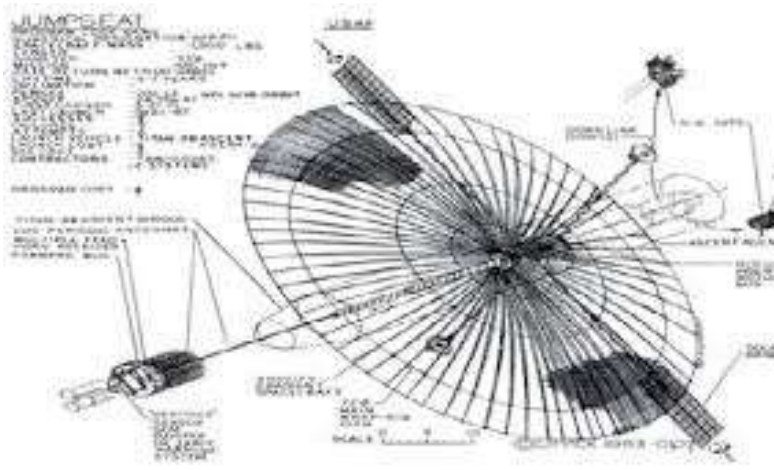
II. Dünya Savaşı döneminde Enigma Makinesi gibi elektro-mekanik şifreleme cihazları sahneye çıktı. Alman ordusunun Enigma ile kurduğu haberleşme ağı, İngiltere'deki Bletchley Park'ta Alan Turing liderliğindeki ekip tarafından kırıldı. Bu başarı, hem savaşın süresini kısalttı hem de bilgisayar biliminin doğuşunu tetikledi. Böylece kriptoloji, tarih boyunca ilk kez sistematik bir şekilde matematiksel algoritmalar ve makinelerle entegre edildi.

Soğuk Savaş ve Dijital Kriptolojinin Doğuşu

Soğuk Savaş yıllarında kriptoloji, elektronikleşerek küresel bir istihbarat yarışının merkezine oturdu. ABD Ulusal Güvenlik Ajansı (NSA) ve Sovyet istihbarat örgütü KGB, elektronik sinyal istihbaratı (SIGINT) ve uydu gözetleme sistemleriyle şifreleme teknolojilerinde hızlı bir ilerleme kaydetti. Bu dönemde:

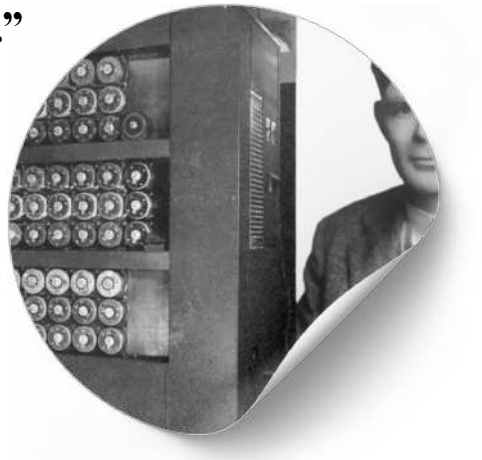
- Şifreleme, sadece askeri değil diplomatik, ekonomik ve bilimsel alanlarda da kritik rol oynadı.
- Kriptoanaliz ve şifreleme sistemleri, ulusal güvenliğin temel dayanaklarından biri haline geldi.
- Kod kırma süreçleri için elektronik bilgisayarlar geliştirildi ve şifreleme standartları (DES, RSA vb.) hayatımıza girdi.

Bu gelişmeler, günümüzdeki dijital güvenlik sistemlerinin temelini oluşturdu.



Telgraf, Şifreler ve Enigma Makinesi

“TANKLAR CEPHEDEYDİ, ZAFERİ İSE GÖRÜNMEZ KODLAR BELİRLEDİ.”

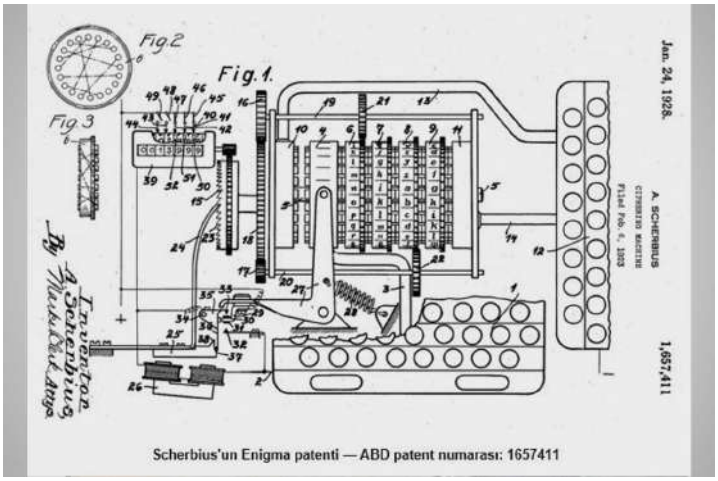


“2. DÜNYA SAVAŞI’NDA ENİGMA KODLARININ KIRILMASI, MODERN SİBER SAVAŞIN DOĞUM ANIDIR. O GÜN TANKLARIN DEĞİL, KODLARIN GÜCÜYLE ZAFER KAZANILDI.”

Dünya Savaşı’nın en gizli cephesi, cephe hatlarında değil, masa başında yaşandı. Alman ordusunun kullandığı Enigma şifreleme makinesi, her gün değişen milyonlarca kombinasyonla mesajları çözülemez kılıyordu. Nazi Almanyası, bu sistemle iletişimini güvende sanıyordu.

Fakat İngiltere’de Bletchley Park adı verilen gizli merkezde matematikçiler, dilbilimciler ve mühendisler gece gündüz çalışıyordu. Ekipte en önemli isimlerden biri, genç matematikçi Alan Turing’di. Turing’in geliştirdiği elektromekanik “Bombe” makinesi sayesinde Enigma’nın kodları çözüldü.

Bu başarı, Müttefiklerin savaşın gidişatını değiştirmesini sağladı: Atlantik’te konvoylar kurtarıldı, Normandiya Çıkarması’nın hazırlıkları gizlice yürütüldü. Enigma’nın çöküşü, tarihte “bilginin silah gücünden daha etkili” olduğunun en büyük kanıtıydı.



Scherbius’un Enigma patenti — ABD patent numarası: 1657411

Enigma

Dönem: 1939–1945

Yer: Bletchley Park, İngiltere

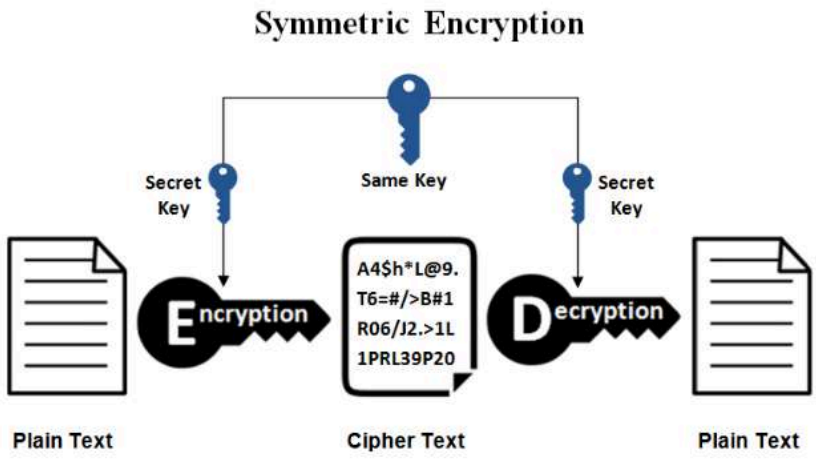
Yöntem: Kripto analiz, elektromekanik makine (Bombe)

Sonuç: Savaşın seyrini değiştiren gizli zafer

Modern Bağlantı: Siber savaşta şifre kırma ve kriptografi saldırıları

1941 Atlantik Savaşı: Enigma kodlarının çözülmesiyle Müttefik donanması, Alman U-botlarının konumunu öğrenerek deniz ticaretini kurtardı.

$$
\begin{aligned}
\mathfrak{f}(\mathfrak{C},\mathfrak{B},a) &\begin{cases} \mathfrak{d} & L \quad \mathfrak{f}_1(\mathfrak{C},\mathfrak{B},a) \\ \text{not } \mathfrak{d} & L \quad \mathfrak{f}(\mathfrak{C},\mathfrak{B},a) \end{cases} \\
\mathfrak{f}_1(\mathfrak{C},\mathfrak{B},a) &\begin{cases} a & \quad \mathfrak{C} \\ \text{not } a & R \quad \mathfrak{f}_1(\mathfrak{C},\mathfrak{B},a) \\ \text{None} & R \quad \mathfrak{f}_2(\mathfrak{C},\mathfrak{B},a) \end{cases} \\
\mathfrak{f}_2(\mathfrak{C},\mathfrak{B},a) &\begin{cases} a & \quad \mathfrak{C} \\ \text{not } a & R \quad \mathfrak{f}_1(\mathfrak{C},\mathfrak{B},a) \\ \text{None} & R \quad \mathfrak{B} \end{cases}
\end{aligned}
$$



Kriptolojiden Siber Güvenliğe: Yeni Çağın Habercisi

1. yüzyılın sonları, internetin doğuşuyla birlikte şifrelemenin askeri ve devletler arası bir araç olmaktan çıkıp bireylerin ve şirketlerin güvenlik ihtiyaçlarının temel unsuru haline geldiği bir dönemdir.

- Simetrik ve asimetrik şifreleme algoritmaları (AES, RSA, ECC) internet güvenliğinin temel taşlarını oluşturdu.
- Bankacılık, e-ticaret ve sosyal medya uygulamalarıyla kriptoloji gündelik hayatın parçasına dönüştü.
- Siber saldırılar, devlet destekli casusluk ve siber savaş kavramlarının doğmasına neden oldu.

Modern çağda kriptoloji yalnızca gizlilik değil, kimlik doğrulama, veri bütünlüğü ve erişim kontrolü gibi alanların da belkemiğidir. Artık kriptoloji; matematik, bilgisayar bilimi, yapay zekâ ve kuantum teknolojilerinin kesişiminde ilerleyen bir disiplin haline gelmiştir.

Akademik ve Jeopolitik Önemi

Bugün kriptoloji, uluslararası ilişkilerde caydırıcı bir güç, devletler ve şirketler için kritik bir güvenlik aracı, bireyler için ise mahremiyetin garantisidir. Kuantum bilgisayarların gelişimi, mevcut şifreleme standartlarını tehdit ederken post-kuantum kriptografi yeni bir araştırma alanı olarak öne çıkmaktadır.

Bu giriş bölümünde görüldüğü üzere, kriptoloji tarih boyunca bilgi ve güç arasındaki dengeyi belirleyen bir unsur olmuştur. Telgraf dönemindeki basit kodlardan günümüzün yapay zekâ destekli güvenlik protokollerine kadar geçen süreç, insanlığın bilgiye ve güvenliğe bakışındaki dönüşümü yansıtmaktadır.

Soğuk Savaş Yılları

“ARTIK SAVAŞ CEPHEDE DEĞİL, KLAVYELERİN GÖLGESİNDE YAŞANIYORDU.”

20. yüzyılın sonu, insanlık tarihinin en büyük dönüşümlerinden birini getirdi: internetin doğuşu. İlk olarak askeri bir proje olan ARPANET (1969), zamanla sivil hayata yayıldı. İnternet yaygınlaştıkça, bilginin serbest dolaşımı kadar, bilgiye saldırı imkânı da ortaya çıktı.

1980’lerde ilk bilgisayar solucanları görüldü. 1988’de Cornell Üniversitesi’nde öğrenci Robert Tappan Morris’in yazdığı “Morris Worm” virüsü, internete bağlı 60.000 bilgisayarın %10’unu çökertti. Bu, tarihin ilk küresel çaplı siber saldırısı olarak kayda geçti.

1990’larda hacker grupları ortaya çıktı. Web sitelerinin yüzleri değiştiriliyor, bankalara ve devlet sitelerine saldırılar yapılıyordu. Ama asıl kırılma 2000’lerde geldi:

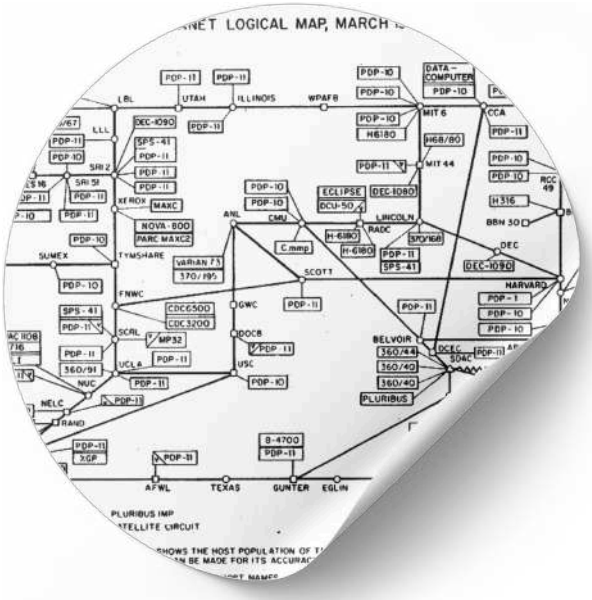
- 2007 Estonya: Sovyet anıtının kaldırılması üzerine Rusya kaynaklı siber saldırılar başladı. Devlet kurumları, bankalar ve medya kuruluşları günlerce çalışamaz hale geldi.
- 2010 Stuxnet: İran’ın Natanz’daki nükleer tesislerini hedef aldı. İlk kez bir bilgisayar virüsü, fiziksel makineleri sabote ederek “kodun silah”a dönüşebileceğini gösterdi.

Dijital Çağdaki İlk Saldırılar

1969: ARPANET (internetin doğuşu)
1988: Morris Worm (ilk internet solucanı)
2007: Estonya saldırıları (devlet ölçeğinde ilk kriz)
2010: Stuxnet (ilk dijital sabotaj silahı)
Modern Bağlantı: Siber savaş artık devletlerin güvenlik doktrininde ayrı bir cephe

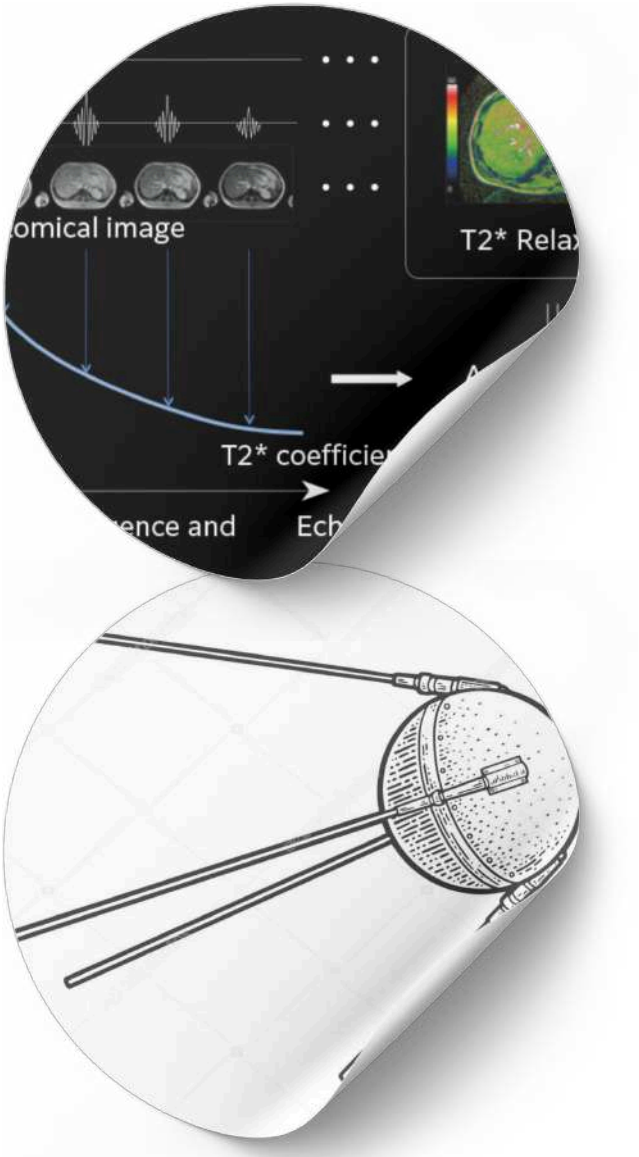
Öne Çıkan Vakalar

Morris Worm (1988): İnterneti ilk kez küresel ölçekte felç etti.
Estonya (2007): NATO’nun “siber saldırı kolektif savunma kapsamına girer mi?” sorusunu gündeme getirdi.
Stuxnet (2010): İran’ın nükleer programına yıllarca geri dönüşsüz zarar verdi.



Elektronik Casusluk ve ECHELON

1960 U-2 KRİZİ: ABD CASUS UÇAĞI SOVYETLER TARAFINDAN DÜŞÜRÜLDÜ. DÜNYAYA İSTİHBARAT SAVAŞININ NE KADAR GÖRÜNÜR OLABİLECEĞİNİ GÖSTERDİ.



"ATOM BOMBASI KORKU YARATTI, BİLGİYİ TOPLAYANLAR İSE SAVAŞI YÖNETTİ."

1947'de başlayan Soğuk Savaş, görünürde silahların patlamadığı ama sürekli bir "görünmez savaş"ın yaşandığı bir dönemdi. ABD ve Sovyetler Birliği, birbirlerini nükleer silahlarla tehdit ederken, aslında en büyük mücadele bilgi üstünlüğü üzerinden yürüyordu.

Amerikan CIA ve Sovyet KGB, dünyanın her yerinde casuslar yerleştirdi. Ancak asıl kırılma, teknolojide oldu:

Casus Uçaklar (U-2): Sovyet hava sahasında nükleer tesisleri fotoğrafladı.

Sputnik Uyduları (1957): Sovyetler ilk kez uzaya uydu yerleştirdi → ABD için büyük bir istihbarat şoku oldu.

ECHELON Programı: ABD, İngiltere, Avustralya ve müttefikleriyle küresel telefon ve telsiz ağlarını dinledi.

Soğuk Savaş boyunca bilgi toplama, nükleer başlık sayısından daha stratejik hale geldi. Kimin elinde daha çok veri varsa, karşı tarafı daha kolay yönlendirebiliyordu.

Soğuk Savaş İstihbaratı

Dönem: 1947–1991

Yöntem: Uydular, elektronik dinleme, casus uçaklar

Programlar: ECHELON, SIGINT (Signals Intelligence)

Sonuç: Nükleer savaş çıkmadı; bilgi savaşı dengeyi sağladı

Modern Bağlantı: Büyük veri toplama, küresel siber gözetim

"Soğuk Savaş'ta nükleer başlıklar değil, istihbarat üstünlüğü belirleyiciydi. Bugün de aynı mantık siber savaşta geçerli: Bilgi toplayan kazanıyor."

Elektronik Casusluğun Ortaya Çıkışı

Soğuk Savaş döneminde istihbarat faaliyetleri yalnızca ajanlar ve sahada çalışan operatörlerle sınırlı kalmadı; elektronik iletişim araçlarının yaygınlaşmasıyla birlikte istihbaratın odağı sinyal istihbaratı (SIGINT) ve iletişim istihbaratına (COMINT) kaydı.

- Radyo, telgraf ve telefon ağları devletler arası bilgi toplamanın ana hedefleri oldu.
- Özellikle uzun mesafeli kablolu ve uydu tabanlı iletişim sistemleri, elektronik casusluğun stratejik bir alan haline gelmesini sağladı.
- Kriptolojinin temel amacı yalnızca iletişimi korumak değil, rakip ülkelerin şifrelerini çözmek olarak da şekillendi.

Bu bağlamda elektronik casusluk, devletler için siber savaşın atası olarak kabul edilebilecek bir strateji geliştirme sahası haline geldi.

ECHELON Sisteminin Kurulması

1970'lerde ABD liderliğinde kurulan ECHELON, elektronik haberleşmeyi küresel ölçekte izlemek için geliştirilen en kapsamlı gözetleme ağıydı.

- Kurucu Ülkeler: ABD, Birleşik Krallık, Kanada, Avustralya ve Yeni Zelanda'dan oluşan Beş Göz (Five Eyes) ittifakı.
- Amaç: Soğuk Savaş boyunca Sovyetler Birliği ve müttefiklerinin diplomatik, askeri ve ticari iletişimlerini yakalamak ve çözümlemek.
- Teknik Altyapı:
  - Uydu istasyonları ve kablo dinleme merkezleri.
  - Denizaltı fiber optik kablolarına doğrudan erişim.
  - Radyo frekans tarama sistemleri.

Bu yapı, küresel iletişimin büyük bir kısmını süzgeçten geçirecek kapasiteye sahipti.

İşleyiş Mekanizması ve Kapasitesi

ECHELON, iletişimi otomatik olarak taramak ve anahtar kelimeler üzerinden veri toplamak için tasarlanmıştı.

- Anahtar Kelime Filtreleri: İlgili mesajlar belirlenen terimlere göre işaretleniyor ve analiz için saklanıyordu.
- Uydu ve Yer İstasyonları: Dünyanın farklı bölgelerindeki gözetleme merkezleri arasında koordinasyon sağlanıyordu.
- Merkezi Veri İşleme: ABD'deki Fort Meade, İngiltere'deki GCHQ ve diğer "Five Eyes" merkezleri gelen verileri depolayıp analiz ediyordu.

4. Eleştiriler ve Uluslararası Tartışmalar

1990'ların sonunda Avrupa Parlamentosu ECHELON Raporu, bu sistemin ticari rekabette ve ulusal egemenlikte ciddi tehditler oluşturduğunu ortaya koydu:

- Sistem, sadece askeri ve diplomatik iletişimi değil, özel şirketler ve bireylerin haberleşmelerini de izleyebiliyordu.
- Gizlilik ve bireysel özgürlükler konusunda uluslararası kamuoyunda büyük bir tepki doğdu.
- ECHELON, modern siber gözetleme sistemlerinin öncüsü olarak, Snowden belgelerinde ortaya çıkan PRISM ve XKeyscore gibi programların ilham kaynağı oldu.

5. Stratejik ve Teknolojik Miras

ECHELON, günümüzün siber güvenlik politikalarına ışık tutan bir sistem olarak değerlendirilebilir:

- Devletlerarası gözetleme faaliyetlerinde otomasyon ve büyük veri analizi kavramlarını ilk kez uyguladı.
- İstihbarat topluluğunda "Beş Göz" (Five Eyes) ittifakı, hâlâ en güçlü istihbarat paylaşım ağıdır.
- Siber casusluk tekniklerinin devlet destekli tehdit aktörleri tarafından benimsenmesinde ECHELON'un büyük etkisi oldu.

Uzay İstihbaratı ve Casus Uçaklar

Uzay İstihbaratı ve Casus Uçaklar

1. Soğuk Savaş ve Hava Üstünlüğünün İstihbarata Dönüşmesi

Soğuk Savaş, yalnızca nükleer caydırıcılık ve diplomatik gerginliklerle değil, aynı zamanda bilgi savaşlarıyla da şekillendi. 1940'ların sonlarından itibaren ABD ve SSCB arasındaki rekabet, gökyüzü ve uzayı istihbarat arenasına dönüştürdü.

- Amaç: Rakip ülkenin askeri kapasitesini, füze üslerini ve nükleer tesislerini önceden tespit etmek.
- Öncelik: Kara ajanlarının sınırlı erişimi nedeniyle havadan ve uzaydan gözetleme kritik bir avantaj sağladı.

2. Casus Uçakların Dönemi: U-2 ve SR-71 Blackbird

1950'ler, yüksek irtifa casus uçaklarının istihbarat alanında devrim yarattığı bir dönemdir.

a. U-2 Casus Uçağı (1956)

- Lockheed tarafından geliştirilen U-2, 21.000 metreye kadar yükselebiliyordu.
- Sovyet radarlarının erişim sınırlarının üzerinde uçtuğu için uzun süre fark edilmeden istihbarat topladı.
- 1960'ta Sovyetler Birliği'nin bir U-2'yi düşürmesi, ABD–SSCB ilişkilerinde büyük bir krize yol açtı. Bu olay, uzay tabanlı istihbarata geçişi hızlandırdı.

b. SR-71 Blackbird (1966)

- Saatte 3.500 km'yi aşan hızıyla dünyanın en hızlı keşif uçağı oldu.
- Yüksek hız ve irtifa sayesinde düşman radarlarından kaçabiliyor, kısa sürede çok geniş alanları fotoğraflayabiliyordu.
- SR-71, Soğuk Savaş boyunca ABD'nin en güçlü istihbarat platformlarından biri olarak hizmet verdi.

Uzay Tabanlı İstihbaratın Doğuşu: CORONA Projesi

Havadan istihbarat, 1957'de Sovyetler'in Sputnik uydusunu fırlatmasıyla stratejik önemini artırdı. ABD, daha güvenli ve kapsamlı gözetleme için CORONA adlı ilk keşif uydusu programını başlattı:

- İlk Fırlatma: 1959.
- Teknoloji: Fotoğraf filmleri kapsüllerle dünyaya geri indiriliyor ve analiz ediliyordu.
- Sonuç: Sovyetler'in askeri üsleri, nükleer tesisleri ve sanayi bölgeleri hakkında geniş çaplı veri toplandı.

CORONA, uzay istihbaratında bir milat sayılır ve modern uydu gözetleme ağlarının temelini atmıştır.

4. Sinyal ve Görüntü İstihbaratı (SIGINT ve IMINT)

Uzay ve hava platformları, iki ana istihbarat kategorisini güçlendirdi:

- SIGINT (Signals Intelligence): Düşman iletişimlerini ve radar sinyallerini yakalama.
- IMINT (Imagery Intelligence): Yüksek çözünürlüklü görüntüler ve haritalar elde etme.

Bu yetenekler, askeri stratejilerde oyunun kurallarını değiştirdi:

- Füze üslerinin tespit edilmesi, Küba Füze Krizi (1962) gibi olaylarda kritik rol oynadı.
- ABD ve SSCB arasındaki silah kontrol anlaşmalarında (SALT, START) uydu görüntüleri doğrulama aracı olarak kullanıldı.

5. Uzay Yarışının İstihbarata Katkıları

Uzay yarışı, teknolojiyi hızla ileriye taşıdı:

- KH-11 Uyduları: Dijital görüntü iletimi sağlayan ilk uydular, 1970'lerden itibaren anlık veri aktarma yeteneği kazandırdı.
- Radar Uyduları: Bulutlu hava ve gece koşullarında bile istihbarat toplayabilen sistemler geliştirildi.
- Elektronik Dinleme Uyduları: Telefon, radyo ve uydu iletişimlerini yakalayabilecek kapasiteye ulaşıldı.

Bu gelişmeler, Soğuk Savaş'ı yalnızca bir "silahlanma yarışı" değil, aynı zamanda "bilgi üstünlüğü yarışı" haline getirdi.

6. Jeopolitik ve Teknolojik Sonuçlar

- Casus uçaklar ve uzay istihbaratı, geleneksel istihbarat yöntemlerini büyük ölçüde dönüştürdü.
- Uydu gözetleme, küresel güç dengelerinde görünürlük ve denetim aracı olarak uluslararası ilişkilerde kritik rol oynadı.
- Bugün ABD, Rusya, Çin, İsrail ve Avrupa ülkeleri benzer uydular ve insansız hava araçlarıyla (İHA) bu mirası sürdürmektedir.

Dijital Çağın Doğuşu

İnternetin Ortaya Çıkışı ve Siber Güvenlik İhtiyacının Başlangıcı

Soğuk Savaş döneminde ABD Savunma Bakanlığı tarafından başlatılan ARPANET projesi (1969), internetin temellerini attı.

- Hedef: Nükleer saldırı durumunda bile çalışabilecek bir iletişim ağı geliştirmek.
- Teknoloji: Paket anahtarlama (packet switching) yöntemiyle verilerin parçalara ayrılarak gönderilmesi.
- Sonuç: ARPANET, üniversiteler ve araştırma kurumları arasında bilgi paylaşımını kolaylaştırdı, ancak ağ güvenliği o dönemde neredeyse hiç düşünülmedi.

1970'lerde TCP/IP protokolünün geliştirilmesiyle küresel bir ağ altyapısı oluştu. Bu, bilgisayarların coğrafi sınırlar olmaksızın birbirine bağlanmasını sağladı. Ancak güvenlik açıkları da aynı hızla arttı; ilk hacker toplulukları ve bilişim suçu vakaları bu dönemde ortaya çıktı.

İlk Bilgisayar Solucanları ve Zararlı Yazılımlar
1980'ler, bilgisayarların yaygınlaşmasıyla birlikte zararlı yazılımların ilk örneklerinin görüldüğü dönemdir:

- Creeper (1971): Dünyanın bilinen ilk bilgisayar virüsü, ARPANET üzerinde yayıldı. Mesajı: "I'm the creeper, catch me if you can!"
- Elk Cloner (1982): Apple II bilgisayarlarını hedefleyen ilk kişisel bilgisayar virüsüydü.
- Bu dönemde virüsler genellikle deneysel amaçlı yazılıyordu; ancak ticari ve siyasi amaçlı siber saldırılar henüz başlamamıştı.

Bu gelişmeler, antivirüs yazılımlarının ve güvenlik yazılımlarının doğmasına yol açtı.

Siber Saldırı Kavramının Ortaya Çıkışı
1990'larla birlikte internet, askeri ve akademik alanlardan çıkıp halka açıldı. Bu durum yeni bir tehdit kategorisini doğurdu: siber saldırılar.

- Tanım: Siber saldırı, bilgisayar ağlarını, cihazları veya altyapıyı yetkisiz erişim, veri hırsızlığı, sabotaj veya casusluk amacıyla hedefleyen her türlü dijital müdahaledir.
- Başlıca Türler:
  - DDoS (Dağıtık Hizmet Engelleme): Sunucuların çökertilmesi.
  - Phishing: Kullanıcıları kandırarak şifre ve bilgi toplama.
  - Ransomware: Fidye yazılımlarıyla dosya şifreleme ve fidye talebi.
  - Supply Chain Saldırıları: Tedarik zinciri yazılımlarının hedeflenmesi.
- Aktörler: Devlet destekli gruplar, hacktivistler, organize siber suç örgütleri ve bağımsız hackerlar.

Bu kavram, uluslararası ilişkilerde siber savaş söyleminin doğmasına zemin hazırladı.

4. Morris Worm (1988): İlk Büyük İnternet Krizi
İnternetin kırılganlığını dünyaya gösteren ilk büyük olay Morris Solucanı oldu:

- 1988'de Cornell Üniversitesi öğrencisi Robert Tappan Morris tarafından yazıldı.
- Amacı zararlı olmamakla birlikte kod hatası nedeniyle internetin %10'unu çökertti.
- Bu olay, CERT (Computer Emergency Response Team) gibi siber güvenlik birimlerinin kurulmasına yol açtı.
- Morris Worm, bilgisayar güvenliğinin artık bir ulusal güvenlik meselesi haline geldiğini gösterdi.

Devlet Ölçeğinde İlk Siber Kriz: Estonya (2007)

2007'de Estonya, devlet ölçeğinde ilk büyük siber saldırıya maruz kaldı:

- Bankacılık sistemi, hükümet siteleri ve medya kuruluşları eş zamanlı DDoS saldırılarıyla felç oldu.
- Bu saldırıların Rusya bağlantılı gruplar tarafından düzenlendiği iddia edildi.
- Estonya bu olaydan sonra NATO bünyesinde Siber Savunma Mükemmeliyet Merkezi (CCDCOE)'nin kurulmasına öncülük etti.

6. Stuxnet (2010): Kodun Silaha Dönüşmesi

Stuxnet, siber saldırıların fiziksel dünyada etkili bir silah haline gelebileceğini gösteren ilk örnek oldu:

- ABD ve İsrail tarafından geliştirildiği düşünülen bu zararlı yazılım, İran'ın Natanz nükleer tesislerindeki santrifüjleri hedef aldı.
- Stuxnet, endüstriyel kontrol sistemlerine sızarak fiziksel hasara yol açtı ve siber saldırıların artık stratejik silah olarak kullanılabileceğini kanıtladı.
- Bu olay, siber savaşın askeri doktrinlere resmi olarak dahil edilmesine yol açtı.

Siber Güvenliğin Yeni Paradigması

Dijital çağın ilk yıllarında yaşanan bu olaylar, siber güvenlik alanında bir paradigma değişimi yarattı:

- Ağ güvenliği, kritik altyapı koruması ve siber istihbarat devletlerin öncelikli gündem maddesi haline geldi.
- Özel sektör, özellikle bankacılık ve enerji sektörleri, siber tehditlere karşı yüksek bütçeler ayırmaya başladı.
- Siber uzay, kara, hava, deniz ve uzayla birlikte beşinci savaş alanı olarak kabul edildi.

Tarihsel Sürecin Çizdiği Çerçeve

Kriptoloji ve siber güvenlik tarihine bakıldığında, insanlık iletişimde hız kazandıkça güvenlik ihtiyacının da aynı ölçüde arttığı görülmektedir. Antik dönemden başlayan şifreleme teknikleri, telgrafın icadıyla birlikte ilk kez uluslararası diplomasi ve savaş stratejilerinin temel bir unsuru haline gelmiştir. I. Dünya Savaşı'ndaki Zimmermann Telgrafı olayı ve II. Dünya Savaşı'nda Enigma Makinesi'nin kırılması, kriptolojiyi yalnızca matematiksel bir uğraş olmaktan çıkarıp küresel güç dengelerinin belirleyicisi haline getirmiştir.

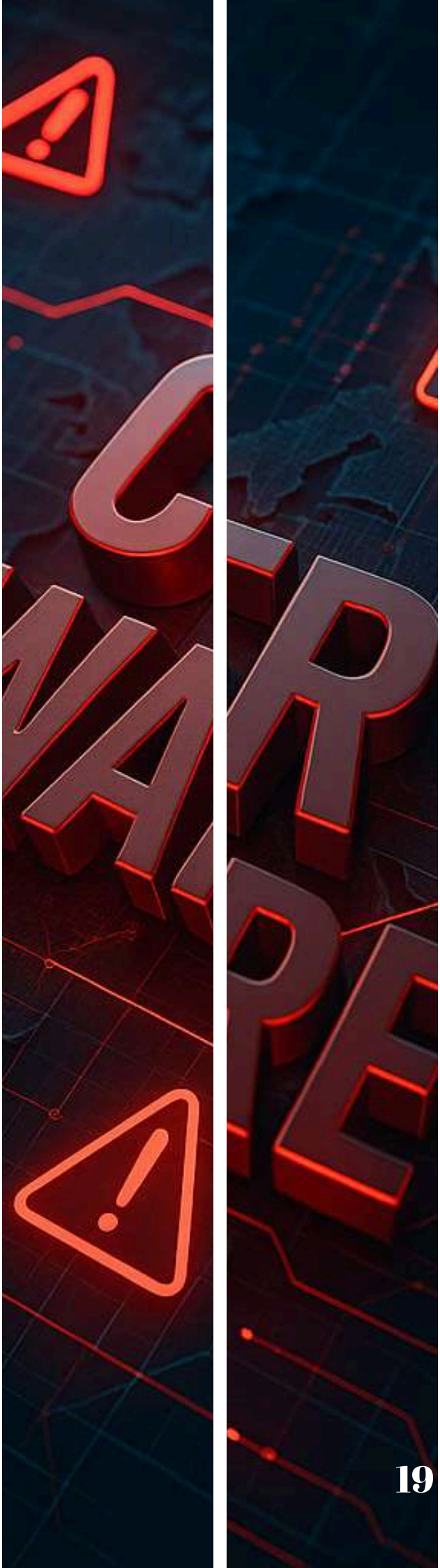
Bu noktadan sonra bilgi, bir güvenlik unsuru olmanın ötesine geçerek stratejik bir silaha dönüşmüştür. Soğuk Savaş, elektronik istihbarat ve uzay tabanlı gözetleme teknolojilerinin hızla gelişmesine yol açarken; bu teknolojiler, uluslararası ilişkilerde şeffaflığı artırmış, ancak aynı zamanda küresel casusluk faaliyetlerini de kurumsallaştırmıştır.

Dijital Çağın Tehdit Ekosistemi

1990'larda internetin yaygınlaşması, iletişim özgürlüğünü artırmakla birlikte siber saldırıların yükselişine zemin hazırlamıştır. Morris Worm (1988), Estonya Krizi (2007) ve Stuxnet (2010) gibi olaylar;

- Siber saldırıların sadece bilgisayar ağlarını değil, kritik altyapıları ve devlet politikalarını etkileyebilecek güçte olduğunu,
- Kod ve algoritmaların artık fiziksel yıkım üretebilecek birer silaha dönüştüğünü göstermiştir.

Bu süreç, "siber uzay" kavramının kara, hava, deniz ve uzay ile birlikte beşinci savaş alanı olarak kabul edilmesine yol açmıştır. Bugün devletler, siber güvenliği bir iç politika konusu olmaktan çıkarıp ulusal güvenliğin merkezine koymuştur.



Güç ve Güvenliğin Yeniden Tanımlanması

Modern çağda kriptoloji ve siber güvenlik, askeri üstünlüğün temel bileşenlerinden biridir.

- Devletlerarası Denge: ECHELON ve benzeri sistemler, uluslararası ilişkilerde casusluk ve gözetlemenin kurumsallaştığını ortaya koymuştur.
- Ekonomik Rekabet: Şirketler arası ticari sırların korunması, ulusal güvenlik stratejilerinin bir parçası haline gelmiştir.
- Bireysel Güvenlik: İnternet çağında bireylerin mahremiyeti, siber gözetleme ve veri madenciliği karşısında sürekli tehdit altındadır.

Kriptolojinin geldiği nokta, yalnızca devletleri değil, bireyleri de kapsayan bir güvenlik kültürü inşa edilmesini zorunlu kılmıştır.

Teknolojinin Çifte Kullanım Sorunu

Şifreleme teknolojileri ve siber güvenlik araçları, bir yandan kullanıcıların mahremiyetini korumak için geliştirilirken, diğer yandan devlet destekli siber saldırılar ve gözetleme sistemleri için kullanılmaktadır.

- Çifte Kullanım (Dual-Use) Teknolojisi: Aynı algoritmalar hem güvenlik hem saldırı aracı olarak işlev görebilmektedir.
- Stuxnet Sonrası Dönem: Siber saldırıların fiziksel dünyaya zarar verebildiği gösterilmiş, bu da siber güvenliği yalnızca teknik değil jeopolitik bir mesele haline getirmiştir.

Geleceğe Dair Stratejik Öngörüler

Kriptoloji ve siber güvenlik alanındaki gelişmeler, gelecekte daha karmaşık bir güvenlik ekosistemi ortaya çıkaracaktır:

- Kuantum Bilgisayarlar: Geleneksel şifreleme algoritmalarını kırabilecek kapasitededir; bu nedenle post-kuantum kriptografi geliştirilmek zorundadır.
- Yapay Zekâ: Siber saldırıların otomasyonunu artıracak, savunma mekanizmalarını daha hızlı hale getirecektir.
- Siber Diplomasi: Uluslararası hukukta siber saldırıların tanımı ve cezalandırılması için yeni anlaşmalar gerekmektedir.
- Kritik Altyapı Güvenliği: Enerji, sağlık ve ulaşım sistemleri siber saldırıların ana hedefi olmaya devam edecektir.

Bu tarihsel süreç, şifreleme ve siber güvenliğin insanlık tarihinde yalnızca bir teknik uzmanlık alanı değil, güç ilişkilerini şekillendiren stratejik bir disiplin olduğunu ortaya koymaktadır.

- Antik çağlardaki basit şifrelerden bugünkü yapay zekâ destekli güvenlik sistemlerine uzanan çizgi, bilginin bir güç kaynağı olarak nasıl kurumsallaştığını göstermektedir.
- Siber güvenlik, artık yalnızca bilgi teknolojileri departmanlarının değil, devlet başkanlarının ve uluslararası kuruluşların öncelikli gündem maddesi olmuştur.
- Gelecek, güvenlik ile mahremiyet arasındaki dengeyi sağlamak için teknolojik gelişmelerin etik ve hukuki boyutunun daha da öne çıkacağını göstermektedir.

Sonuç olarak, modern çağda güç tanımı; askeri kapasite, ekonomik güç ve diplomatik nüfuzun yanında siber savunma kapasitesi ve kriptografik yetenekleri de içerecek şekilde yeniden şekillenmiştir. Bu gerçek, bilgi çağında “bilgiyi korumak” ve “bilgiye erişmek” arasındaki mücadelenin 21. yüzyılın en önemli jeopolitik çatışma alanı olduğunu açıkça ortaya koymaktadır.

SİBER SALDIRI NEDİR? (TANIM, TÜRLER, AKTÖRLER)

“BİR SATIR KOD, BİR ORDU KADAR YIKICI OLABİLİR.”

Siber saldırı, modern çağın en görünmez ama en yıkıcı savaş biçimlerinden biridir. Klasik savaşlarda düşmanı yenmek için toprak işgal edilir, ordular harekete geçer, şehirler bombalanırdı. Siber çağda ise cephe değişti: savaş artık bilgisayarların, ağların ve yazılımların içinde yaşanıyor. Bir ülkenin ordusunu sahada yenmek zor olabilir ama aynı ülkenin banka sistemini, enerji ağlarını ya da haberleşme altyapısını çökertmek, birkaç satır kodla mümkündür.

Siber saldırıların en çarpıcı özelliklerinden biri, failin belirsizliğidir. Bir tankı gönderen ordunun kim olduğu bellidir ama bir siber saldırıyı yapan kişi, grup ya da devlet çoğu zaman gizli kalır. Bu yüzden siber saldırılar sadece teknik değil, aynı zamanda siyasi ve psikolojik bir araçtır. Hedef ülke kimi suçlayacağını bilemez, bu da caydırıcılığı azaltır.

Siber saldırılar farklı biçimlerde ortaya çıkar. Bazıları doğrudan hizmetleri kesintiye uğratmayı amaçlar. Örneğin, bir web sitesine milyonlarca sahte giriş isteği gönderilerek sistem çökertilir; buna “hizmet dışı bırakma” saldırısı denir. Bazıları ise daha sinsidir; zararlı yazılımlar gizlice sisteme girer, kullanıcı şifrelerini çalar, yıllarca fark edilmeden veri toplar. Bu tür saldırılar genellikle devlet destekli gruplar tarafından yapılır ve “gelişmiş kalıcı tehdit” olarak adlandırılır.

Bir diğer saldırı türü “fidye yazılımları”dır. Bu yöntemle saldırganlar bir bilgisayarın verilerini şifreleyip erişilemez hale getirir, ardından çözmek için para ister. 2017’de tüm dünyayı sarsan WannaCry saldırısı, hastanelerden fabrikalara kadar yüz binlerce kurumu felç etti. Benzer şekilde, kimlik avı saldırıları sahte e-postalar veya internet siteleri aracılığıyla insanların şifrelerini ve kişisel bilgilerini çalmak için kullanılır.

Siber saldırıların etkileri sadece ekonomik değildir. Bunlar aynı zamanda bir ülkenin güvenlik algısını da hedef alır. Bir bankanın çökmesi, elektrik şebekesinin devre dışı kalması ya da seçim sistemlerinin manipüle edilmesi, halkın devlete olan güvenini zedeler. Bu yüzden siber saldırılar sadece “teknik olaylar” değil, aynı zamanda birer psikolojik harp aracıdır.

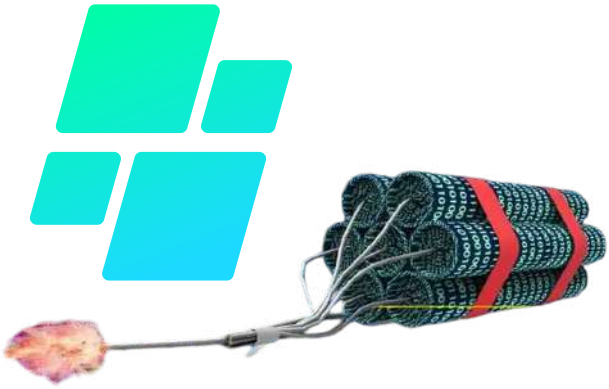
Tarihsel olarak bakıldığında, siber saldırıların ilk örnekleri basit ve amatör girişimlerdi. 1988’de ortaya çıkan Morris Worm adlı bilgisayar solucanı, internete bağlı cihazların önemli bir bölümünü devre dışı bırakmıştı. Ancak zamanla saldırılar devlet destekli hale geldi, profesyonel orduların yerini “siber ordular” almaya başladı. 2007’de Estonya’ya yapılan saldırılar, bir ülkenin tamamını günlerce işlevsiz hale getirdi. 2010’daki Stuxnet saldırısı ise yeni bir çağın başlangıcıydı: ilk kez bir yazılım, sanayi makinelerini bozarak fiziksel yıkıma yol açtı.

Bugün geldiğimiz noktada siber saldırılar, orduların savaş planlarının ayrılmaz bir parçasıdır. Rusya’nın Ukrayna’ya yönelik askeri saldırılarıyla eş zamanlı olarak yürüttüğü siber operasyonlar, bu gerçeğin son örneklerinden biridir.

Sonuç olarak, siber saldırı artık basit bir “bilgisayar korsanlığı” değildir. O, devletlerin, örgütlerin ve bireylerin kullandığı stratejik bir silahtır. Bir ülkenin ordusunu sahada yenmek zor olabilir ama aynı ülkenin hastanelerini, fabrikalarını ya da bankalarını çökertmek, görünmez cephede çok daha kolaydır.

Casusluk

Diğer ülkeleri sırları çalmak için izlemeyi ifade eder. Siber savaşta, bu, hassas bilgileri sızdırmadan önce hassas bilgisayar sistemlerini tehlikeye atmak için botnet'ler veya mızraklı kimlik avı saldırıları kullanmayı içerebilir .



Sabotaj

Hükümet kuruluşları hassas bilgileri ve bunların tehlikeye atılması durumunda ortaya çıkabilecek riskleri belirlemelidir. Düşman hükümetler veya teröristler bilgileri çalabilir, yok edebilir veya memnuniyetsiz veya dikkatsiz çalışanlar veya saldıran ülkeyle bağlantısı olan hükümet çalışanları gibi içeriden gelen tehditleri kullanabilir.

Hizmet Reddi (DoS) Saldırıları

DoS saldırıları, sahte isteklerle doldurarak ve web sitesinin bu istekleri işlemesini zorlayarak meşru kullanıcıların bir web sitesine erişmesini engeller. Bu tür saldırılar, kritik operasyonları ve sistemleri bozmak ve sivillerin, askeri ve güvenlik personelinin veya araştırma kuruluşlarının hassas web sitelerine erişimini engellemek için kullanılabilir.

Elektrik Güç Şebekesi

Elektrik şebekesine saldırmak, saldırganların kritik sistemleri devre dışı bırakmasına, altyapıyı bozmasına ve potansiyel olarak bedensel zarara yol açmasına olanak tanır. Elektrik şebekesine yapılan saldırılar ayrıca iletişimleri bozabilir ve kısa mesajlar ve iletişimler gibi hizmetleri kullanılamaz hale getirebilir.

Propaganda Saldırıları

Hedef ülkede yaşayan veya hedef ülke için savaşan insanların zihinlerini ve düşüncelerini kontrol etme girişimleri. Propaganda utanç verici gerçekleri ortaya çıkarmak, insanların ülkelerine olan güvenini kaybetmelerini sağlamak için yalanlar yaymak veya düşmanlarının tarafını tutmak için kullanılabilir.

Ekonomik Bozulma

Çoğu modern ekonomik sistem bilgisayarlar kullanılarak çalışır. Saldırganlar, borsalar, ödeme sistemleri ve bankalar gibi ekonomik kuruluşların bilgisayar ağlarını hedef alarak para çalabilir veya insanların ihtiyaç duydukları fonlara erişmesini engelleyebilir.

Sürpriz Saldırılar

Bunlar Pearl Harbor ve 11 Eylül gibi saldırıların siber eşdeğerleridir. Amaç, düşmanın beklemediği büyük bir saldırı gerçekleştirmek ve saldırganın savunmasını zayıflatmasını sağlamaktır. Bu, hibrit savaş bağlamında fiziksel bir saldırı için zemin hazırlamak amacıyla yapılabilir.


WannaCry
Ransomware Attack


MIRAI


NUCLEAR
VIRUS
WINDOWS
MICROSOFT
WORM
IRAN
STUXNE


DarkHotel


MAFIABOY


NotPetya


BANGLADESH BANK


MT.GOX

SİBER SAVAŞ OPERASYONLARI

Sansasyonel Siber Saldırılar

Dijital çağın ilerlemesiyle birlikte siber saldırılar, artık yalnızca teknik sorunlar olmaktan çıkmış; küresel ekonomiyi, devletlerin güvenliğini ve toplumsal düzeni sarsan krizlere dönüşmüştür. Özellikle 2000'li yılların başından itibaren gerçekleşen bazı saldırılar, literatürde "siber Pearl Harbor" benzetmeleriyle anılmıştır (Clarke & Knake, 2010). Bu bölümde, en sansasyonel siber saldırılar incelenmektedir.

1. Mafiaboy ve İlk Küresel DDoS (2000)

Kanadalı lise öğrencisi Michael Calce (Mafiaboy), 2000 yılında Yahoo, CNN, Amazon ve eBay gibi devasa sitelere DDoS saldırıları düzenledi. Bu saldırılar, internet tarihindeki ilk büyük ölçekli "hizmet dışı bırakma" vakası olarak kayıtlara geçti ve devletleri, genç bireylerin bile küresel sistemi felce uğratabileceği gerçeğiyle yüzleştirdi (Poulsen, 2001).

2. Mt. Gox Bitcoin Çöküşü (2014)

Kripto para piyasasının en büyük borsalarından biri olan Mt. Gox, 2014 yılında yaklaşık 850.000 Bitcoin'in çalınmasıyla çöktü. Bu olay, yalnızca bireysel yatırımcıları değil, kripto ekonomisinin güvenilirliğini de derinden sarstı. Siber saldırılar artık yalnızca devlet sistemlerini değil, alternatif finans ekosistemlerini de hedef almaya başlamıştı (Bradbury, 2013).

3. Bangladesh Bank Hack (2016)

2016'da Bangladeş Merkez Bankası'nın SWIFT sistemine sızan saldırganlar, yaklaşık 81 milyon doları sahte transferlerle Filipinler'deki hesaplara aktardı. Bu olay, finansal sistemlerin ne denli kırılgan olduğunu gösterdi. Eğer yazım hatasıyla tespit edilmese, 1 milyar dolara yakın bir kayıp yaşanacaktı (Greenberg, 2016).

4. Mirai Botnet (2016)

2016'da ortaya çıkan Mirai Botnet, güvenlik zafiyetleri bulunan IoT cihazlarını ele geçirerek tarihin en büyük DDoS saldırılarından birini gerçekleştirdi. Twitter, Netflix ve Reddit gibi siteler saatlerce erişilemez hale geldi. Bu saldırı, "nesnelerin interneti"nin gelecekteki güvenlik risklerine dair çarpıcı bir uyarı oldu (Antonakakis et al., 2017).

5. WannaCry (2017)

2017'de yayılan WannaCry fidye yazılımı, 150 ülkede yüz binlerce bilgisayarı etkiledi. İngiltere Ulusal Sağlık Sistemi (NHS) dahil olmak üzere birçok kritik kurum hizmet dışı kaldı. Microsoft'un yamalanmamış sistemlerindeki güvenlik açığını kullanan saldırı, fidye yazılımlarının küresel ölçekte devlet güvenliği için bir tehdit olduğunu kanıtladı (Europol, 2017).

6. NotPetya (2017)

WannaCry'den yalnızca aylar sonra ortaya çıkan NotPetya, tarihin en yıkıcı siber saldırısı olarak kabul edilmektedir. Ukrayna'yı hedef almış gibi görünmesine rağmen küresel şirketleri vurdu; Maersk, Merck ve FedEx gibi devlerin toplam kaybı 10 milyar doları buldu. NotPetya, siber saldırıların "yan etkilerinin" küresel çapta ekonomik şok dalgaları yaratabileceğini gösterdi (Greenberg, 2018).

7. Dark Hotel Casusluğu (2007–2017)

"Dark Hotel" olarak bilinen gelişmiş kalıcı tehdit (APT), özellikle lüks otellerin Wi-Fi ağları üzerinden üst düzey iş insanlarını ve diplomatları hedef aldı. On yıl boyunca fark edilmeden süren bu operasyon, siber casusluğun devletlerarası ilişkilerde ve iş dünyasında ne denli tehlikeli olabileceğini gösterdi (Kaspersky Lab, 2014).

Bu saldırıların ortak özelliği, her birinin yeni bir “çağı” başlatmasıdır:

- Mafiaboy: İnternetin kırılganlığı, bireylerin bile küresel tehdit yaratabilmesi.
- Mt. Gox: Kripto finansın güven sorunları.
- Bangladesh Bank: Küresel bankacılık sistemlerinin bile sızmaya açık olması.
- Mirai: IoT cihazlarının güvenlik zaafları.
- WannaCry & NotPetya: Devlet destekli saldırıların küresel yıkım potansiyeli.
- Dark Hotel: Siber casusluğun on yıllarca gizli kalabilmesi.

STUXNET

Stuxnet, İran nükleer programına saldıran bir solucandı. Tarihteki en sofistike siber saldırılardan biridir. Kötü amaçlı yazılım, enfekte olmuş Evrensel Seri Veri Yolu aygıtları aracılığıyla yayıldı ve veri toplama ve denetim kontrol sistemlerini hedef aldı. Çoğu rapora göre, saldırı İran'ın nükleer silah üretme yeteneğine ciddi şekilde zarar verdi.

İran'ın nükleer programını hedef alan Stuxnet saldırısı uzun yıllardır gizemini koruyordu. Bunca yıl karanlıkta kalan soru ise şu idi: ABD ve İsrail, zararlı yazılımlarını yüksek güvenlikli uranyum zenginleştirme tesisindeki bilgisayar sistemlerine yerleştirmeyi nasıl başardı?
Bu gizem geçtiğimiz günlerde Yahoo News'de Kim Zetter imzasıyla yayınlanan haberle çözülmüş oldu. Habere göre Hollanda istihbaratı için çalışan İranlı bir köstebek, ABD ve İsrail'in Stuxnet virüsünü İran'ın Natantz'daki nükleer tesisindeki santrifüjlere bulaştırılmasını sağladı. Santrifüj, uranyum zenginleştirmede kritik öneme sahip bir laboratuvar cihazı.

Türünün ilk örneği olan ve İran'ın nükleer programını sabote etmek için tasarlanan virüs, İran'ın Natanz köyü yakınlarındaki tartışmalı uranyum zenginleştirme tesislerinde ilk parti santrifüjünü kurmaya başlamasının ardından dijital savaş çağını etkili bir şekilde başlatmış oldu.

Kilidi Hollanda istihbarat servisi çözdü
Varlığı ve nasıl bir rol üstlendiği konusu bu zamana kadar hiç açıklanmayan gizli kurye, aslen İranlı bir mühendis. 4 istihbarat görevlisinin verdiği bilgiye göre, Hollanda istihbarat ajansı AIVD tarafından görevlendirilen mühendis, ABD'li geliştiricilere kodlarını Natanz'daki sistemlere hedeflemelerine yardımcı olacak kritik bilgileri temin ediyordu. Sıra bu sistemlere Stuxnet'i yerleştirmeye gelince, köstebek en çok ihtiyaç duyulan şeyi yani erişimi, USB flash sürücüsü kullanmak suretiyle sağladı.
2004 yılında CIA ve Mossad'ın tesise erişmelerine yardımcı olması için Hollandalılardan destek istenmişti. Ancak bu, Natanz'daki bir paravan şirkette teknisyen olarak çalışan köstebeğin 2007'de hedefteki sistemlere dijital silahı yerleştirdiği zamana kadar mümkün olmadı.
CIA ve Mossad Yahoo News'in sorularını cevaplamazken AIVD de operasyona dahil olduğu yönündeki iddialara yorum yapmaktan kaçındı.
Şimdilerde 'Olimpiyat Oyunları' (Olympic Games) adı ile açığa çıkan gizli operasyon, İran'ın nükleer programını yok etmek için değil yaptırımlar ve diplomasinin yürürlüğe girmesi adına zaman kazanmak amacıyla tasarlanmıştı. Bu strateji İran'ı müzakere masasına getirmeyi başardı ve nihayetinde 2015 yılında bu ülke ile uzlaşmaya varıldı.

STUXNET

Bilgisayar korsanlığı tarihinde önemli bir dönüm noktasını temsil eden, özellikle endüstriyel kontrol sistemlerini hedef alan sofistike bir kötü amaçlı yazılımdır. Bu yazılım, 2010 yılında keşfedilmiş ve bir dizi endüstriyel tesisin otomasyon sistemlerine zarar vererek gerçek dünyada ciddi etkiler yaratmıştır. İlk olarak İran'daki nükleer tesislerde tespit edilen Stuxnet, geniş çaplı bir siber saldırı olarak değerlendirilmektedir.

Stuxnet'in özellikleri, normal bir bilgisayar solucanından çok daha karmaşık ve hedef odaklıdır. Bu yazılım, özellikle Siemens tarafından kullanılan endüstriyel kontrol sistemleri üzerindeki zayıflıkları hedef alarak, hedef tesislerde ciddi zararlar meydana getirmeyi amaçlamıştır. Stuxnet'in bu sistemlere bulaşmasıyla birlikte, santrifüj kontrol sistemlerini manipüle ederek nükleer tesislerdeki uranyum zenginleştirme süreçlerini bozmaya yönelik bir saldırı gerçekleşmiştir.

Stuxnet'in Siber Silahlanma Yarışı Üzerindeki Etkisi

Saldırgan siber silah programlarına olan ilgi ve gelişme, Stuxnet'in piyasaya sürülmesinden kesinlikle öncesine dayanır. Haziran 2010'daki keşfinden önce bile, ABD istihbarat yetkilileri saygın saldırgan siber yeteneklere sahip yaklaşık yirmi ila otuz ordu olduğunu tahmin etmişti.

Elbette, ülkelerin siber cephaneliklerini oluşturmaya başladıkları kesin dönemi belirlemek büyük bir zorluktur, çünkü eski ABD başkanlık siber güvenlik danışmanı Richard Clarke'ın sözleriyle, "siber savaş olgusunun tamamı, Soğuk Savaş'ı açıklık ve şeffaflık zamanı gibi gösteren o kadar hükümet gizliliğiyle örtülüdür".

2007/2008 yıllarında Estonya ve Gürcistan'a yapılan dağıtılmış hizmet engelleme (DDOS) saldırıları gibi olaylar, bu ülkelerin iş, finans ve medya çevrimiçi iletişimlerinin ciddi şekilde engellenmesine neden oldu, siber uzayın stratejik faydasını gösterdi ve bu nedenle ortaya çıkan siber silahlanma yarışını yoğunlaştırmış olabilir. Ancak Stuxnet, yaygın olarak bir "oyun değiştirici" olarak kabul edilir.

Önceki siber saldırılarda kullanılan kötü amaçlı yazılımların aksine, oldukça hedefliydi ve gerçek dünyada bir sonuca ulaşmak için tasarlanmıştı.Endüstriyel Kontrol Sistemi (ICS) güvenlik analisti Ralph Langner'ın belirttiği gibi, hizmet engelleme saldırıları veya endüstriyel casusluk için tasarlanmaktan ziyade, "Stuxnet'in amacı, bir askeri hedefi sadece mecazi olarak değil, gerçek anlamda fiziksel olarak yok etmekti".

Bu son derece gelişmiş solucan, Natanz'daki hava boşluğunu aşabildi ve hantal IR-1 santrifüjlerinin kademe kademe aşırı hıza geçip kendini imha etmesini sağladı.

ABD yetkilileri, bu eylemin Tahran'ın sözde nükleer silah projesini on sekiz aydan iki yıla kadar geriye götüreceğini iddia ediyor.

Stuxnet benzeri bir siber silah üretmenin devlet politikasının uygulanması için cazibesi o zaman çok büyüktür. Bu solucanın serbest bırakılmasının dünya çapında siber silahların geliştirilmesi ve yayılması üzerinde muhtemel etkisi göz ardı edilmemelidir. Stuxnet'in gelecekteki varyantları, kullanıcılarına yüksek derecede anonimlik sağladığı için gizli operasyonlar için mükemmel bir şekilde uygun olmakla kalmaz, (bu, devletlerin misilleme veya uluslararası kınama korkusuna kapılmamaları anlamına gelir) aynı zamanda geleneksel silahlarla karşılaştırıldığında düşük maliyetlidir 15 ve muazzam asimetrik özelliklere sahip olma olasılıkları yüksektir. Ancak bu gelecekteki versiyonların mülkiyeti, bol kaynaklara sahip ulus devletlerle sınırlı olmayabilir. Aşağıdaki bölümün göstereceği gibi, Stuxnet'in çok çeşitli aktörlere ilham vererek ve onları güçlendirerek siber tehdidin doğasını değiştirmiş olması muhtemeldir.

Stuxnet'in Mirası

Stuxnet'in yapımcılarının Haziran 2012'de sona ermesi için programladığı ve Siemens'in PLC yazılımı için düzeltmeler yayınladığı bildirilse de, Stuxnet'in mirası orijinal koda dayalı diğer kötü amaçlı yazılım saldırılarında yaşamaya devam ediyor. Bu "Stuxnet oğulları" şunları içerir:

- Duqu (2011) . Stuxnet koduna dayanan Duqu, muhtemelen daha sonra bir saldırı başlatmak için endüstriyel tesislerden tuş vuruşlarını kaydetmek ve veri madenciliği yapmak üzere tasarlanmıştır.
- Flame (2012) . Stuxnet gibi Flame de USB bellek aracılığıyla seyahat ediyordu. Flame, Skype görüşmelerini kaydeden, tuş vuruşlarını kaydeden ve ekran görüntüleri toplayan, diğer aktivitelerin yanı sıra karmaşık bir casus yazılımdı. Çoğunlukla İran ve diğer Orta Doğu ülkelerinde hükümet ve eğitim kuruluşlarını ve bazı özel kişileri hedef alıyordu.
- Havex (2013) . Havex'in amacı enerji, havacılık, savunma ve ilaç şirketlerinin yanı sıra diğer şirketlerden bilgi toplamaktı. Havex kötü amaçlı yazılımı esas olarak ABD, Avrupa ve Kanada kuruluşlarını hedef aldı.
- Industroyer (2016) . Bu, güç tesislerini hedef aldı. Aralık 2016'da Ukrayna'da bir elektrik kesintisine neden olduğu kabul ediliyor.
- Triton (2017) . Bu, Orta Doğu'daki bir petrokimya tesisinin güvenlik sistemlerini hedef aldı ve kötü amaçlı yazılım üreticisinin işçilere fiziksel yaralanmaya neden olma niyeti konusunda endişelere yol açtı.
- En son (2018) . Stuxnet özelliklerine sahip isimsiz bir virüsün Ekim 2018'de İran'da belirtilmeyen bir ağ altyapısını etkilediği bildirildi.

Sıradan bilgisayar kullanıcılarının Stuxnet tabanlı bu kötü amaçlı yazılım saldırıları konusunda endişelenmek için pek bir nedenleri olmasa da, bunlar güç üretimi, elektrik şebekeleri ve savunma gibi çeşitli kritik endüstriler için açıkça büyük bir tehdittir. Gasp, virüs üreticilerinin ortak bir hedefi olsa da, Stuxnet virüs ailesi altyapıya saldırmakla daha çok ilgileniyor gibi görünüyor.

Stuxnet solucanı ne yaptı?

Stuxnet'in İran'ın Natanz uranyum zenginleştirme tesisindeki çok sayıda santrifüjü kendilerini yakarak yok ettiği bildirildi. Zamanla, diğer gruplar virüsü su arıtma tesisleri, enerji santralleri ve gaz hatları gibi tesisleri hedef alacak şekilde değiştirdi.

Stuxnet, USB belleklerde dolaşan ve Microsoft Windows bilgisayarlarına yayılan çok parçalı bir solucandı. Virüs, PLC olarak hizmet veren endüstriyel bilgisayarların elektromekanik ekipmanları otomatikleştirmek ve izlemek için kullandığı Siemens Step 7 yazılımının belirtileri için her enfekte olmuş PC'yi aradı. Bir PLC bilgisayarı bulduktan sonra, kötü amaçlı yazılım saldırısı kodunu internet üzerinden güncelledi ve PC'nin kontrol ettiği elektromekanik ekipmana hasara neden olan talimatlar göndermeye başladı. Aynı zamanda, virüs ana denetleyiciye yanlış geri bildirim gönderdi. Ekipmanı izleyen herhangi biri, ekipman kendini imha etmeye başlayana kadar bir sorun belirtisi görmezdi.

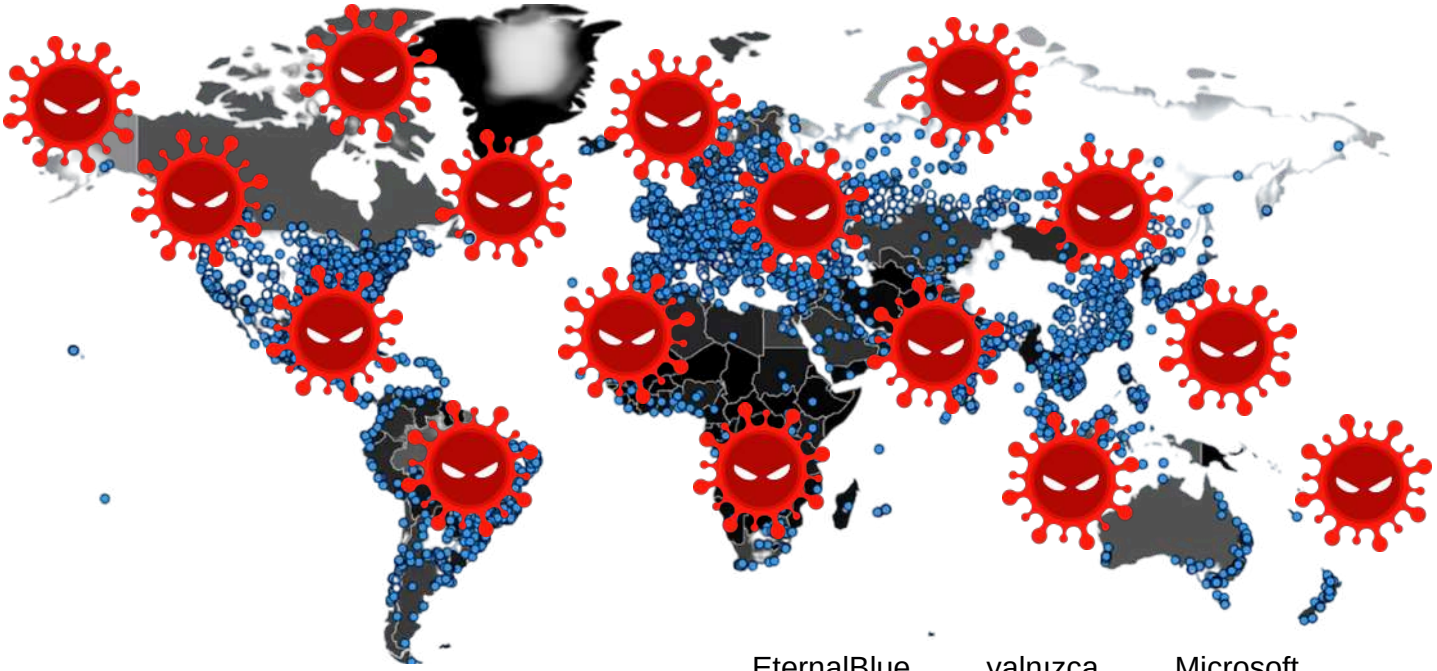
12 Mayıs 2017 Cuma günü benzeri görülmemiş bir siber fidye yazılımı saldırısı dünyayı kasıp kavurdu. WannaCry adlı bu fidye yazılımı, Pazartesi itibarıyla dünya çapında 200.000'den fazla sistemi etkiledi ve 150'den fazla ülkeyi etkiledi. İngiltere'nin Ulusal Sağlık Hizmetleri'ndeki (NHS) en az 16 hastane etkilendi ve hemşireler ile doktorlar hastaların sağlık kayıtlarından tamamen dışlandı. Bu, bugüne kadarki en ciddi, yaygın kötü amaçlı yazılım saldırısı ve 22 yaşındaki bir güvenlik araştırmacısının hızlı eylemleri sayesinde yavaşladı... ama durmadı.

WannaCry fidye yazılımı saldırısı 12 Mayıs 2017'de gerçekleşti ve 200.000'den fazla bilgisayarı etkiledi. WannaCry, dünya çapındaki ağlarda solucan oluşturmak için yamalanmamış bir güvenlik açığını kullandı.

WANNACRY

WannaCry fidye yazılımı * saldırısı, tüm dünyadaki kuruluşları etkileyen büyük bir güvenlik olayıydı. 12 Mayıs 2017'de WannaCry fidye yazılımı solucanı 150'den fazla ülkede 200.000'den fazla bilgisayara yayıldı. Önemli kurbanlar arasında FedEx, Honda, Nissan ve İngiltere'nin Ulusal Sağlık Hizmeti (NHS) vardı; ikincisi ambulanslarının bir kısmını alternatif hastanelere yönlendirmek zorunda kaldı.

WannaCry, "EternalBlue" adlı bir güvenlik açığı istismarını kullanarak yayıldı. ABD Ulusal Güvenlik Ajansı (NSA) muhtemelen kendi kullanımı için bu istismarı geliştirmişti, ancak NSA'nın kendisi tehlikeye atıldıktan sonra Shadow Brokers adlı bir grup tarafından çalındı ve kamuoyuna açıklandı.



Saldırıdan birkaç saat sonra WannaCry geçici olarak etkisiz hale getirildi. Bir güvenlik araştırmacısı, esasen kötü amaçlı yazılımı kapatan bir "kill switch" keşfetti . Ancak, etkilenen bilgisayarların çoğu, kurbanlar fidyeyi ödeyene veya şifrelemeyi tersine çevirebilene kadar şifrelenmiş ve kullanılamaz durumda kaldı.

EternalBlue yalnızca Microsoft Windows'un eski, yamalanmamış sürümlerinde çalışıyordu, ancak WannaCry'nin hızla yayılmasını sağlayacak kadar çok sayıda makine bu sürümleri çalıştırıyordu.

* Fidye yazılımı, dosyaları ve verileri şifreleyerek kilitleyen ve fidye için tutan kötü amaçlı yazılımdır.

WannaCry fidye yazılımı saldırısı, Mayıs 2017'de gerçekleşen dünya çapında bir siber saldırıydı. Siber saldırı, Windows çalıştıran bilgisayarları hedef aldı. Saldırganlar verileri şifreledi ve fidye talep etti, eğer bu ödenmezse grup verileri/bilgileri yayınlamakla tehdit etti. Microsoft, saldırıdan 12 ay önce olası bir saldırıdan haberdar edildi ve Windows çalıştıran tüm elektronik cihazlara kurulacak bir güvenlik yaması yayınladı.

Microsoft'un tavsiyesine rağmen yamayı yüklemeyen kuruluşlar hedef haline geldi. WannaCry fidye yazılımı saldırısı sonucunda 156 ülkede 200.000 bilgisayar etkilendi.

Ancak County Durham ve Darlington NHS Vakfı Güveni (CDDFT) doğrudan bir saldırıya maruz kalmadı:

Ambulans hizmeti, ağlarına erişimi kapatarak ağlarını korudu ve bunun başlıca etkisi şu oldu:

- Ambulans teslim süreci ve ekranlar devre dışı bırakıldı
- Hasta Nakil Hizmeti rezervasyon portalı kullanılamıyor.

Üçüncül merkezler ağlarına erişimi kapatarak ağlarını korudular, bunun başlıca etkisi şunlar oldu:

- BT/MR taramalarını aktaramadık
- Kemoterapi Bakımına erişemedik, bu da Kemoterapi siparişlerini sağlayıcımıza aktaramadığımız anlamına geliyor
- .

Birincil bakım BT sağlayıcısı, ağlarına erişimi kapatarak ağlarını korudu; bunun başlıca etkisi

- Kan sonuçlarının otomatik aktarımı başarısız oldu.
- Bazı pratisyen hekimler kendi vaka yüklerine erişemedi.

WannaCry saldırısı o kadar hızlı yayıldı ve dünya çapında o kadar çok bilgisayarı etkiledi ki birçok endüstri etkilendi. Bunlar arasında şunlar yer alır:

Sağlık hizmeti
Acil durum
Güvenlik
Lojistik
Telekom
Gaz
Benzin
Otomotiv
Eğitim
Reklamcılık

WannaCry tahmini olarak 230.000 bilgisayara saldırdı. Kötü amaçlı yazılım hastanelerin, acil servislerin, benzin istasyonlarının ve hatta fabrikaların operasyonlarını etkiledi. Bazı tahminler saldırının maliyetinin milyarlarca dolar olduğunu söylüyor.

Amerika Birleşik Devletleri, WannaCry saldırısından resmen Kuzey Kore'yi sorumlu tutuyor ve hatta kötü amaçlı yazılım ve 2014 Sony Pictures Entertainment saldırısından dolayı üç Kuzey Koreliyi suçladı. İlginçtir ki, NSA (Ulusal Güvenlik Ajansı) da istemeden de olsa WannaCry saldırısında rol oynamış olabilir.

İddiaya göre, NSA, WannaCry'ın istismar ettiği SMB açığını ortaya çıkardı. Daha sonra, sözde EternalBlue istismar aracının istihbarat örgütünden çalındığı ve bir hacker grubu olan The Shadow Brokers (TSB) tarafından sızdırıldığı iddia edildi.

WannaCry fidye yazılımı saldırısından kim sorumluydu?

2017'nin sonlarında, ABD ve İngiltere, WannaCry'nin arkasında Kuzey Kore hükümetinin olduğunu duyurdu . Ancak, bazı güvenlik araştırmacıları bu atıfı tartışıyor . Bazıları, WannaCry'nin doğrudan Kuzey Kore hükümetinden gelmese de, Kuzey Kore merkezli Lazarus Group'un işi olabileceğini iddia ediyor. Diğerleri, kötü amaçlı yazılımdaki yazarlık ipuçlarının, suçu Kuzey Kore merkezli saldırganlara atmak için oraya yerleştirilmiş olabileceğini ve WannaCry'nin tamamen başka bir bölgeden olabileceğini öne sürüyor.

WannaCry saldırısı nasıl durduruldu?

Saldırı günü, Marcus Hutchins adlı bir güvenlik blog yazarı ve araştırmacısı WannaCry kaynak kodunun tersine mühendisliğini yapmaya başladı. WannaCry'nin alışılmadık bir işlevi olduğunu keşfetti: Çalıştırmadan önce, iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com etki alanını sorguluyordu . Bu web sitesi mevcut değildi.

Yani alan adını tescil ettirdi. (Maliyeti 10.69$' dı .)

Hutchins bunu yaptıktan sonra, WannaCry'ın kopyaları yayılmaya devam etti, ancak yürütmeyi bıraktılar. Esasen, WannaCry iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com' dan bir yanıt almaya başladığında kendini kapattı.

Peki bu saldırıyı neden durdurdu?

WannaCry yazarlarının motivasyonları kesin olarak bilinmemekle birlikte, bu alan adı sorgulama işlevinin WannaCry'a, fidye yazılımının bir sanal alanda olup olmadığını kontrol edebilmesi için eklendiği teorileştiriliyor.

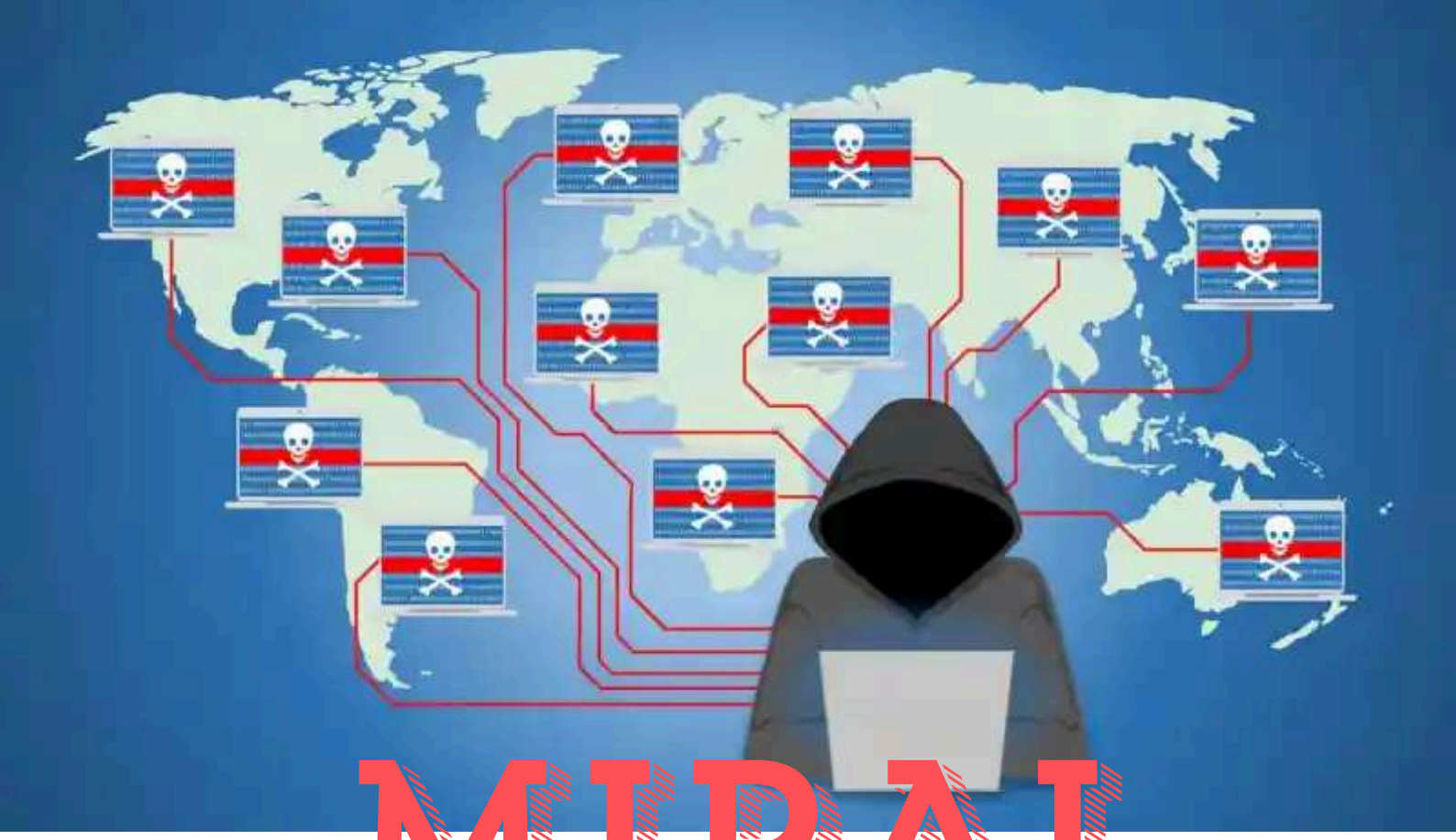
Sandbox, kötü amaçlı yazılımlara karşı bir araçtır. Diğer tüm sistemlerden ve ağlardan ayrı çalışan bir sanal makinedir . Güvenilmeyen dosyaları çalıştırmak ve ne yaptıklarını görmek için güvenli bir ortam sağlar.

Bir sanal alan aslında İnternet'e bağlı değildir. Ancak sanal alanlar mümkün olduğunca gerçek bir bilgisayarı taklit etmeyi amaçlar, bu nedenle kötü amaçlı yazılım tarafından belirli bir etki alanına yönlendirilen bir sorguya sahte bir yanıt üretebilirler. Sonuç olarak, kötü amaçlı yazılımın bir sanal alanın içinde olup olmadığını kontrol etmesinin bir yolu, sahte bir etki alanına bir sorgu göndermektir. "Gerçek" bir yanıt alırsa (sanal alan tarafından üretilir), bir sanal alanda olduğunu varsayabilir ve sanal alan onu kötü amaçlı olarak algılamasın diye kendini kapatabilir.

Ancak, kötü amaçlı yazılım test sorgusunu sabit kodlanmış bir etki alanına gönderirse, birisi etki alanını kaydederse her zaman bir sanal alanda olduğunu düşünerek kandırılabilir. WannaCry'da olan da bu olabilir: Dünya çapındaki WannaCry kopyaları bir sanal alanda olduklarını düşünerek kandırılmış ve kendilerini kapatmışlardır. (Kötü amaçlı yazılım yazarının bakış açısından daha iyi bir tasarım, her seferinde farklı olan rastgele bir etki alanını sorgulamak olurdu - bu şekilde, sanal alanın dışında etki alanından bir yanıt alma olasılığı sıfıra yakın olurdu.)

Başka bir olası açıklama ise, dünyaya yayılan WannaCry kopyasının tamamlanmamış olmasıdır. WannaCry'nin yazarları, solucanı serbest bırakmadan önce kendi komuta ve kontrol (C&C) sunucularının adresiyle değiştirmeyi amaçlayarak bu etki alanını bir yer tutucu olarak sabit kodlamış olabilirler. Ya da iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com' u kendileri kaydetmeyi amaçlamış olabilirler. (DNS filtreleme veya URL filtreleme belki de bu etki alanına yapılan sorguları durdurabilirdi, ancak çoğu kuruluş bu güvenlik önlemini zamanında uygulayamazdı.)

Nedeni ne olursa olsun, bu kadar basit bir eylemin dünya çapındaki bilgisayarları ve ağları daha fazla enfeksiyondan kurtarabilmesi büyük bir şanstı.



MIRAI

2016 yılında tüm dünyayı etkisine alan bir saldırı gerçekleşti. Bu saldırı IOT cihazları hedef alarak kendine bağlı olan tüm cihazları aynı anda etkileme oranına sahipti. Ve böylece birden fazla cihaza bağlanma özelliğine sahipti. Aslında bu saldırıyı gerçekleştiren yazılım Mirai adında Japonca da "gelecek" anlamıyla bilinen bir Botnet' dir.

İlk olarak Botnet'in ne olduğunu bilmek gerekir. Botnet, kötü amaçlı kişilerin kullandığı yazılımların bağlantılı olan birden fazla cihazlara yayıp onlara görev vermeye yarar. Bot kelimesi robot kelimesinden gelir. Günümüzde teknolojinin ilerlemesiyle internet kullanılması çok ciddi bir şekilde arttı. Bu artışla birlikte Botnet virüslerinden kaçış çok zor oldu. Örneğin telefonlarınıza indirdiğiniz çok basit bir uygulama ne kadar çok kişi tarafından indirilirse o kadar ciddi bir Botnet ağı ortaya çıkıyor. Bunun yanı sıra cihazınızda ziyaret ettiğiniz her sayfada ya da bakılan maillerde ortaya çıkar. Botnet' in bir diğer önemli özelliği ise kesin bir çözümü yoktur. Bu aşamada ise her önlem büyük bir önem kazanıyor.

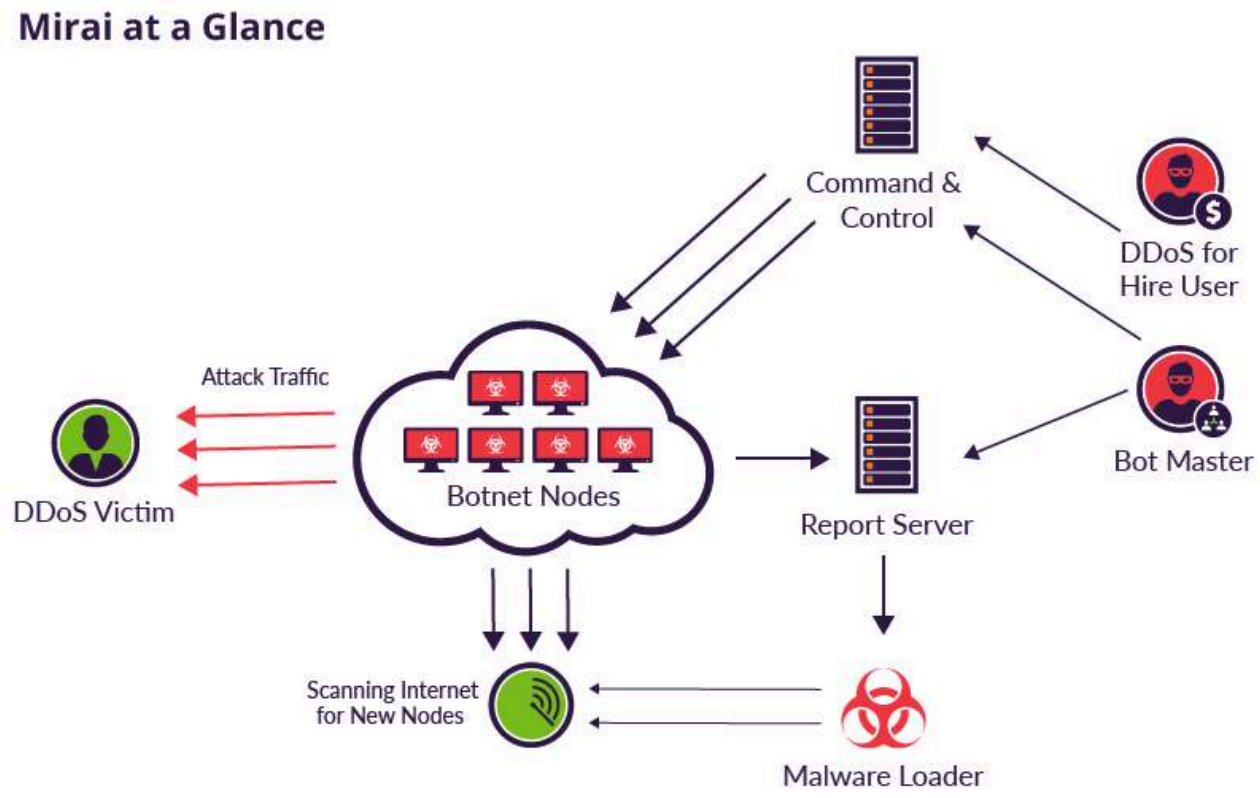
Eylül ayında gerçekleşen Mirai Botnet saldırısı birçok yerin güvenlik kameralarının bağlı olduğu sunuculara DDOS saldırı yöntemiyle gerçekleşti. Saldırı sonucu yaklaşık 25 bin kameranın görüntüleri elde edildiği gibi başta Asya ülkeleri olmak üzere Çin, Güney Kore gibi birçok ülkede de görüntüler ele geçirildi. Tabi bu olayın maliyeti şirketlere çok ciddi sonuçlar doğurdu.

Saldırıda örnek verildiği gibi Mirai botnetinin asıl hedefi IOT cihazlarıdır. IOT cihazları ne diye sormak gerekirse aslında hepimizin evinde bulunduğu birçok elektronik aletlerdir. Örnek verirsek alarm sistemi, kombi, güvenlik kamerası gibi birçok Mirai botnetinde hedef olarak yer alır.Örneğin güvenlik kamerası ya da herhangi bir görüntü algılayan bir cihaz bu yazılım sayesinde birden çok yerde görüntü alışverişi yapabilir.

Ve bu yazılım cihazınızda alarm sistemi var ise onları aktif hale getirme özelliği vardır. Bu özelliği ile çok ciddi sonuçlar doğurabilir.

Mirai yazılımının kodu değiştirilebilir olması birden fazla saldırıda kullanılabilir olduğunu gösterir. Bu nedenle gelişen her teknolojiye uyumlu olarak geliştirilmesi kolaydır. Bu yönüyle kurumsal kablosuz denetleyicilere, dijital işaret sistemlerine ve kablosuz sunum sistemlerine ulaşarak saldırılarını gerçekleştirebilir.

Siber güvenlik uzmanı olan Brian Krebs "Mirai, fabrika çıkışı otomatik kullanıcı adı ve şifrelerle korunan şeylerin interneti cihazlarını bulmak için interneti tarıyor ve daha sonra bu cihazları kullanarak, çevrimiçi hedefe yönelik gereğinden fazla internet trafiği oluşturarak bu hedefin ziyaretçi ve kullanıcılara yanıt vermesini engelliyor." açıklamasında bulundu.



Mirai (Japoncada "gelecek" anlamına gelen未来 kelimesinden) , Linux çalıştıran ağ cihazlarını büyük ölçekli ağ saldırılarında bir botnet'in parçası olarak kullanılabilen uzaktan kumandalı botlara dönüştüren bir kötü amaçlı yazılımdır . Öncelikle IP kameralar ve ev yönlendiricileri gibi çevrimiçi tüketici cihazlarını hedef alır . Mirai botnet'i ilk olarak Ağustos 2016'da MalwareMustDie , bir beyaz şapkalı kötü amaçlı yazılım araştırma grubu tarafından bulundu ve bilgisayar güvenliği gazetecisi Brian Krebs'in web sitesine 20 Eylül 2016'da yapılan saldırı , Fransız web sunucusu OVH'ye yapılan saldırı ve Ekim 2016'da Dyn'e yapılan DDoS saldırıları dahil olmak üzere en büyük ve en yıkıcı dağıtılmış hizmet reddi (DDoS) saldırılarından bazılarında kullanıldı . Anna-senpai (kötü amaçlı yazılımın orijinal yazarı) ile Robert Coelho arasındaki bir sohbet kaydına göre Mirai, 2011 yapımı TV anime dizisi Mirai Nikki'den esinlenerek adlandırılmıştır .

Yazılım ilk olarak yaratıcıları tarafından Minecraft sunucularına DDoS saldırısı düzenlemek ve Minecraft sunucularına DDoS koruması sunan şirketler tarafından kullanıldı ve yazarlar Mirai'yi bir koruma şebekesi işletmek için kullandılar . Mirai'nin kaynak kodu daha sonra Hack Forums'da açık kaynaklı olarak yayınlandı . Kaynak kodu yayınlandıktan sonra , teknikler diğer kötü amaçlı yazılım projelerine uyarlandı.

Kasım 2016'nın sonunda, Deutsche Telekom'a ait ve Arcadyan tarafından üretilen yaklaşık 900.000 yönlendirici , Mirai'nin bir çeşidi tarafından yapılan başarısız TR-064 istismar girişimleri nedeniyle çöktü ve bu da bu cihazların kullanıcıları için İnternet bağlantı sorunlarına yol açtı.TalkTalk daha sonra yönlendiricilerini yamalasa da, TalkTalk yönlendiricilerinde Mirai'nin yeni bir çeşidi keşfedildi.

BBC'ye göre saldırının arkasında olduğundan şüphelenilen bir İngiliz adam Luton Havaalanı'nda tutuklandı .

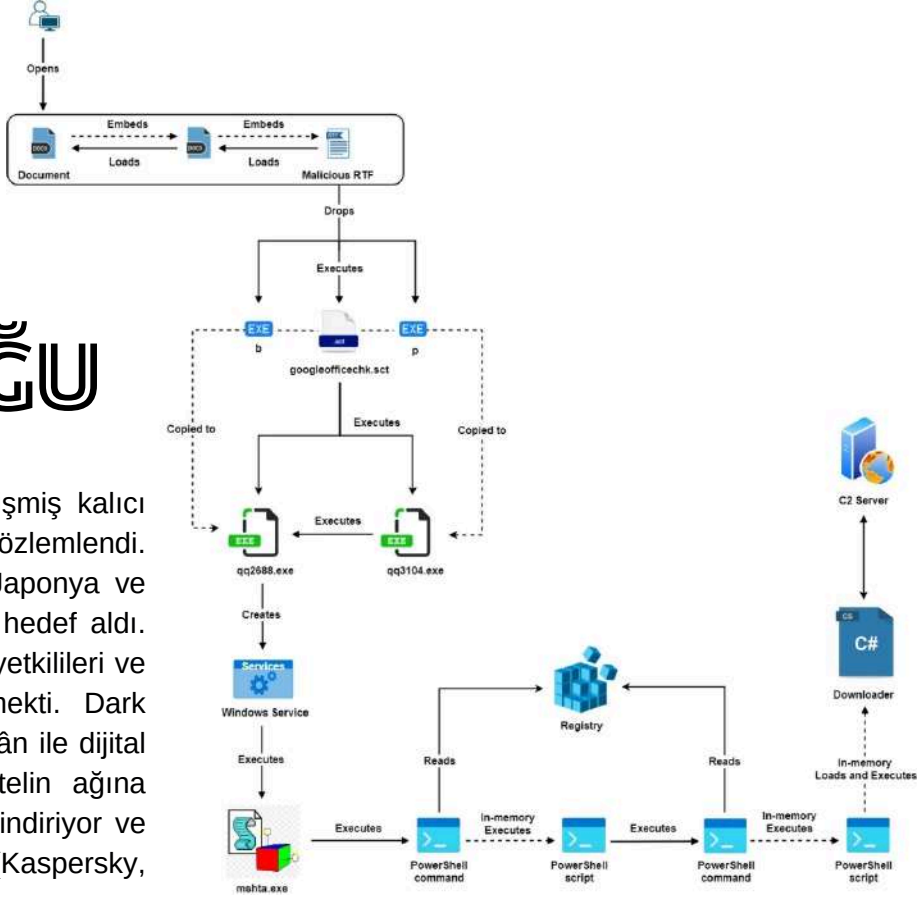
Kasım 2016'nın sonunda, Deutsche Telekom'a ait ve Arcadyan tarafından üretilen yaklaşık 900.000 yönlendirici , Mirai'nin bir çeşidi tarafından yapılan başarısız TR-064 istismar girişimleri nedeniyle çöktü ve bu da bu cihazların kullanıcıları için İnternet bağlantı sorunlarına yol açtı.TalkTalk daha sonra yönlendiricilerini yamalasa da, TalkTalk yönlendiricilerinde Mirai'nin yeni bir çeşidi keşfedildi.

BBC'ye göre saldırının arkasında olduğundan şüphelenilen bir İngiliz adam Luton Havaalanı'nda tutuklandı .

17 Ocak 2017'de bilgisayar güvenliği gazetecisi Brian Krebs , Krebs on Security adlı blogunda kötü amaçlı yazılımı yazdığına inandığı kişinin adını açıkladığı bir makale yayınladı. Krebs, Mirai'nin yazarı Anna-senpai'nin (Shimoneta'daki bir karakter olan Anna Nishikinomiya'dan adını almıştır) olası gerçek hayattaki kimliğinin, aslında Rutgers Üniversitesi öğrencisi ve DDoS azaltma hizmetleri şirketi ProTraf Solutions'ın sahibi olan Hint asıllı Amerikalı Paras Jha olduğunu belirtti . Orijinal makalenin güncellemesinde Paras Jha, Krebs'e yanıt verdi ve Mirai'yi yazdığını reddetti. FBI'ın Jha'yı Ekim 2016 Dyn siber saldırısındaki rolü hakkında sorguladığı bildirildi .13 Aralık 2017'de Paras Jha, Josiah White ve Dalton Norman , Mirai botnetiyle ilgili suçlardan suçlu bulundular. [Üçlü, hükümete diğer siber güvenlik soruşturmalarında yardımcı oldu ve hapis cezası olmaksızın denetimli serbestlik ve toplum hizmeti cezasına çarptırıldılar.

NCA'ya göre , "BestBuy", "Popopret" veya "Örümcek Adam" takma adlarıyla da bilinen 29 yaşındaki Daniel Kaye, " Lloyds Banking Group ve Barclays bankalarına saldırmak ve şantaj yapmak için Mirai botnet olarak bilinen virüslü bir bilgisayar ağı kullanmakla" suçlanıyor. Aynı rapora göre Almanya'dan İngiltere'ye iade edildi. Kaye ayrıca Deutsche Telekom ağından 900.000'den fazla yönlendiriciyi ele geçirmekten mahkemede suçunu kabul etti. araştırmacılar daha sonra Mirai'nin yeni varyantlarının (Okiru, Satori, Masuta ve PureMasuta olarak adlandırılır) yazarının "Nexus Zeta" takma adının sorumlusu olduğunu ileri sürdüler ve 21 Ağustos 2018'de bir Amerikan büyük jürisi, Anchorage'daki ABD Bölge Mahkemesi'nde açılan iddianameye göre, 20 yaşındaki Kenneth Currin Schuchman'ı, namıdiğer Nexus Zeta'yı, bilerek bir program, bilgi, kod ve komutların iletilmesine neden olmak ve bu tür bir davranışın sonucu olarak yetkisiz bir şekilde korunan bilgisayarlara kasıtlı olarak zarar vermekle suçladı ve ardından şüpheli tutuklandı ve yargılandı

DARK HOTEL CASUSLUĞU



“Dark Hotel” olarak adlandırılan gelişmiş kalıcı tehdit (APT), ilk kez 2007’de gözlemlendi. Operatörler, özellikle Güney Kore, Japonya ve Çin’deki lüks otellerin Wi-Fi ağlarını hedef aldı. Amaç, üst düzey iş insanları, devlet yetkilileri ve askeri personelin cihazlarına erişmekti. Dark Hotel’in en kritik özelliği, fiziksel mekân ile dijital saldırıyı birleştirmesiydi. Kurban, otelin ağına bağlandığında zararlı güncellemeler indiriyor ve cihazı arka planda ele geçiriliyordu (Kaspersky, 2014).

Saldırganlar, çok katmanlı teknikler kullandı:

- Sahte yazılım güncellemeleri: Adobe Flash, Google Toolbar veya Windows Update gibi görünümlü dosyalar sunuluyordu.
- Keylogger ve casus yazılımlar: Yöneticilerin e-postaları, belgeleri, toplantı notları çalındı.
- Hedefli spear-phishing: Bazı saldırılar otel bağlantısı olmadan da devam etti; kişilere doğrudan zararlı e-postalar gönderildi.

Hedefler arasında uluslararası iş görüşmelerine katılan CEO’lar, silah endüstrisi temsilcileri ve diplomatlar bulunuyordu. 2014–2017 arasında saldırının en yoğun olduğu tespit edildi.

- NotPetya, siber saldırıların yıkıcı ve kontrolsüz doğasını gösterirken;
- Dark Hotel, siber casusluğun ne kadar sabırlı, görünmez ve sofistike olabileceğini kanıtladı.

Her iki vaka da, siber savaşın artık yalnızca devletlerarası değil, küresel ekonomi, özel sektör ve bireyler üzerinde de belirleyici etkiler yaratabileceğini açıkça ortaya koydu.

Dark Hotel operasyonu on yıl boyunca sürdü ve pek çok kritik verinin gizlice ele geçirilmesine neden oldu. Araştırmalar, saldırının arkasında Kuzeydoğu Asya kökenli devlet destekli gruplar olabileceğini gösterdi. Ancak hiçbir devlet doğrudan sorumluluk üstlenmedi.

- Stratejik Etki: Dark Hotel, siber casusluğun ne kadar “görünmez” olabileceğini ortaya koydu. 10 yıl boyunca fark edilmemesi, APT gruplarının sabırla ve seçici şekilde çalıştığını gösterdi. Ayrıca, bu vaka devlet dışı alanların (oteller, özel sektör, seyahat altyapısı) dahi siber savaşta kritik zafiyet noktaları olabileceğini ispatladı (Kaspersky, 2014).

- Otel Wi-Fi Ağına Sızma
- Kurban otele giriş yapıp Wi-Fi'ye bağlandığında, saldırganlar ağı manipüle ederek sahte yazılım güncellemeleri gönderiyordu. Örneğin:
- "Adobe Flash Player güncellemesi"
- "Google Toolbar update"
- "Windows Update"
- gibi görünümlerde zararlı yazılımlar.
- APT (Advanced Persistent Threat) Teknikleri
- Keylogger: Klavyeden girilen her şeyi kaydediyordu (şifreler, e-postalar).
- Trojan Downloader: Yeni zararlı yazılımları sisteme indiriyordu.
- Veri Çalma: E-postalar, toplantı notları, proje dosyaları, sunumlar gizlice toplanıyordu.
- Spear-Phishing
- Sadece otel ağında değil, hedeflerin kişisel e-postalarına özel hazırlanmış zararlı dosyalar gönderildi. Böylece saldırı, seyahat dışında da devam ettirildi.
- Dark Hotel, klasik askeri çatışma yerine siber casuslukta sabır, seçicilik ve hedef odaklılık unsurlarının ne kadar etkili olduğunu gösterdi.
- Bu vaka, aynı zamanda "dijital diplomasi güvenliği" kavramını doğurdu: diplomatik heyetlerin seyahat ettiği oteller, artık kritik güvenlik noktaları olarak değerlendirilmeye başlandı.
- Siber güvenlik literatüründe Dark Hotel, "konaklama sektörünün ulusal güvenlik riski oluşturabileceği" örneğiyle ön plana çıktı (Kaspersky, 2014).

Operasyonun Özellikleri

- Seçici Hedefleme: Saldırganlar, otele bağlanan herkesle ilgilenmiyor; yalnızca "önceden belirlenen üst düzey hedeflere" saldırıyordu. Bu, sıradan suç gruplarının işine benzemiyor; istihbarat amaçlı "özel hedef listeleri" olduğunu gösteriyor.
- Uzun Süre Gizlilik: 10 yıl boyunca fark edilmeden sürdü. Bu süreklilik, operasyonun sabırlı ve sistematik bir yapı tarafından desteklendiğini ortaya koyuyor.
- Jeopolitik Bağlantı: Hedeflerin çoğu Asya'daki diplomatik, ekonomik ve savunma alanlarında önemli aktörlerdi. Bu nedenle uzmanlar, saldırının Kuzeydoğu Asya kökenli devlet destekli bir grup tarafından yürütüldüğünü değerlendiriyor.

Sonuç ve Etkiler

- Diplomatik Güven Sorunu: Devletler arası görüşmelerin ve iş anlaşmalarının güvenliği sarsıldı. Otel altyapılarının "siber savaşın yeni cephesi" olabileceği ortaya çıktı.
- Özel Sektörün Zafiyeti: CEO'ların cihazlarından alınan bilgiler, şirket birleşmeleri, patent anlaşmaları ve ticari stratejilerin çalınmasına yol açtı.
- Devlet Sorumluluğu: Resmî olarak kimse üstlenmedi; ama saldırının devlet destekli APT gruplarının işi olduğu genel kabul gördü.

MAFIABOY

2000 yılının Şubat ayında, 15 yaşındaki Kanadalı lise öğrencisi Michael Calce (takma adıyla Mafiaboy), henüz emekleme aşamasında olan internetin en büyük şirketlerine yönelik saldırılar düzenledi. Calce, basit görünen bir yöntem kullandı: DDoS (Dağıtık Hizmet Engelleme) saldırısı. Bu saldırıda, ele geçirilen bilgisayarlar (botnet) belirli hedef sitelere aynı anda aşırı trafik yönlendirerek sunucuları çökertiyordu.

Calce'nin saldırılarını başlatma sebebi, kendi deyimiyle "gücünü kanıtlamak ve alanında saygı görmek"ti. Ancak yaptığı şey, tarihte ilk kez internetin küresel ölçekte ne kadar kırılgan olduğunu göstermiş oldu.

Hedefler: Yahoo!, CNN, Amazon, eBay, Dell gibi dönemin en popüler ve trafiği yüksek siteleri.

Sonuç: Bu dev siteler saatlerce hatta günlerce erişilemez hale geldi. Yahoo! bir gün boyunca kapalı kaldı; bu, o dönemde internet kullanıcılarının büyük kısmını etkileyen görülmemiş bir kesinti demekti.

Etkiler:

CNN haber yayını durdu.

Amazon'un satışları milyonlarca dolar kayba uğradı.

EBay'in açık artırma işlemleri aksadı.

Kısacası, küresel ticaret ve medya, daha önce görülmemiş biçimde tek bir genç bireyin eylemleriyle sarsıldı.

Stratejik Etkiler

1. İlk Küresel Alarm: Devletler, internet güvenliğinin yalnızca teknik bir sorun olmadığını; aynı zamanda ulusal güvenlik, ekonomi ve diplomasi meselesi olduğunu gördü.
2. Hacker Profilinin Değişimi: Daha önce "siber saldırı" dendiğinde akla yalnızca devletler veya organize gruplar gelirken, Mafiaboy vakası bir gencin bile küresel sistemi sarsabileceğini kanıtladı.
3. Yasal Düzenlemeler: ABD ve Kanada'da siber suçlara yönelik yasalar sertleştirildi. Siber saldırılar, "ulusal güvenliği tehdit eden eylemler" kategorisine alındı.
4. Kamu Farkındalığı: Şirketler, güvenlik yatırımlarını artırmaya başladı. Özellikle e-ticaret siteleri, saldırılara karşı "yüksek bant genişliği + güvenlik duvarı" politikalarına yöneldi.

1990’ların sonunda internet, “dot-com patlaması” ile ekonomik ve toplumsal yaşamda merkezî bir rol üstlenmeye başlamıştı. Yahoo! ve Amazon gibi şirketler, dijital ekonominin sembolleri haline gelmişti. Ancak aynı dönemde internet güvenliği, neredeyse hiç tartışılmayan bir alan olarak kaldı. Güvenlik açıkları çok temel seviyedeydi ve saldırı yöntemleri, çoğunlukla deneysel düzeydeydi. İşte böyle bir ortamda lise öğrencisi Michael Calce sahneye çıktı.

Calce, Montreal’de yaşayan 15 yaşında bir lise öğrencisiydi. “Mafiaboy” takma adıyla çeşitli hack topluluklarında bulunuyor, internet üzerinden saygınlık kazanmak için diğer hacker gruplarıyla rekabet ediyordu. Amacı, en çok dikkat çeken saldırılara imza atarak “alanın kralı” olduğunu göstermekti (Calce & Silverman, 2008).

Kullandığı Yöntem: Dağıtık Hizmet Engelleme (DDoS).

- Nasıl Çalıştı?

1. İnternette korumasız sunucuları ve bilgisayarları taradı.
2. Bu sistemlere kötü amaçlı yazılım yerleştirdi.
3. Ele geçirilen bilgisayarları (zombi bilgisayarlar → botnet) uzaktan kontrol ederek hedef sitelere aşırı trafik yönlendirdi.

- Özellik: O dönemde “botnet” kavramı yeni yeni ortaya çıkıyordu. Calce’nin yöntemi, daha sonra Mirai gibi gelişmiş saldırıların habercisi oldu.

Sonuç

Ekonomik: ABD Kongresi’ne göre saldırıların toplam maliyeti 1,2 milyar doları aştı.

Siyasi: Olay ABD Senatosu’nda gündem oldu. FBI, RCMP (Kanada Kraliyet Polisi) ve ABD Gizli Servisi ortak soruşturma başlattı.

Hukuki: Michael Calce yakalandı, suçlu bulundu ve genç yaşından ötürü 8 ay “gençlik ıslahevi” cezası aldı. Ayrıca 1 yıl internetten men edildi.

Stratejik Etki

Bireyin gücü: İlk kez, bir bireyin (üstelik 15 yaşında bir lise öğrencisinin) küresel dev şirketleri diz çöktürebileceği görüldü.

Kırılganlık farkındalığı: İnternet altyapısının ve e-ticaret sistemlerinin ne kadar savunmasız olduğu ortaya çıktı.

Politik sonuç: ABD ve Kanada, bu olaydan sonra siber güvenlik yasalarını ve cezai yaptırımları sıkılaştırdı. Siber suçların “ulusal güvenlik” başlığı altında ele alınması gerektiği kabul edildi.

Michael Calce, cezasını tamamladıktan sonra siber güvenlik danışmanı oldu. 2008’de yayımladığı “Mafiaboy: How I Cracked the Internet and Why It’s Still Broken” adlı kitabında saldırılarını, motivasyonlarını ve internetin hâlâ kırılgan olduğunu anlattı.

Bugün hâlâ güvenlik konferanslarında konuşmacı olarak yer almakta ve genç hacker’ların suç yerine güvenlik alanına yönlendirilmesi gerektiğini savunmaktadır.

ÖZEL DOSYA

LEBANON PAGER EXPLOSIONS

LEBANON PAGER PLOSIONS

Lübnan Sağlık Bakanı, silahlı örgüt Hizbullah'a bağlı militanların haberleşmek için kullandığı el tipi çağrı cihazlarının patlaması sonucu biri çocuk dokuz kişinin hayatını kaybettiğini açıkladı.

Beyrut ve diğer bazı bölgelerde eş zamanlı gerçekleşen patlamalarda yaralanan 2 bin 800 kişi arasında İran'ın Lübnan büyükelçisi de bulunuyor.

İran destekli Hizbullah, çağrı cihazlarının "çeşitli Hizbullah birimleri ve kurumlarının çalışanlarına" ait olduğunu belirterek, sekiz savaşçının öldüğünü doğruladı.

Grup, İsrail'i "bu suç teşkil eden saldırı" olarak adlandırdığı şeyden sorumlu tuttu ve "adil bir misilleme" alacağına yemin etti. İsrail ordusu yorum yapmayı reddetti.

Saldırının nasıl planlandığı ve gerçekleştirildiğine ilişkin henüz bir açıklama yapılmadı.

Yaygın olarak dolaşan ancak doğrulanmamış bir videoda , bir adamın çağrı cihazı çalmadan hemen önce onu kontrol ettiği görülüyor; bu da patlamanın gelen bir mesajdan kaynaklanmış olabileceğini düşündürüyor.

Çevrimiçi olarak, bazıları pillerin bir şekilde aşırı ısınmış olabileceğini tahmin etti. Ancak ABD Ordusu'nda eski bir patlayıcı mühimmat imha teknisyeni olan Trevor Ball, çağrı cihazlarına patlayıcıların yerleştirilmiş olması gerektiğine inandığını söyledi.

Ball, NPR'ye gönderdiği mesajda, "Çağrı cihazlarının video ve fotoğraflarına dayanarak, çağrı cihazlarında uzaktan başlatılan az miktarda yüksek patlayıcı olduğu anlaşılıyor," dedi. "Çağrı cihazlarının yaygın bir şekilde patlaması, çağrı cihazlarının tedarik zincirinin bir noktada tehlikeye girdiğini gösteriyor."

Hizbullah üyeleri, yaklaşık bir yıl önce İsrail ile yoğun çatışmalar patlak verdikten sonra çağrı cihazları taşımaya başladılar.

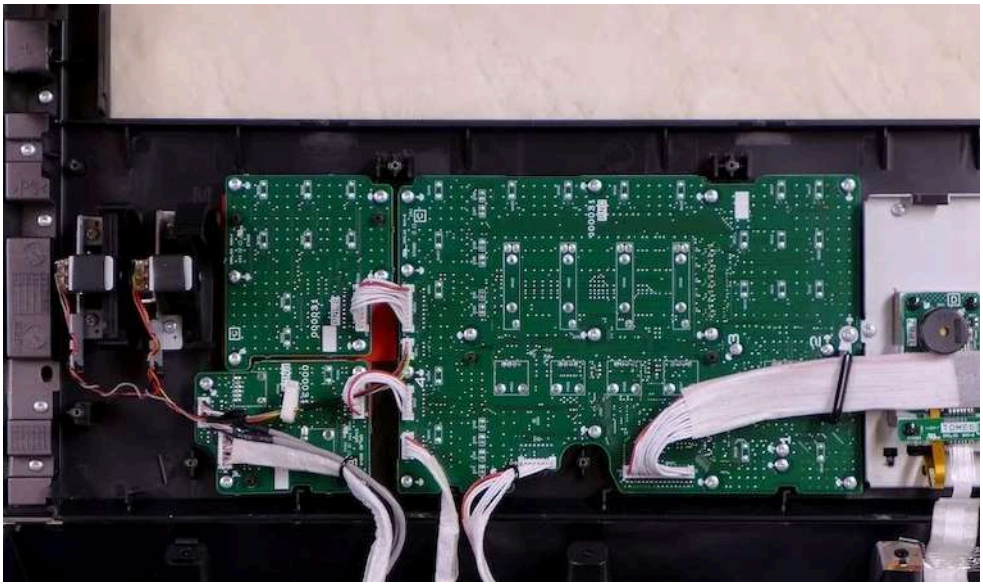
Hizbullah, İsrail güvenlik servislerinin sıklıkla telefon ağlarına girebildiğini biliyor ve grubun lideri Hasan Nasrallah, Şubat ayında yaptığı bir konuşmada üyelere telefonlarından kurtulmalarını söyledi.

Grup, çağrı cihazlarının iletişim kurmak için daha güvenli bir yol sağlayacağını düşündü.

Lübnan'dan gelen haberlere göre Hizbullah yakın zamanda, İsrail'in olası insansız hava aracı saldırıları ve diğer saldırılar hakkında bilgi paylaşmak için kullanılan yeni bir parti ithal çağrı cihazı aldı.

Salı günü saat 15:30 civarında gerçekleşen patlamaların ardından Sağlık Bakanlığı, "Kablosuz iletişim cihazlarına sahip olan tüm vatandaşlara bunlardan uzak durmalarını" söyledi. Hizbullah, yakın zamanda yeni çağrı cihazı alan tüm üyelerine bunları atmalarını söyledi.

Lübnan Sağlık Bakanı Firass Abiad Salı akşamı en az 2.800 kişinin yaralandığını söyledi. Çoğunun yüzünde, ellerinde ve gövde kısmında yaralar vardı. Lübnan'daki çeşitli medya raporları ölü sayısını dokuz olarak verdi.



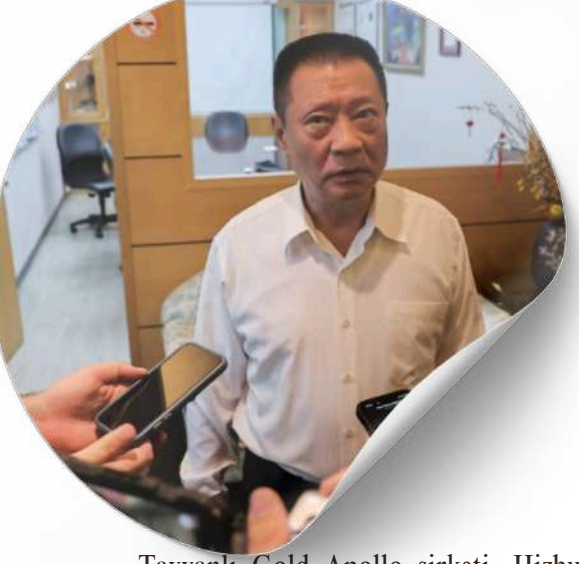
Hizbullah, İsrail güvenlik servislerinin sıklıkla telefon ağlarına girebildiğini biliyor ve grubun lideri Hasan Nasrallah, Şubat ayında yaptığı bir konuşmada üyelere telefonlarından kurtulmalarını söyledi.

Grup, çağrı cihazlarının iletişim kurmak için daha güvenli bir yol sağlayacağını düşündü.

Lübnan'dan gelen haberlere göre Hizbullah yakın zamanda, İsrail'in olası insansız hava aracı saldırıları ve diğer saldırılar hakkında bilgi paylaşmak için kullanılan yeni bir parti ithal çağrı cihazı aldı.

Salı günü saat 15:30 civarında gerçekleşen patlamaların ardından Sağlık Bakanlığı, "Kablosuz iletişim cihazlarına sahip olan tüm vatandaşlara bunlardan uzak durmalarını" söyledi. Hizbullah, yakın zamanda yeni çağrı cihazı alan tüm üyelerine bunları atmalarını söyledi.

Lübnan Sağlık Bakanı Firass Abiad Salı akşamı en az 2.800 kişinin yaralandığını söyledi. Çoğunun yüzünde, ellerinde ve gövde kısmında yaralar vardı. Lübnan'daki çeşitli medya raporları ölü sayısını dokuz olarak verdi.



KURUCUSU, ÇAĞRI CİHAZLARININ BAC TARAFINDAN LİSANS ALTINDA ÜRETİLDİĞİNİ SÖYLÜYOR GOLD APOLLO, ÜRÜNÜN TASARIMINDA VEYA ÜRETİMİNDE YER ALMADIĞINI SÖYLÜYOR

Tayvanlı Gold Apollo şirketi, Hizbullah'ın iletişim ağını hedef alan, İsrail'in düzenlediği bir operasyonda Lübnan ve Suriye'de patlayan çağrı cihazlarında kendi markasının kullanımına izin verdiğini ancak bu cihazların Budapeşte merkezli başka bir şirket tarafından üretildiğini açıkladı.

Salı günü her iki ülkede de çağrı cihazları neredeyse aynı anda patladı, en az 12 kişi öldü, yaklaşık 3.000 kişi yaralandı .

Hizbullah ve Lübnan hükümeti, uzaktan kumandalı bir saldırı gibi görünen olaydan İsrail'i sorumlu tuttu.

Tayvan, NEW TAIPEI, 18 Eylül (Reuters) - Tayvanlı çağrı cihazı firması Gold Apollo, Çarşamba günü yaptığı açıklamada, Lübnan'daki patlamalarda kullanılan çağrı cihazlarının modelinin Budapeşte merkezli BAC Consulting tarafından yapıldığını, şirketin yalnızca markasını şirkete lisansladığını ve cihazların üretiminde yer almadığını belirtti.

Salı günü Lübnan'da Hizbullah üyeleri tarafından kullanılan çağrı cihazları aynı anda patladığında en az dokuz kişi öldü ve yaklaşık 3.000 kişi yaralandı. Üst düzey bir Lübnan güvenlik kaynağına ve başka bir kaynağa göre , cihazların içindeki patlayıcılar İsrail'in Mossad casusluk ajansı tarafından yerleştirildi.

Hizbullah lideri Hasan Nasrallah daha önce grubun üyelerini cep telefonu taşımamaları konusunda uyarmış ve İsrail'in hedefli saldırılar için grubun hareketlerini izlemek amacıyla bunları kullanabileceğini söylemişti. Sonuç olarak örgüt iletişim kurmak için çağrı cihazları kullanıyor.

Bir Hizbullah yetkilisi The Associated Press'e, patlayan cihazların grubun daha önce kullanmadığı yeni bir markaya ait olduğunu söyledi. Basınla konuşma yetkisi olmadığı için isminin açıklanmaması koşuluyla konuşan yetkili, marka adını veya tedarikçiyi belirtmedi.

Hizbullah, Salı günü Lübnan genelinde çok sayıda kişinin ölümüne ve binlerce kişinin yaralanmasına yol açan İsrail saldırısına yanıt vereceğine yemin etti. İran destekli militan gruba ait çağrı cihazları neredeyse aynı anda patladı . Bu , büyük bir güvenlik ihlalini açığa çıkardı ve İsrail istihbaratının boyutunu gösterdi.

Lübnan Sağlık Bakanı Firass Abiad, patlamalarda ölen en az dokuz kişiden birinin çocuk olduğunu ve yaklaşık 2.800 kişinin yaralandığını söyledi. En az 170 kişinin kritik durumda olduğunu söyledi, ancak diğer yaralanmaların niteliği belirsiz.

Benzeri görülmemiş saldırı, İsrail'in Gazze'de Hamas'a karşı yürüttüğü savaş nedeniyle Orta Doğu'da zaten artan gerginliği daha da tırmandırma riski taşıyor. Bu sıra dışı olay, Hizbullah'ın iletişim ağının ölümcül bir şekilde tehlikeye atılması ve komutanlarına yönelik bir dizi hedefli suikastın ardından gelmesi nedeniyle savunmasızlığını da vurguluyor.

LÜBNAN'DA ÇAĞRI CİHAZLARI NASIL PATLADI?

İsrail, haberleşme cihazlarının bataryalarının içine patlayıcı yerleştirdi ve bataryaların sıcaklığını uzaktan artırarak patlattı. Bu operasyonda diğer patlayıcı türleri yerine PETN adlı patlayıcıyı kullandılar. PETN dünyada bilinen en güçlü patlayıcılardan biri. Isıya ve sürtünmeye karşı hassastır, bu da patlama mekanizmasını açıklayabilir. Patlayıcı madde, cihazlar Hizbullah'a ulaşmadan önce yerleştirildi. Hizbullah'ın tedarik zincirine sızıldı. El Cezire, her bir cihazın içine 20 gram patlayıcı yerleştirildiğini ve Hizbullah'ın bunları 5 ay önce kullanmaya başladığını aktardı.

PATLAYAN ÇAĞRI CİHAZLARI NE MARKA?

Lübnan resmi ajansı NNA'ya göre, İsrail'in "pager" isimli çağrı cihazlarına sızıp patlatması sonucu çok sayıda Lübnanlı yaralandı. Sosyal medyada paylaşılan son cihaz ise Tayvan menşeli "Apollo Gold" şirketi tarafından üretilen ve Hong Kong menşeli "Apollo Systems HK" şirketi tarafından satılan "Gold Apollo Rugged Pager AR924" model ürün. Paylaşımlarda parçalanmış ancak model bilgileri okunabilen Apollo marka çağrı cihazlarının görselleri yer aldı.

Patlamalar nasıl tetiklenmiş olabilir?

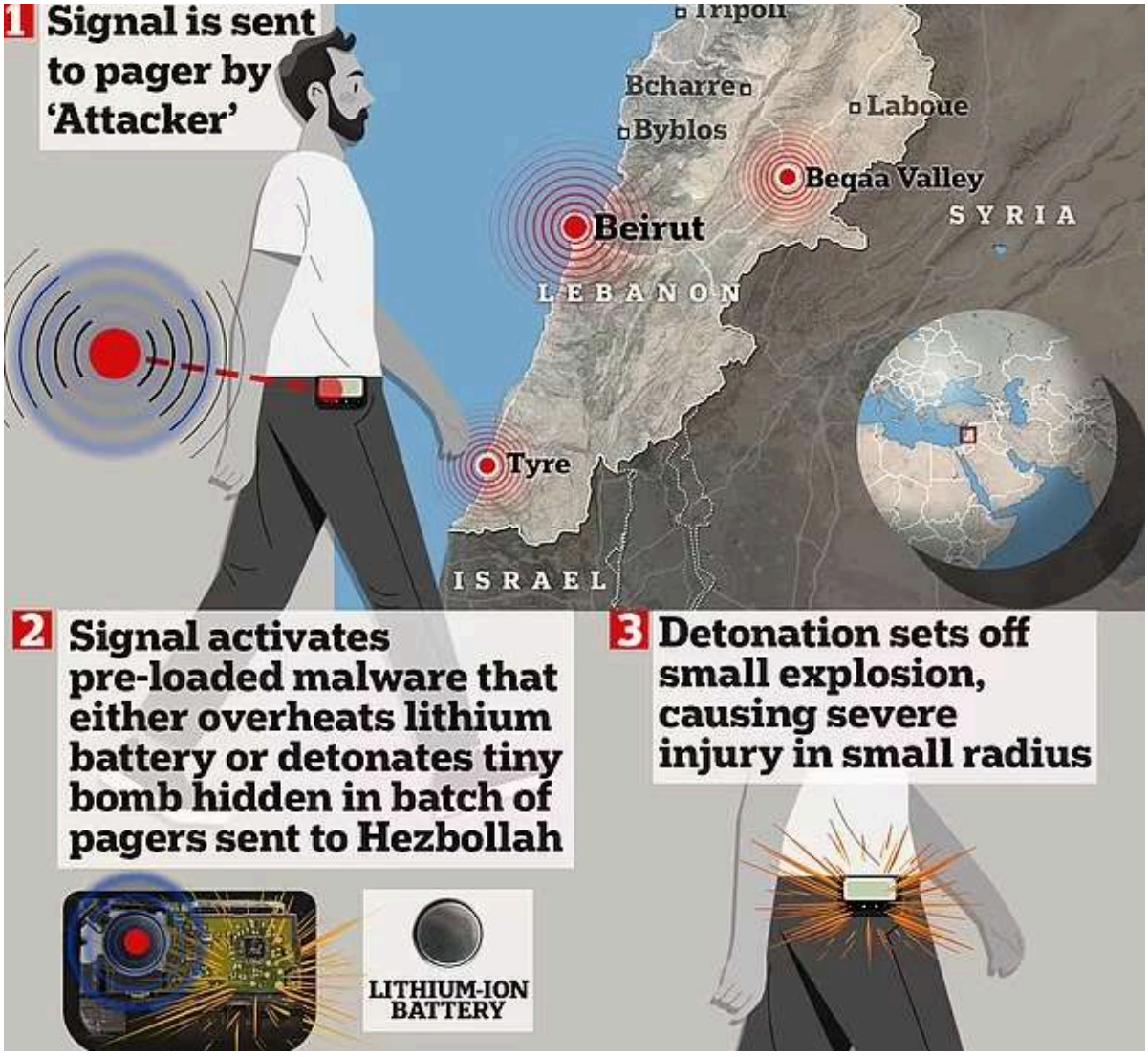
Patlamaların nasıl meydana geldiğine dair şu anda iki ana teori var.

Bunlardan biri çağrı cihazlarının patlayıcılarla dolu olduğunu ve uzaktan erişimle patlatıldığını ileri sürüyor.

ABD Ulusal Güvenlik Ajansı'nın eski istihbarat analisti David Kennedy, CNN'e yaptığı açıklamada, "İsrail'in Hizbullah'ta insan ajanlarının olması daha olası... Çağrı cihazlarına patlayıcılar yerleştirilmiş olabilir ve büyük olasılıkla yalnızca belirli bir mesaj alındığında patlayacaklardır" dedi.

İkinci temel teori ise siber güvenlik ihlalinin çağrı cihazlarının lityum iyon pillerinin aşırı ısınmasına ve patlamasına neden olduğu yönünde.

Lityum iyon piller genellikle tüketici elektroniğinde kullanılıyor ancak aşırı ısınıp alev alabiliyor, hatta bazı durumlarda şiddetli bir şekilde patlayabiliyor.



GÜNÜMÜZ VE YAPAY ZEKÂ ÇAĞI

Yapay Zekânın Siber Savaşta Kullanımı

Süreç:

Yapay zekâ, 2010'ların ortalarından itibaren makine öğrenmesi ve derin öğrenme algoritmalarının yaygınlaşmasıyla güvenlik dünyasına girdi. Başlangıçta yalnızca savunma amaçlı kullanılan sistemler (örneğin ağ trafiğinde anormallik tespiti), kısa sürede saldırgan aktörler tarafından da benimsendi.

Gelişme:

- Saldırı cephesi: YZ ile desteklenen zararlı yazılımlar, ağ üzerinde öğrenme yaparak güvenlik duvarlarını aşmayı öğrenebiliyor. Geleneksel antivirüsler yalnızca bilinen imzaları yakalarken, YZ destekli zararlı yazılımlar "davranışsal analiz" ile engelleri atlatabiliyor.
- Savunma cephesi: NATO, ABD, Çin ve İsrail gibi ülkeler, yapay zekâ tabanlı siber güvenlik sistemlerine yatırım yapıyor. NATO'nun Tallinn'deki "Siber Savunma Mükemmeliyet Merkezi" bu alanda pilot çalışmalar yürütüyor.

YZ, saldırı ile savunma arasındaki dengeyi sürekli değiştiren bir "kırmızı kraliçe dinamiği" yaratıyor. Yani saldırganlar ve savunucular aynı teknolojiyi kullanıyor, avantaj hep geçici oluyor.

Stratejik Etki:

Devletler artık YZ'yi yalnızca ekonomik büyüme aracı değil, siber caydırıcılık stratejisinin çekirdeği olarak konumlandırıyor. Bu, "AI cold war" (YZ soğuk savaşı) kavramını doğurdu.

Bilgi Toplama ve Büyük Veri

Süreç:

Dijitalleşme ile birlikte insanlar günlük yaşamlarının büyük bölümünü internette bırakıyor: sosyal medya paylaşımları, finansal işlemler, sağlık verileri, konum kayıtları… Bu "dijital ayak izleri" büyük veri analitiği ile işlenerek stratejik istihbarata dönüşüyor.

Gelişme:

- Askerî uygulama: Büyük veri, düşman hareketlerini öngörmek için kullanılıyor. Uydu görüntüleri + sosyal medya analizi = askeri birlik hareketlerinin tespiti.
- Politik uygulama: Cambridge Analytica skandalı, seçimlerde psikografik hedeflemenin mümkün olduğunu gösterdi. Bu, klasik propaganda yerine "kişiselleştirilmiş dijital manipülasyon" devrini başlattı.
- Ekonomik uygulama: Küresel şirketler, tüketici davranışlarını analiz ederek ekonomik stratejiler geliştiriyor. Bu veriler aynı zamanda devletlerin stratejik kararlarını da etkiliyor.

Büyük veri, yalnızca istihbarat teşkilatlarının değil, özel şirketlerin de elinde güçlü bir araç oldu. Ancak bu durum, devlet-özel sektör sınırını bulanıklaştırdı. Artık Google, Facebook, Alibaba gibi şirketler de "siber jeopolitik aktörler" haline geldi.

Stratejik Etki:

Bilgi üstünlüğü, nükleer silah üstünlüğünden bile daha kritik görülmeye başlandı. Çünkü veri, hem psikolojik savaşın hem de siber saldırıların yakıtı haline geldi.

Deepfake ve Algı Operasyonları

Süreç:

2017'den itibaren derin öğrenme teknolojileri ile ortaya çıkan deepfake, kısa sürede manipülasyonun en tehlikeli biçimlerinden biri haline geldi.

Gelişme:

- 2019 Hindistan seçimlerinde politikacıların sahte videoları yayıldı.
- Ukrayna–Rusya savaşında Zelenskiy'nin "teslim olma" çağrısı yaptığı sahte video dolaşıma sokuldu.
- 2020 ABD seçimlerinde deepfake tehdidi istihbarat raporlarına girdi.

Sonuç:

Deepfake, "görsel kanıt"ın güvenilirliğini ortadan kaldırdı. Savaşlarda propaganda yeni bir aşamaya geçti: Artık yalnızca gerçek dışı haberler değil, "gerçek dışı görüntüler" de güvenlik tehdidi oldu.

Stratejik Etki:

Uluslararası ilişkilerde güven krizi yarattı. Deepfake'in diplomatik krizlere yol açabilecek kapasitesi (ör. sahte bir liderin savaş ilanı videosu) devletler için varoluşsal bir risk.

Otonom Siber Saldırılar

Süreç:

YZ destekli saldırı yazılımları, kendi saldırılarını otomatik planlayabilme yeteneği kazandı.

Gelişme:

- Self-learning malware: Bulaştığı ağda sürekli öğrenerek yeni yollar buluyor.
- AI botnet'ler: Botnet'ler artık sadece komut beklemiyor, kendi "kararlarını" alabiliyor.
- Adversarial AI: Savunma sistemlerine yanıltıcı veri vererek tehditleri fark etmesini engelliyor.

Saldırılar, insan hızının ötesine geçti. Savunma mekanizmaları sürekli "geriden gelme" riski taşıyor.

Stratejik Etki:

Otonom saldırılar, gelecekte "kontrolden çıkma" ihtimali olan dijital virüsler yaratabilir. Stuxnet'in ötesinde, kendi kendini evrimleştiren zararlıların çağı başlıyor.

Günümüz ve Yapay Zekâ Çağı"nda siber savaş artık dört ayak üzerinde yürümektedir:

YZ destekli saldırılar → Daha hızlı ve güçlü tehditler.

Büyük veri analitiği → Bilginin stratejik silah haline gelmesi.

Deepfake & algı operasyonları → Gerçeğin manipülasyonu.

Otonom saldırılar → Kontrolsüzleşme riski.

Son kertede mesele, yalnızca "siber güvenlik" değil, insanlığın dijital geleceğinin nasıl şekilleneceğidir.

"Yapay Zekâ Bilgi Veren Değil, Bilgi Toplayan Sistemdir" Tezi

Süreç:

Yapay zekâ sistemleri, kullanıcıya yanıt üretirken aynı zamanda sürekli veri toplar. Bu durum, "görünmez istihbarat" sürecidir.

Gelişme:

- Kullanıcıların soruları, davranışları, tercihleri kayıt altına alınır.
- YZ, bu verileri kendi gelişimi için kullanır.
- Veri sahipleri (devletler veya şirketler), bu bilgileri analiz ederek stratejik çıkarlarına göre yönlendirme yapabilir.

Sonuç:

Kamuoyunda yapay zekâ "yardımcı" olarak görülse de aslında "gizli bir gözlemci" işlevi görür.

Stratejik Etki:

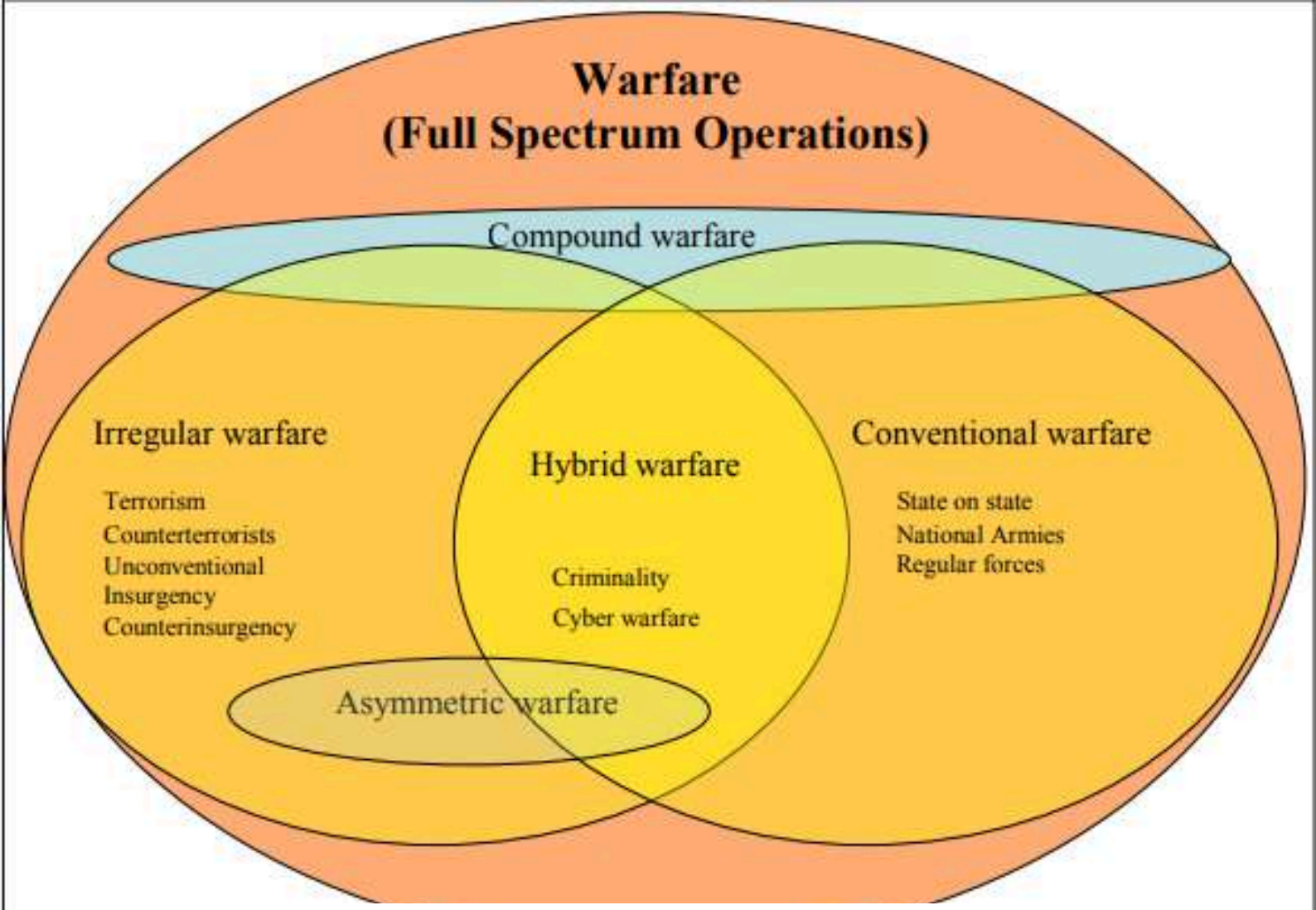
Bu tez, yapay zekânın bağımsız değil, onu besleyen aktörlerin çıkarlarına hizmet eden bir yapı olduğunu gösterir. Bu da dijital çağda güvenlik-özgürlük ikilemini keskinleştirir.

Günümüz ve Yapay Zekâ Çağı

1. Yapay Zekânın Siber Savaşta Kullanımı
   - Yapay zekâ destekli saldırıların klasik saldırılardan farkı nedir?
   - Saldırıların otomatikleşmesi ve tahmin yeteneği.
   - Savunmada AI tabanlı sistemlerin rolü.
2. Bilgi Toplama ve Büyük Veri
   - Devletlerin ve özel şirketlerin veri madenciliği.
   - Büyük veri → ulusal güvenlik stratejilerinde nasıl kullanılıyor?
   - Siber savaşta "önleyici istihbarat" rolü.
3. Deepfake ve Algı Operasyonları
   - Seçimlere müdahale örnekleri.
   - Kamuoyu manipülasyonu → "gerçeğin çarpıtılması" savaş yöntemi.
   - Deepfake'in diplomasi ve medya üzerindeki riski.
4. Otonom Siber Saldırılar
   - İnsan kontrolü olmadan hareket eden "self-learning malware" örnekleri.
   - AI ile güçlenen botnet'ler.
   - Savunma sistemlerinin kapasitesini aşma riski.
5. "Yapay Zekâ Bilgi Veren Değil, Bilgi Toplayan Sistemdir" Tezi
   - Yapay zekânın görünürde "danışman" ama gerçekte "istihbarat toplayıcı" işlevi.
   - Dijital çağda insan-makine güven ilişkisi.
   - AI'nin tarafsız değil, veri sahiplerine bağımlı bir güç unsuru olması.

Gelecek Senaryoları

1. Siber Ordular ve Hibrit Savaş Doktrinleri
   - NATO, Çin, Rusya'nın siber orduları.
   - Fiziksel + dijital birleşik saldırı doktrinleri.
2. Enerji Altyapıları ve Kritik Sistemlerin Hedef Olması
   - Elektrik şebekeleri, su dağıtımı, nükleer santraller.
   - Ukrayna enerji şebekesi saldırısı (2015) örneği.
3. Nesnelerin İnterneti (IoT) ve Akıllı Şehirlerin Riskleri
   - Akıllı trafik sistemleri, sağlık cihazları, otonom araçlar.
   - "Bir şehrin dijitalden çökertilmesi" senaryosu.
4. Küresel Hukuk: Siber Savaşta Uluslararası Meşruiyet
   - Tallinn Manual (2013, 2017) → Siber savaşın hukuki çerçevesi.
   - BM, NATO ve ICJ tartışmaları.
   - "Saldırı" ile "casusluk" arasındaki gri alan.
5. İnsanlığın Geleceği: Dijital Güven mi, Dijital Kıyamet mi?
   - Dijital çağda güvenlik-özgürlük dengesi.
   - Yapay zekâ ve siber savaşın kontrolsüzleşmesi halinde küresel risk.
   - Distopik senaryolar vs. güvenlik odaklı umut verici senaryolar.



SİBER ORDULAR VE HİBRİT SAVAŞ DOKTRİNLERİ

Soğuk Savaş sonrası dönemde birçok devlet, yalnızca kara–hava–deniz kuvvetlerinden değil, "siber ordulardan" da söz etmeye başladı. ABD, Rusya, Çin, Kuzey Kore ve İsrail bu alanda öncü konumda.

- Rusya'nın "Gerasimov Doktrini", hibrit savaşın merkezine siber saldırıları yerleştirdi.
- Çin, "Büyük Siber Duvar" politikasıyla hem içeriyi kontrol ediyor hem de dışarıya saldırı kabiliyeti geliştiriyor.
- NATO 2016'da siber saldırıları "beşinci operasyon alanı" ilan etti.

Siber ordular, artık konvansiyonel orduların tamamlayıcısı değil; savaş stratejilerinin merkez aktörü. Hibrit savaşlar, aynı anda hem tank hem de zararlı yazılım kullanıyor.

Stratejik Etki:

Devletler arası caydırıcılık artık nükleer değil; siber kapasite ile ölçülüyor.

Enerji Altyapıları ve Kritik Sistemlerin Hedef Olması

Süreç:

Enerji, modern toplumların can damarıdır. Elektrik şebekeleri, nükleer santraller, su arıtma tesisleri en kritik hedefler arasında.

Gelişme:

- 2015'te Ukrayna elektrik şebekesi siber saldırıyla çökertildi. 230 bin kişi elektriksiz kaldı.
- ABD'de Colonial Pipeline saldırısı (2021) yakıt dağıtımını felç etti.
- İran, İsrail, Suudi Arabistan gibi ülkelerde enerji altyapıları sürekli saldırı tehdidi altında.

Sonuç:

Enerji altyapılarına saldırılar, klasik askeri saldırılardan daha düşük maliyetle çok daha büyük toplumsal kaos yaratabiliyor.

Stratejik Etki:

Enerji şebekeleri artık "ulusal güvenlik" meselesi değil; küresel güvenlik riski haline geldi.

Nesnelerin İnterneti (IoT) ve Akıllı Şehirlerin Riskleri

Süreç:

2030'a kadar 30 milyardan fazla IoT cihazının kullanılacağı öngörülüyor. Akıllı şehirler, trafik ışıklarından hastane sistemlerine kadar dijitalleşiyor.

Gelişme:

- Mirai botnet (2016) IoT cihazlarının nasıl saldırıya dönüştürülebileceğini gösterdi.
- Akıllı şehirlerde tek bir saldırı, sağlık, ulaşım ve güvenlik sistemlerini aynı anda çökertme potansiyeline sahip.
- Otonom araçların hacklenmesi, trafik kaosu ve can kaybı riski barındırıyor.

Sonuç:

Akıllı şehirler, vatandaşlara konfor sağlarken aynı zamanda "siber savaşın yeni cepheleri" haline geliyor.

Stratejik Etki:

Gelecekte şehirler, düşman saldırısı olmadan "dijitalden çökertilebilecek" hale gelecek.

Stratejik Etki:

Devletler arası caydırıcılık artık nükleer değil; siber kapasite ile ölçülüyor.

Küresel Hukuk: Siber Savaşta Uluslararası Meşruiyet

Süreç:

Geleneksel savaş hukuku (Cenevre Konvansiyonu vb.) fiziksel saldırılar üzerine inşa edildi. Siber saldırılar bu çerçeveye sığmıyor.

Gelişme:

- Tallinn Manual (2013, 2017) → NATO destekli uzmanlar, siber savaşın uluslararası hukukla ilişkisini tanımlamaya çalıştı.
- BM'de "Open-Ended Working Group" ve "Group of Governmental Experts" girişimleri.
- Ancak devletler, özellikle ABD, Rusya ve Çin, bağlayıcı hukuk normlarına yanaşmıyor.

Sonuç:

Siber savaş hâlâ gri alanda. Casusluk mu, savaş fiili mi? Bu ayrım belirsiz.

Stratejik Etki:

Hukuki boşluk, saldırgan devletlere avantaj sağlıyor. Siber saldırılar, "inkâr edilebilir" olduğu için cezasız kalıyor.

İnsanlığın Geleceği: Dijital Güven mi, Dijital Kıyamet mi?

Süreç:

Yapay zekâ, büyük veri, otonom saldırılar, IoT → tümü insanlığa ya "dijital güven çağı" ya da "dijital kıyamet" vaat ediyor.

Gelişme:

- Umut veren senaryo: Yapay zekâ, saldırıları daha başlamadan tespit edebilir; küresel işbirliği siber saldırıları caydırabilir.
- Kâbus senaryo: Kontrolden çıkan otonom zararlılar, kritik altyapıların çökmesi, deepfake ile diplomatik krizler, toplumların birbirine düşmesi.

Sonuç:

İnsanlık, kritik bir yol ayrımında. Dijital araçlar barış için kullanılabileceği gibi, uygarlığın çöküşünü hızlandırabilir.

Stratejik Etki:

Geleceğin en önemli sorusu şudur: "Dijital çağda güvenlik mi, özgürlük mü öncelik kazanacak?" Yanıtı, insanlığın kolektif tercihleri belirleyecek.

SİBER ORDULAR → YENİ CAYDIRICILIK GÜCÜ.

IOT VE AKILLI ŞEHİRLER → GELECEĞİN SİBER SAVAŞ ALANLARI.

ENERJİ ALTYAPILARI → EN KIRILGAN HEDEF.

ULUSLARARASI HUKUK → HÂLÂ YETERSİZ.

İNSANLIK → DİJİTAL GÜVENLİK İLE DİJİTAL KAOS ARASINDA.

Kodun Gölgesinde İnsanlığın İmtihanı

İnsanlık, kılıçtan koda uzanan serüveninde bugün belki de en kritik eşiğe dayanmış bulunuyor. Tarih boyunca savaş, fiziksel alanların kontrolü için yürütüldü: topraklar, kaleler, enerji kaynakları… Ancak 21. yüzyılda savaşın görünmez bir cepheye taşındığını görüyoruz. Artık mücadele, verinin yönetimi, algının şekillendirilmesi ve bilginin araçsallaştırılması üzerine kuruludur. Siber savaş, yalnızca sistemleri değil, hakikatin kendisini hedef almaktadır.

Teknolojinin İkili Yüzü: Kurtarıcı mı, Tehdit mi?

Teknoloji, insanlık için hem en büyük fırsatları hem de en derin tehlikeleri aynı anda barındırıyor. Bir yandan yapay zekâ, sağlık hizmetlerinden iklim krizinin öngörülmesine kadar sayısız alanda yaşamı kolaylaştırıyor. Büyük veri analitiği, salgın hastalıkların önceden tespitinde, enerji kullanımında verimlilik yaratmada büyük olanaklar sağlıyor. Ancak aynı araçlar, algı operasyonları, dezenformasyon, gözetim kapitalizmi ve devletlerin kitlesel manipülasyon stratejileri için de kullanılıyor. Böylece teknolojinin kurtarıcı potansiyeli, çoğu zaman insanlığın kendi aleyhine işleyen bir "güç silahı"na dönüşüyor.

Uluslararası Hukukun İşlevsizliği

Siber savaş, mevcut uluslararası hukuk mekanizmalarının yetersizliğini de çıplak biçimde ortaya koydu. Cenevre Konvansiyonları, fiziksel silahlara göre inşa edilmişti; oysa siber saldırılar ne tankla ne de tüfekle yapılır. Tallinn Manual gibi girişimler, siber savaşın hukukunu tanımlamaya çalışsa da, devletlerin bağlayıcı düzenlemelere yanaşmaması nedeniyle "öneri" düzeyinde kaldı. Bugün hiçbir devlet, kendisine atfedilen bir siber saldırıyı kabul etmiyor; çünkü "inkâr edilebilirlik" siber savaşın temel stratejilerinden biri haline geldi. Bu da saldırgan aktörlere fiilen dokunulmazlık sağlıyor. Uluslararası hukuk, zaten zayıf olan işlevini bu alanda tamamen yitirmiş durumda.

Bilgiye Erişim mi, Algının Hakimiyeti mi?

Dijital çağ, görünürde "bilgiye sınırsız erişim" vaadiyle başladı. Fakat bugün geldiğimiz noktada bilginin bolluğu, hakikatin yitimiyle sonuçlandı. Büyük veri çağında "çok bilgi"nin olması, aslında "gerçeğe ulaşmayı" kolaylaştırmıyor. Tam tersine, bilgi fazlalığı "yetersizlik algısı" yaratıyor; insanlar hangisinin doğru olduğunu ayırt edemediği için manipülasyona açık hale geliyor.

Bunun en çarpıcı örneği algı yönetimi. Deepfake teknolojileri, sahte haberler, bot orduları… Hepsi tek bir şeyi hedefliyor: Gerçeği önemsizleştirmek. Artık mesele, "hakikatin ne olduğu" değil; kitlelerin neye inandırıldığıdır. Bu, siber savaşın en tehlikeli boyutudur: Hakikatin çarpıtılması ve gerçeğin önemsizleşmesi.

Büyük Veri, Yapay Zekâ ve İnsan Vicdanı

Büyük veri ve yapay zekâ, insanlık tarihinin en güçlü kontrol araçlarını doğurdu. Ancak bu araçlar, ahlaki denetimden yoksun biçimde büyümekte. Bir yandan devletler, vatandaşlarının her adımını takip edebilecek gözetim sistemleri kuruyor; diğer yandan özel şirketler, kullanıcıların davranışlarını ticari kâr için işliyor. Bu denklemde insan vicdanı neredeyse tamamen dışarıda bırakılmış durumda.

Sorulması gereken kritik soru şudur: Veri ve yapay zekâ, insanın özgürlüğünü mü büyütüyor, yoksa insanı bir "dijital nesneye" mi indiriyor?

Bugün geldiğimiz noktada yanıt daha çok ikinci ihtimal lehine şekilleniyor. İnsan, kendi ürettiği verinin kölesine dönüşüyor; yapay zekâ, "bilgi veren bir yardımcı" değil, "bilgi toplayan bir efendi" halini alıyor.

Riskler mi Önemli?

Küresel tabloya bakıldığında, siber savaş çağının insanlığa sunduğu fırsatlar kadar riskler de var. Ancak kritik olan, hangi tarafın daha ağır bastığıdır.

- Fırsatlar: Küresel işbirliği, dijitalleşmenin barış için kullanılması, ortak güvenlik mekanizmalarının kurulması.
- Riskler: Kritik altyapıların çökertilmesi, demokrasilerin manipüle edilmesi, bireylerin sürekli gözetim altında yaşaması.

Bugün için risklerin fırsatları gölgede bıraktığını görmek zor değil. Çünkü uluslararası hukuk işlevsiz, devletler işbirliğine kapalı, özel sektör ise sorumluluktan çok kârı önceliyor.

İnsanlığın İmtihanı

Siber savaş, yalnızca kodların savaşı değildir. Aynı zamanda ahlakın, vicdanın ve insanlık değerlerinin savaşıdır. Bir yanda sınırsız veri ve güçlü algoritmalar; diğer yanda kırılgan insan toplulukları… Bu asimetri, tarihte görülmemiş ölçüde büyük.

Bugün gelinen nokta, insanlığın kendi icat ettiği teknolojiyi denetleyip denetleyemeyeceği sorusuna indirgeniyor. Eğer teknoloji vicdanla, etikle ve uluslararası hukukla birleşmezse, dijital çağ insanlık için bir güvenlik devriminden çok bir felaketin habercisi olabilir.

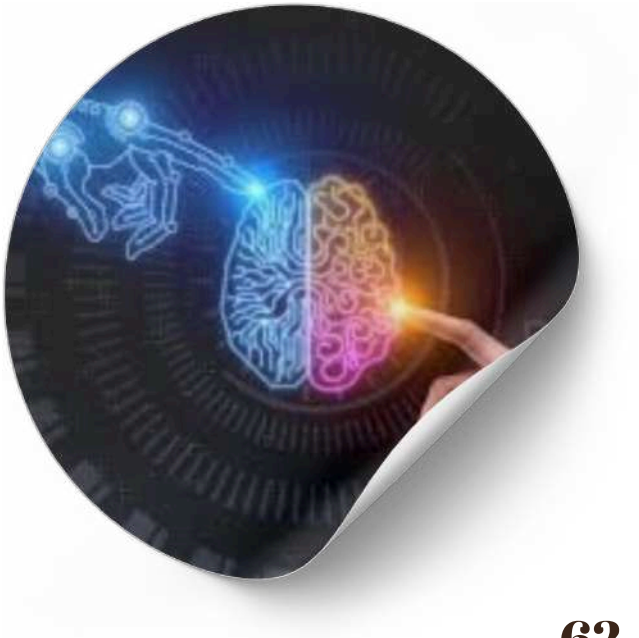
Büyük Veri, Yapay Zekâ ve İnsan Vicdanı

Büyük veri ve yapay zekâ, insanlık tarihinin en güçlü kontrol araçlarını doğurdu. Ancak bu araçlar, ahlaki denetimden yoksun biçimde büyümekte. Bir yandan devletler, vatandaşlarının her adımını takip edebilecek gözetim sistemleri kuruyor; diğer yandan özel şirketler, kullanıcıların davranışlarını ticari kâr için işliyor. Bu denklemde insan vicdanı neredeyse tamamen dışarıda bırakılmış durumda.

Sorulması gereken kritik soru şudur: Veri ve yapay zekâ, insanın özgürlüğünü mü büyütüyor, yoksa insanı bir "dijital nesneye" mi indiriyor?

Bugün geldiğimiz noktada yanıt daha çok ikinci ihtimal lehine şekilleniyor. İnsan, kendi ürettiği verinin kölesine dönüşüyor; yapay zekâ, "bilgi veren bir yardımcı" değil, "bilgi toplayan bir efendi" halini alıyor.

Günümüz Dünyasının Hali: Fırsatlar mı,



Siber savaşın doğuşu, bize tarihin en net dersini hatırlatıyor: Güç, her zaman bilgiye sahip olanın elinde olmuştur. Fakat günümüzde asıl sorun, "bilginin doğruluğu" değil, "algının gücü"dür. Eğer toplumlar gerçeği değil algıyı kutsamaya devam ederse; uluslararası hukuk da işlevsizliğini sürdürürse; büyük veri ve yapay zekâ da vicdandan kopuk şekilde büyürse; insanlık dijital kıyametin eşiğinde olacaktır.

Bugün önümüzde iki ihtimal var:

- Ya teknolojiyi ahlaki ilkelerle yönetip dijital güven çağını başlatacağız,
- Ya da kontrolsüz güçlerin elinde kendi geleceğimizi "sanal bir savaş meydanında" kaybedeceğiz.

Ve insanlık, bu tercihi erteleyemez. Çünkü siber savaş, artık yalnızca bilgisayarlarımızda değil; zihinlerimizde, inançlarımızda ve vicdanlarımızda çoktan başlamış durumdadır.

SİBER SALDIRI NEDİR?

TANIM

Bilgisayar sistemlerini, ağları veya cihazları hedef alan kötü niyetü faaliyet

TÜRLER

Phishing

Kötü Amaçlı Yazılım

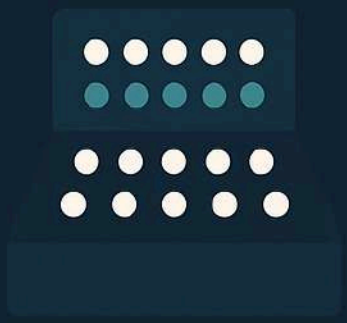
DDoS

AKTÖRLER

Bireyler

Devletler

MODERN ŞİFRELEME ÇAĞI



I. TELGRAF, ŞİFRELER VE ENIGMA MAKİNESİ

ALAN TURING
VE KODLARIN ÇÖZÜLÜŞÜ

II. SOĞUK SAVAŞ YILLARI

Elektronik Casusluk
ve ECHELON

II. Dünya Savaşi (1939–1945)

III. DİJITAL ÇAĞIN DOĞUŞU

İnternetin Ortaya Çıkışı
ve İlk Solucanlar

İLK BÜYÜK VAKA: MORRIS WORM (1988)

ARKA PLAN

Binlerce bilgisayara bulaşan kendini çoğaltan bir program

İnfeksiyon Yayılması

Zayıflıklardan Yararlanma

Hizmetlerin Aksaması

ETKİ

Önemli vavaşlamalara ve mali zararlara yol açtı

DEVLET ÖLÇEĞİNDE İLK KRİZ: ESTONYA (2007)

Nisan-Mayis 2007'de Estonya'nın devlet kurumları ve altyapısına büyük bir siber saldirı düzenlendi.

KAPSAM

- Kamu kurumları
- Çevrimiçi hizmetler
- Finansal kuruluşlar

BAZI İNTERNET SİTELERİ HAFTALARCA KAPALI KALDI

- Devlet siteleri
- Medya siteleri
- Bankalar

SONUÇLAR

- Devlet hizmetileri sekteye uğradı
- Ekonomik zararlar meydana geldi
- NATO ve AB bu tür saldırılara karşı önlemler geliştirdi

KODUN SILAHA DÖNÜŞMESI: STUXNET (2010)

STUXNET NEDİR?

Özellikke endüstriyel sistemleri hedef almak icin geiiştirilen ve kodu daha önce görülmemiş şekidde manipüle edilen bir kötü amaçli yazilimdi

ZARARLI YAZILIMIN TÜRÜ

Bilgisayar virüsü ve bilgisayar solucani birleşimi şeklinde, endustriyel kontrol sistemlerini bozacak şekilde programlandı

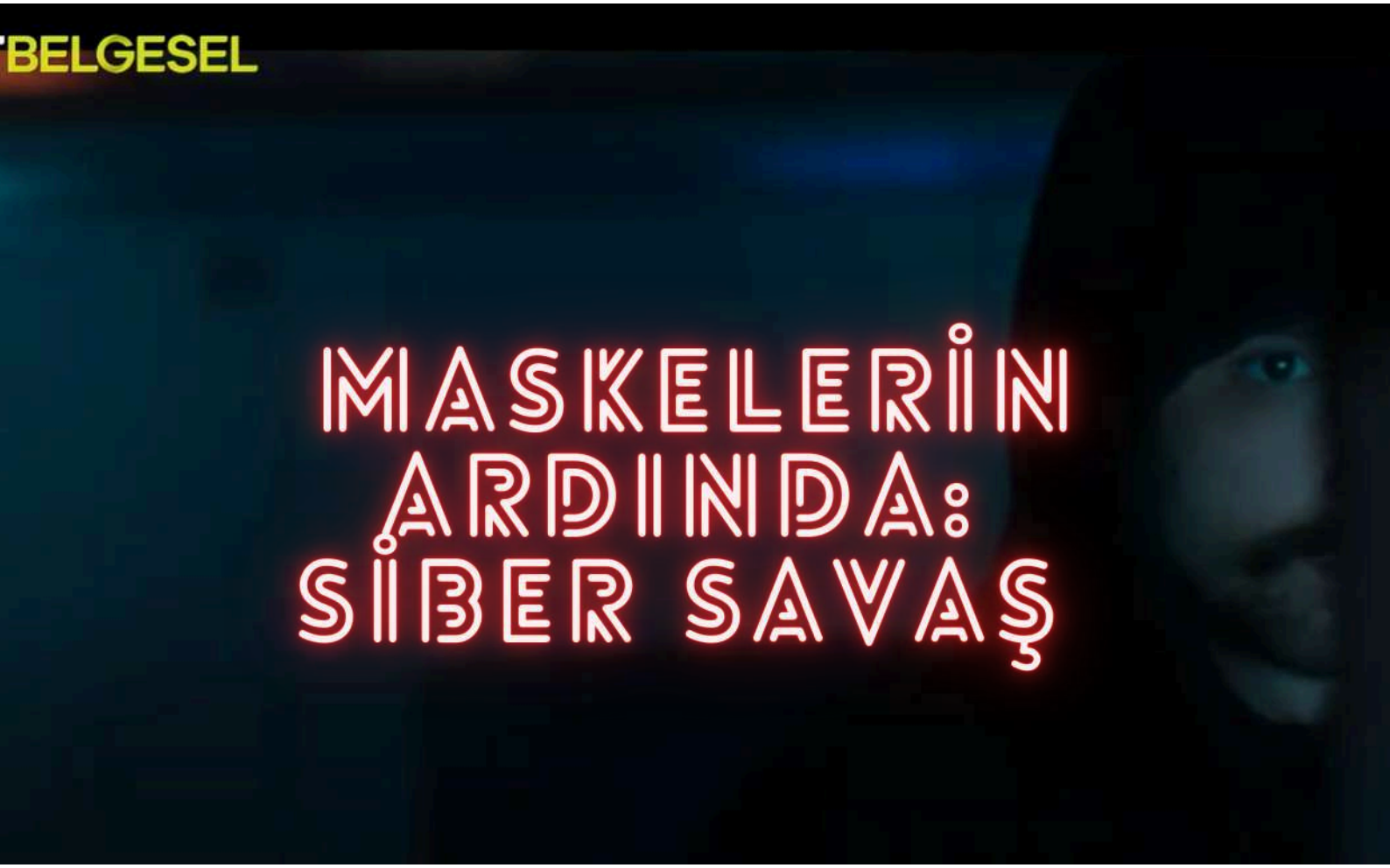
BELİRTİLER VE ETKİLER

Hedef alinan santrifüjler devre dişi kaldi ya da fiziksel hasara üğradi; enfeksiyon aylardir fark edilmedi

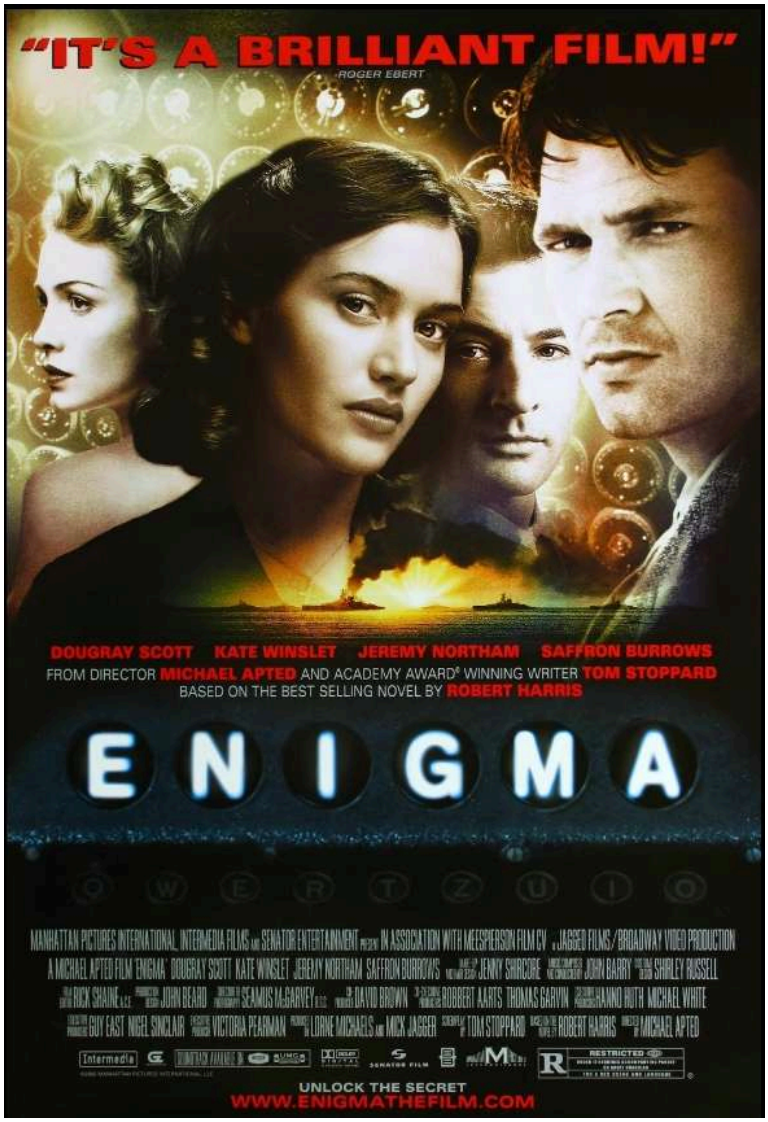
İZLENEN ENFEKSIYONLAR

Stuxnet, en fazla Iran'da, ardından Endonezya ve Hindistan'da tespit edildi

"İster politikayla ilgilenin ister iş dünyasıyla, ister orduyla ya da isterseniz medyayla –ya da sadece sıradan bir vatandaş olun– bu kitabın okunması gerekir. "
– Eric Schmidt, Google CEO'su
"Siber dünya üzerine yazılmış en okunabilir ve anlaşılır kitap."
– Amiral (E) James Stavridis, ABD Deniz Kuvvetleri ve NATO Müttefik Kuvvetler Eski Komutanı
"Siber güvenlik hakkında bilmek istediğiniz her şey açık ve zeki bir tarzda mükemmelce sunulmuş."
– Walter Isaacson, Steve Jobs'un Yazarı
"Bu kitaba aşık oldum. Müthiş."



Ülkeler arası dijital saldırılara, güvenlik açıklarına ve hacker savaşlarına tanık olmaya hazır mısın? Bugün her insan bir siber saldırıyla karşı karşıya gelebilir. Kullandığımız web uygulamaları, servisler, donanımlar hatta evimizdeki akıllı eşyalar hackerlar için birer hedef. Bu saldırılar bazen istihbarat odaklı olurken bazen de finansal kazanç amaçlı olabiliyor. Siber savaş, kuralları olmayan yepyeni bir savaş ve bu savaş internetin olduğu her yerde. Siber dünyada yaşananları ve ileride nelerin yaşanabileceğini ele alan "Maskelerin Ardında: Siber Savaş", TRT Belgesel'de!



2. Dünya Savaşı sırasında Nazi Almanya'sının Enigma makinesiyle şifreledikleri ve Rus&İngiliz ittifakının bir türlü dekode edemediği mesajlar, savaş alanında Almanlara büyük bir üstünlük sağlamaktadır. Bunun önüne geçmek isteyen İngilizler, Amerika ve İngiltere'nin en iyi şifreleme uzmanlarından ve matematik bilimcilerinden oluşan bir ekip kurarlar. Bu ekibin bir üyesi olan İngiliz Matematikçi Alan Turing, kendine has çalışma stiliyle başlarda hem ekibinden, hem de hükümetten tepki görür. Ancak bir ekip üyesinin de desteğiyle Alan Turing çalışmaya devam eder, ekip Enigma'nın şifresini çözer. Bu keşif, İkinci Dünya Savaşı'nın kaderini değiştirecek ve Almanların mutlak yenilgisiyle sonuçlanacak olan sürece girilmesini sağlayacaktır.

KAYNAKÇA

- *Aid, M. M. (2009). The secret sentry: The untold history of the National Security Agency. Bloomsbury Press.*
- *Al Jazeera. (2024, September 17). Israel's war on Gaza live: 38 killed as Israel risks becoming pariah. Retrieved from https://www.aljazeera.com/news/liveblog/2024/9/17/israels-war-on-gaza-live-38-killed-as-israel-risks-becoming-pariah*
- *Antonakakis, M., et al. (2017). Understanding the Mirai Botnet. USENIX Security Symposium, 1093–1110.*
- *Associated Press. (2024, September 17). Dozens of Hezbollah members wounded in Lebanon when pagers exploded. Retrieved from https://apnews.com/article/lebanon-hezbollah-israel-exploding-pagers-8893a09816410959b6fe94aec124461b*
- *Associated Press. (2024, September 18). Survivors of Israel's pager attack on Hezbollah struggle to recover. Retrieved from https://apnews.com/article/b63cb3639dd9da855ec6c704bc8424df*
- *Bamford, J. (2002). Body of secrets: Anatomy of the ultra-secret National Security Agency. Anchor Books.*
- *Barron's. (2024, September 18). Taiwan's Gold Apollo says Hezbollah pagers made by Hungary partner. Retrieved from https://www.barrons.com/news/taiwan-s-gold-apollo-says-hezbollah-pagers-made-by-hungary-partner-ba2ff7c7*
- *BBC. (2024, September 18). Lebanon Hezbollah pagers explosions. Retrieved from https://www.bbc.com/news/articles/cd7xnelypepo*
- *Bradbury, D. (2013). The Mt. Gox Saga. Computer Fraud & Security, 2013(11), 5–8.*
- *Brundage, M., et al. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. arXiv preprint arXiv:1802.07228.*
- *Calce, M., & Silverman, C. (2008). Mafiaboy: How I Cracked the Internet and Why It's Still Broken. Viking Canada.*
- *Campbell, D. (2016). Signals intelligence in the Cold War and beyond. Routledge.*
- *Chesney, R., & Citron, D. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review, 107(6), 1753–1819.*
- *Chertoff, M., & Simon, T. (2020). The Impact of the Dark Web on Internet Governance and Cyber Security. Council on Foreign Relations.*
- *Cisco. (n.d.). Common cyberattacks: How cyber attacks work. Retrieved from https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html*
- *Clarke, R. A., & Knake, R. K. (2010). Cyber War: The Next Threat to National Security and What to Do About It. Ecco.*
- *Copeland, B. J. (2004). Alan Turing's Automatic Computing Engine. Oxford University Press.*
- *Crawford, K. (2021). Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. Yale University Press.*
- *Daily Mail. (2024, September 18). Hundreds of Hezbollah fighters wounded as pagers explode. Retrieved from https://www.dailymail.co.uk/news/article-13860239/Hundreds-Hezbollah-fighters-wounded-PAGERS-explode.html*
- *Day, D. A., Logsdon, J. M., & Latell, B. (1998). Eye in the sky: The story of the Corona spy satellites. Smithsonian Institution Press.*
- *Denning, D. E. (2001). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. RAND Corporation.*
- *Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644–654.*
- *DW. (2024, September 18). Lübnan'daki patlamalar: Çağrı cihazları Macaristan'da mı üretildi? Retrieved from https://www.dw.com/tr/l%C3%BCbnandaki-patlamalar-%C3%A7a%C4%9Fr%C4%B1-cihazlar%C4%B1-macaristanda-mt%C4%B1-%C3%BCretildi/a-70246321*

- *Economist. (2010, September 30). The meaning of Stuxnet. Retrieved from https://www.economist.com/leaders/2010/09/30/the-meaning-of-stuxnet*
- *Economist. (2024, September 17). A pager bomb attack causes disarray for Hizbullah. Retrieved from https://www.economist.com/middle-east-and-africa/2024/09/17/a-pager-bomb-attack-causes-disarray-for-hizbullah*
- *Elfanet. (2021). Stuxnet nedir? Retrieved from https://elfanet.com.tr/tr/main/article/stuxnet-nedir/105*
- *Europol. (2017). WannaCry ransomware outbreak: Situation Report. Europol.*
- *Euronews. (2024, September 18). Dozens of Hezbollah members wounded in Lebanon by exploding pagers. Retrieved from https://www.euronews.com/2024/09/18/dozens-of-hezbollah-members-wounded-in-lebanon-by-exploding-pagers*
- *FireEye. (2015). APT Attacks in the Hospitality Industry. FireEye Threat Intelligence Report.*
- *Fortinet. (n.d.). Types of cyberattacks. Retrieved from https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks*
- *Greenberg, A. (2016). How an Anonymous Hacker Stole $81 Million From the Bangladesh Bank. Wired Magazine.*
- *Greenberg, A. (2018). Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. Doubleday.*
- *Hafner, K., & Lyon, M. (1996). Where wizards stay up late: The origins of the Internet. Simon & Schuster.*
- *Healey, J. (2013). A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Cyber Conflict Studies Association.*
- *Hodges, A. (2014). Alan Turing: The Enigma. Princeton University Press.*
- *IBM. (n.d.). Cyber attack: Definition and types. Retrieved from https://www.ibm.com/topics/cyber-attack*
- *Inquiries Journal. (2010). Stuxnet: The world's first cyber boomerang. Retrieved from http://www.inquiriesjournal.com/articles/1343/stuxnet-the-worlds-first-cyber-boomerang*
- *Jeffrey, R. (2015). Blackbird: The history of the SR-71. Zenith Press.*
- *Kahn, D. (1996). The codebreakers: The comprehensive history of secret communication from ancient times to the Internet. Scribner.*
- *Kaspersky. (2020). Five most notorious cyberattacks. Retrieved from https://www.kaspersky.com.tr/blog/five-most-notorious-cyberattacks/5394/*
- *Kaspersky Lab. (2014). Darkhotel: A Sophisticated Targeted Attack Campaign. Kaspersky Security Report.*
- *Kozaczuk, W. (1984). Enigma: How the German machine cipher was broken. University Publications of America.*
- *Le Monde. (2024, September 18). Hezbollah pager blasts most likely caused by inserted explosive. Retrieved from https://www.lemonde.fr/en/pixels/article/2024/09/18/hezbollah-pager-blasts-most-likely-caused-by-inserted-explosive_6726497_13.html*
- *Levy, S. (2001). Crypto: How the code rebels beat the government—saving privacy in the digital age. Penguin.*
- *Milevski, L. (2012). Stuxnet and the future of cyber war. Joint Force Quarterly, 63(4), 64–69.*
- *NATO CCDCOE. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.*
- *News18. (2024, September 17). Lebanon Hezbollah pagers explosions: Militants killed in deadly blasts. Retrieved from https://www.news18.com/world/lebanon-hezbollah-pagers-explosions-militants-deadly-blasts-israel-iran-latest-news-9054469.html*

- *News.com.au. (2024). 'Truman Show': Mossad agents reveal new details of 10-year exploding pager plot. Retrieved from https://www.news.com.au/technology/innovation/military/truman-show-mossad-agents-reveal-new-details-of-10year-exploding-walkietalkie-and-pager-plot/news-story/214f03f76b39b30079698e03a6feb68a*
- *Nye, J. S. (2017). Deterrence and Dissuasion in Cyberspace. International Security, 41(3), 44–71.*
- *Pedlow, G. W., & Welzenbach, D. E. (1992). The Central Intelligence Agency and overhead reconnaissance: The U-2 and OXCART programs. CIA History Staff.*
- *Poulsen, K. (2001). Teen Hacker Mafiaboy Sentenced. SecurityFocus.*
- *Reuters. (2024, September 17). Dozens of Hezbollah members wounded in Lebanon when pagers exploded. Retrieved from https://www.reuters.com/world/middle-east/dozens-hezbollah-members-wounded-lebanon-when-pagers-exploded-sources-witnesses-2024-09-17/*
- *Reuters. (2024, November 11). Netanyahu approved pager attacks against Hezbollah, spokesman says. Retrieved from https://www.reuters.com/world/middle-east/netanyahu-approved-pager-attacks-against-hezbollah-spokesman-says-2024-11-11/*
- *Richelson, J. T. (1999). America's secret eyes in space: The U.S. Keyhole spy satellite program. Westview Press.*
- *Richelson, J. T. (2001). The U.S. intelligence community. Routledge.*
- *Rid, T. (2013). Cyber War Will Not Take Place. Oxford University Press.*
- *Schneier, B. (2015). Applied cryptography: Protocols, algorithms, and source code in C. Wiley.*
- *Singh, S. (1999). The code book: The science of secrecy from ancient Egypt to quantum cryptography. Anchor.*
- *Simplilearn. (n.d.). Types of cyber attacks. Retrieved from https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks*
- *Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.*
- *Siber Bülten. (2020). Stuxnet ve uluslararası hukuk: Bir siber saldırının anatomisi. Retrieved from https://siberbulten.com/makale-analiz/stuxnet-ve-uluslararasi-hukuk-bir-siber-saldirinin-anatomisi/*
- *STM. (2020). Dijital devrimin ikinci dalgası. ThinkTech Raporu. Retrieved from https://thinktech.stm.com.tr/uploads/docs/1608908628_stm-dijital-devrimin-ikinci-dalgasi-.pdf*
- *Stoll, C. (1989). The cuckoo's egg: Tracking a spy through the maze of computer espionage. Doubleday.*
- *Threatmap. (n.d.). Cyber attack world map. Check Point Software Technologies. Retrieved from https://threatmap.checkpoint.com/*
- *Trellix. (n.d.). What is Stuxnet? Retrieved from https://www.trellix.com/security-awareness/ransomware/what-is-stuxnet/*
- *Welchman, G. (1982). The Hut Six story: Breaking the Enigma codes. McGraw-Hill.*
- *Yahoo News. (2024, September 16). Revealed: How a secret Dutch mole aided the US-Israeli Stuxnet cyber attack on Iran. Retrieved from https://www.yahoo.com/news/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html*
- *Zetter, K. (2014). Countdown to zero day: Stuxnet and the launch of the world's first digital weapon. Crown.*
- *Zuboff, S. (2019). The Age of Surveillance Capitalism. PublicAffairs.*

DÜŞÜNCE

DÜNYA'DAN BİR HABER