SİBER GÜVENLİK
VE
SİBER SAVAŞLAR

Bilgi Toplumu Olabilmek

Fiziksel
Değişim

Kültürel
Değişim

Siber Dünya

Günümüzde hayat her yönüyle sayısallaşmamış olsa da süreçte varılacak nokta **istisnasız her şeyin sayısallaştığı, uluslar arası protokollerin ve standartların hayatın tüm evrelerine nüfuz ettiği SİBER DÜNYA** olacaktır.

Kültürel Değişim

- **SANAL DÜNYADA BİLGİ MİKTARI**
- Bilgi ve iletişim teknolojileri hızla gelişmiş ve tüm dünya çapında yayılmıştır. 2.27 milyar internet kullanıcısı – Günlük 247 milyar e-posta

- Tüm iş ve işlemler elektronik ortama aktarılmış/aktarılmaktadır
  - ✓ 240 milyon internet adresi,
  - ✓ 19.2 milyar internet sayfası,
  - ✓ 1.6 milyar resim,
  - ✓ 50 milyon ses-görüntü dosyası

- Kişisel, kurumsal ve ulusal açıdan hayati önem taşıyan pek çok bilgi elektronik ortamda ……

Yeni İnternet Kullanım Trendleri: Sosyal Şebekeleşme

2010 yılı, OECD ülkeleri

- e-posta gönderme ya da telefon açma:
  yetişkin kullanıcıların % 67'si

- mal ve hizmetlerini internet yoluyla sipariş edilmesi:
  yetişkin kullanıcıların % 35'i

- internet bankacılığı:
  yetişkin kullanıcıların % 40'u

- sipariş verme:
  OECD ortalamasına göre çalışan sayısı 10 ya da daha fazla olan işletmelerin % 43'ü

- Satış Yapma:
  Bahsi geçen işletmelerin %27 si

Yeni İnternet Kullanım Trendleri: Sosyal Şebekeleşme

İnternet vasıtasıyla gerçekleştirilen faaliyetler;

- Postalama,
- Bilgi Paylaşımı
- Taştışma Platformları
- Telefon açma,
- Alışveriş yapma,
- Pazarlama
- Bankacılık,
- Müzik ve oyun

Sosyal Medya

- Youtupe
- Facebook
- Twitter
- Skype
- RSS
- Google
- Tolk
- Blog
- Linkedin

Siber Saldırı/Siber Savaş

- Hedef seçilen şahıs, şirket, kurum, örgüt, gibi yapıların bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırılara **'siber saldırı'** deniyor. Bunlar, ticari, politik veya askerî amaçlı olabiliyor.

- Aynı saldırıların ülke veya ülkelere yönelik yapılmasına ise **'siber savaş'** deniyor.

- Bu tanımlara göre, Anonymous isimli grubun Türkiye'deki bazı kurumlara yönelik eylemine siber saldırı, Wikileakes'in yaptığına ise siber savaş demek mümkün.

Siber Güvenlik

Tanımı

Siber ortamda, kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür.

Kaynak: ITU X.1205

Siber Güvenlik Tanımı (ABD Başkanı Obama)

“Ülke olarak karşılaşılan çok ciddi ekonomik ve ulusal güvenlik sağlama hedeflerinden birisi olup hükümet veya ülke olarak henüz tam anlamıyla önlem alamadığımız bir husustur.”

“Amerika’nın sayısal altyapısını kapsamlı olarak güven altına alma yaklaşımlarının geliştirilmesi ve bilgi ile haberleşme altyapısının savunulmasına yönelik olarak federal çözümlerin gözden geçirilmesi” emrini verir.

"America's economic prosperity in the 21st century will depend on cybersecurity." *May 2009*

PENTAGON: Sinop'taki kuleye ihtiyaç yok

- RICHARD CLARKE (Beyaz Saray Siber Güvenlik Uzmanı)
- Casusluk artık çok kolaylaştı diyor Clarke. "Eskiden Washington'daki Rus Elçiliği'nde çalışan bir KGB ajanının bir FBI ajanı ayartması çok zordu. Ama şimdi Moskova'da oturuyorsun. Ve hiçbir risk olmadan binlerce sayfa çalabiliyorsun. Eskinin casuslarına artık gerek yok." İstihbarat örgütleri sadece insan kaynağı açısından değişmedi Clarke'a göre. Altyapı da olduğu gibi farklılaştı: "Eskiden Sinop'ta büyük bir kulemiz vardı. Rusya'daki konuşmaları dinliyorduk. Ama şimdi buna ihtiyaç yok. Kimse radyofrekansı kullanmıyor. Ulusal Güvenlik Ajansı'nın (NSA) Maryland'deki kampüsünden bütün dünyadaki internet trafiğini izliyoruz. Bu konudaki bütçe Pentagon'a ait olduğundan, NSA ve Pentagon neredeyse tek bir kuruluş gibi çalışıyor. Amerikalı asker Sinop'a gitmesine gerek kalmadan her işini masasından halledebiliyor."

Siber Savaş

ABD hükümetinin, 2002 yılında sanal güvenlik harcamaları için ayırdığı kaynak 2.7 milyar dolar, 2003'te ise bu oran 4.2 milyar dolar olarak belirlendi. Artık sadece iyi bir orduya sahip olmanız güvenliğiniz için yeterli değil. Bilgisayarın ve enformasyonun gücü artık devletleri içine alabilecek kadar güçlü.

Bu gün ise Amerika'nın siber savaşlarda mücadele etmek için günlük 12 milyon dolar harcadığını düşündüğümüzde geleceğin siber ordular üzerine kurulacağını tahmin etmek çok zor değil.

Siber Savaşlar

- Temelleri 1947 -1991 yılları döneminde yaşanan Soğuk Savaş döneminde atılan **siber savaşlar**, son yıllarda teknolojinin giderek zirve yapmasıyla kendinden iyice söz ettirmeye başladı. Başını ABD, Rusya, Çin, İsrail ve İngiltere'nin çektiği ülkeler savunma ve saldırı timlerini oluşturmanın yanında taşeron hackerlar da kullanmayı ihmal etmiyor.

- **21. yüzyıl teknolojileri her anlamda dünyanın geleceğine şekil vermeye devam ediyor. Öyle ki teknolojinin ulaştığı nokta artık onun doğrudan bir silah olarak da kullanabileceğini göstermekte.**

Siber Savaşlar

- CIA başkanı Leon Panetta,
- "İnternet üzerinden, hükümet birimlerimize saldıranlara karşı en ufak bir tahammül göstermeyeceğiz. Savunmamız da karşı saldırılarımız da en sert biçimde gerçekleşecek. **Soğuk Savaş bitti ama teknoloji savaşları başladı."**

- Eski ABD Savunma Bakanı Albright'a ait şu sözler siber-savaşın ciddiyetini de anlatıyor:

  "Siber saldırılar NATO ya karşı 3 tehditten biri olarak kabul edilecektir."

Siber Saldırılar

- Casusluk
- Manipülasyon
- Propaganda
- İletişim
- Virüs
- Truva atları

- ✓ Sistem bozma
- ✓ Siber bombalarla sabotaj
- ✓ Bilgi kirliliği
- ✓ Sistem kilitleme
- ✓ Dolandırıcılık

İlk Siber Savaşlar

2007 Estonya Siber Savaşı

2008 Gürcistan Siber Savaşı

Her ne kadar bağımsız gibi görünse de hala büyük oranda Rus peyki olan bu iki ülke, Rusya için de mükemmel iki deneme bölgesiydi. Nitekim Rusya bu ülkelere yaptığı saldırılarla ülkede bulunan resmi kuruluşların, finans ve basın-yayının bütün iletişimini 3 hafta süreyle kesintiye uğrattı.

Bu iki olay üzerine NATO 2008 yılında Estonya'nın Talin şehrinde bir siber savunma merkezi kurdu

ABD Savunma Bakanlığı ülkelerin füze sistemlerine, enerji boru hatlarına, basın yayın merkezlerine yapılan **siber saldırıları** savaş sebebi saydı ve klasik savaş unsurlarıyla karşılık vereceğini belirtti

Rusya'nın ABD'ye Siber Saldırısı

- Rusya 2008 yılında ABD'ye yönelik yaptığı siber saldırı ile virüslü bir hafıza kartıyla ABD'nin Irak ve Afganistan savaşlarını yürüten komuta merkezine sızmış ve ciddi sonuçlar almıştır.

- ABD daha sonra bundan haberdar olmuştur ancak bu sızıntının nerelere kadar ulaştığı bilinememiştir..

- ABD kongresinde sunulan bir raporda da Çin'in sadece Tayvan'a bir müdahale gerçekleştirmek için ABD'nin harekete geçmesini engelleyecek yeterli düzeyde siber-silahtan yararlanabilecek konumda olduğu belirtilmiştir.

ABD-İran Siber Savaşı

Rusya'nın Estonya ve Gürcistan Siber saldırılarına karşılık
ABD İran Siber Saldırısını Gerçekleştirdi.

Rusya için sembolik olarak büyük önem taşıyan bir ülke
olan İrana saldırarak karşılık verdi.

İran'ın nükleer programına sınırsız destek veren Rusya'ya karşı Oldukça özgün bir taktik deneyen ABD kendi kendini kopyalayan bir yazılım olan **Stuxnet** ile saldırdı.

Yazılım öncelikle motorları ve sıcaklığı kontrol eden merkezi mantık kontrol birimi olan PLC'yi ele geçirdi. Böylece sistemin kontrol eden diğer yazılımları da birer birer kolaylıkla elemine edebildi. Sonuç olarak özellikle nükleer yakıt zenginleştirme tesislerini hedef alan bu saldırı santrifüjlerin çılgınca dönmesine yol açtı ve ciddi fiziki zararlar verdi. İran ilk başta ne olduğunu tam olarak kavrayamasa da da sonraları durumun vahametini anladı ve en yetkili ağızdan bizzat Ahmedinejad tarafından İran'ın bir **siber saldırıya** Uğradığını doğrulandı.

Stuxnet

Stuxnet'i özel kılan en önemli şey sadece internete bağlı bilgisayarları değil herhangi bir veri girişi yapılan (USB, CD vb. aracılığıyla) bilgisayarı da ele geçirebilmesi ve kendine yönelik kullanabilmesi idi.

İran da bu saldırı sonucu tam 62.867 bilgisayara stuxnet solucanı bulaştı.

ABD'yi Telaş Sardı !

İRAN TEHDİDİNE KARŞI SİBER-GÜVENLİK ALARMI

- **Nükeer savaş tehdidi tartışmaları son bulmadan şimdi de İran'ın siber savaş teknolojileri dünyaya korku salmaya başladı.**

- Nükeer savaş tehdidi tartışmaları son bulmadan şimdi de İran'ın siber savaş teknolojileri dünyaya korku salmaya başladı. İran'ın siber gücünü artırdığını savunan ABD'li uzmanlar alarma geçti.

- ABD Dış Siyaset Konseyi Başkan Yardımcısı Ilan Berman'ın açıklamalarına göre, İran son üç yıldır siber dünyada savunma ve saldırı teknolojilerini geliştirmek için var gücüyle çalışıyor, yatırımlar yapıyor.

  Temsilciler Meclisi İç Güvenlik Komitesi'ne bağlı bir alt komiteye konuşan Berman, ABD ve müttefiklerini sanal olarak vurmak için teknik donanımını artıran İran'a karşı en kısa zamanda savunmaya geçilmesi gerektiğini söyledi

İran’ın ABD yi durduran silahları

- **İran ABD'nin Hayalet Uçak Teknolojisini Kırdı**
- **İran ABD İnsansız Uçak İletişim ve Füze Hedefleme Teknolojilerini Kırdı**
- **Elektromanyetik Darbe Barajı ve Füze Saldırıları ABD ve İsrail Askeri Üslerini Haritadan Siliyor**
- **Modern Bir Truva Atları Donanması**
- **Uyuyan Süper Virüs Kıyamet Günü Siber Saldırılarının İlk Dalgasında Tetiklenir**

  ABD ve İsrail tüm dünyadaki bilgisayar sistemlerine Stuxnet virüsü bulaştırdı. Hacker grubu isimsiz kaynak kodlarını internete sızdırdı. İran virüsü ters çevirdi ve kodları değiştirerek yeniden yazdı, böylece virüs İran yerine ABD ve diğer gelişmiş devletlerin altyapısını hedef almaya başladı. İran'a saldırı başlatıldıktan sonra İran yeni süper virüsünü aktif hale getirdi ve ABD'li hackerlerin Amerikan güç kaynaklarını kapatabilecekleri ve ABD'yi taş devrine geri gönderebileceklerine dair uyarıları gerçek oldu.

Siber Savaşın Hedefleri

Dünyada ilk defa enformasyon savaşları deyimini kullanan insan olan **John Arquilla,** günümüz teknolojisiyle kitlesel ölçekte yıkıcı eylemlerin gerçekleştirilebileceğinin bilindiğini, ancak Stuxnetle birlikte sadece enformatik değil fiziki tahribatın da verilebileceğinin anlaşıldığını söylemektedir.

Siber saldırılarla bir ülkenin trafik ışıklarından güç şebekelerine kara deniz hava yollarına kadar her şeyini felç etmek mümkündür.

Kritik Altyapılar

- Zarar görmesi veya yok olması halinde,
- Vatandaşların sağlığına, emniyetine, güvenliğine ve ekonomik refahına veya hükümetin etkin ve verimli işleyişine ciddi olumsuz etki edecek
- Fiziki ve bilgi teknolojileri tesisleri, şebekeler, hizmetler ve varlıklar

Kaynak: AB Komisyonu

Kritik Altyapılar

AB	ABD
Su	Su
Gıda	Enerji
Sağlık	Ulaşım
Enerji	Tarım ve gıda
Finans	Kolluk hizmetleri
Ulaşım	**Bilgi ve iletişim**
Sivil yönetim	Bankacılık ve finans
Bilgi ve iletişim	Bayındırlık hizmetleri
Uzay ve araştırmaları	Federal ve yerel hizmetler
Kimyasal ve nükleer endüstri	Acil hizmetler (sağlık, itfaiye, vb.)
Kamu düzeni ve güvenlik alanı	

Kaynak: Brunner, E. M., Suter, M., Güvenlik Çalışmaları Merkezi, İsviçre

Kritik Altyapılar

Kaynak: Canbay, C., Kritik Altyapıların Korunması, CEBIT 2008

Kritik Altyapıların Korunması

- Çökme, saldırı, kaza gibi durumlarda
- Kritik altyapıların performanslarının belirli bir kalite düzeyinin üzerinde kalmasını ve zararların asgari düzeyde tutulmasını sağlamak için
- Altyapı sahiplerinin, işletmecilerin, üreticilerin, kullanıcıların, düzenleyici kurumların ve hükümetlerin yaptıkları faaliyetler bütünü

Tüm kritik altyapıları/sektörleri kapsayan bütünsel bir yaklaşım gerektirmektedir

Kaynak: AB Komisyonu

Siber Tehdit Araçları

- Hizmetin engellenmesi saldırıları (DoS, DDoS)
- Bilgisayar virüsleri
- Kurtçuk (worm)
- Truva atı (trojan)
- Klavye izleme (key logger) yazılımları
- İstem dışı ticari tanıtım (adware) yazılımları
- Casus / köstebek (spyware) yazılımlar
- Yemleme (phishing)
- İstem dışı elektronik posta (spam)
- Şebeke trafiğinin dinlenmesi (sniffing ve monitoring)

Siber Tehditlerin Amaçları

- Sisteme yetkisiz erişim
- Sistemin bozulması
- Hizmetlerin engellenmesi
- Bilgilerin değiştirilmesi
- Bilgilerin yok edilmesi
- Bilgilerin ifşa edilmesi
- Bilgilerin çalınması

Araştırmalar & Veriler

- Britanya'da geçen yıl siber saldırıların ülke ekonomisine maliyeti 27 milyar pound'u buldu.
- Yılda 100 binden fazla siber saldırının yaşandığı ABD'de ise bu rakam tahmini olarak 100 milyar dolar civarında.
- **I Love You** virüsü dünya çapında yaklaşık 45 milyon bilgisayara bulaşmış ve yaklaşık **10 milyar USD'lik** maddi kayba yol açmıştır.
- **Nimda** kurtçuğunun dünya çapında yaklaşık **3 milyar USD' lik,**
- **Love Bug**'ın ise **10 milyar USD' lik** kayba yol açmıştır
- **MyDoom** adlı truva atının yol açtığı maddi zarar **4,8 milyar USD** civarında

Kaynak: Schjølberg, S., Hubbard, Lemos, R., Hahn, R.W

5. Güç Siber Ordu

- Siber savaşı ciddiye alarak hazırlanmaya başlayan ülkerler kara, deniz, hava ve uzaydan sonra beşinci bir askeri kuvveti devreye sokmanın mücadelesini veriyor. Siber alem yani tüm sanal ortam.

- ABD Gelecek için ön gördüğü **"Aktif Milli Strateji"**yle siber alem kuvvetlerinin altyapısını ilan etti.

- Başkan Obama Sanal Orduyu kurup bu işin komutanlığına ise Microsoft'un eski güvenlik şefi Howard Schmidt'i atadı

- Daha bu yılın ortasında Pentagon'da devereye girerek Ulusal Güvenlik Bürosu'nun(NSA) başkanı General Keith Alexander'ın komutasında ordular arası siber savaş projesi olan "Cyber-Command Strategy"yi başlattı.
- ABD nin bu yeni digital savaş kuvvetlerinin asıl görevi ABD askeri şebekelerini korumak ve gerektiğinde diğer ülkelerin her türlü sistemlerine saldırılar düzenlemek…

Dünyada Siber Ordular

- Siber savaş için askerler yetiştiren Amerika Birleşik Devletleri, bir yandan da bir çok siber saldırıya maruz kalıyor. Bunu Şubat 2002'de ABD Senatosu'nda bir alt komitede konuşan Bush'un sanal güvenlik danışmanı **Richard Clarke** şöyle dile getirmişti:

- **"Şer ekseninde yer alan İran, Irak ve Kuzey Kore'nin yanı sıra Çin ve Rusya da ABD'ye karşı siber askerler yetiştirmektedir. Altyapımızı hedef alabilecek bu saldırılara bundan sonra aralarında askeri operasyonların da bulunduğu tüm olanaklarla karşılık vereceğimizi duyururuz."**

Dünyada Siber Ordular

- Gelişmiş Batılı ülkelerden sonra Siber ordularıyla Çin, Rusya, Kuzey Kore, İsrail ve İran geliyor.
- İddialara göre Kuzey Kore siber savaş bölümü personel sayısını 500'den 3000'e çıkarmış durumda. Kuzey Kore Üniversitesi'nde her yıl siber savaş operasyonlarını yönetecek 120 öğrenci eğitiliyor
- Çin'in siber-savaş için 2050 yılına kadar stratejiler hazırladığı bilgisi de sızanlar arasında.
- İran " Dünya'nın en büyük ikinci siber ordusu " nu kurmak iddiasında.
- İngiltere 10 bin katılımcıya açık olarak ordu hesabına siber güvenlik elemanları yetiştirecek ABD'nin **Cyber Challenge** programından esinlenerek Savunma Bakanlığı desteğiyle geleceğin sanal güvenlik elemanlarını yetiştirmek üzere **SANS Institute** çalışmalara başladı.

Siber Güvenlik

Kişilerin Kurumların Kuruluşların Devletlerin bilgi varlıkları ve kaynaklarını hedeflenen amaçlar doğrultusunda organizasyon, insan, finans, teknik ve bilgi değerlerini dikkate alarak, kritik altyapıların varlıkların ve kaynakların başlarına **KÖTÜ BİR ŞEYLER GELMEDEN** korumaktır.

Kaynak: http://www.itu.int/ITU-D/asp/CMS/Events/2009/PacMinForum/doc/Background%20Note-Theme-4-ICT%20Apps%20&%20Cybersecurity.pdf

Siber Güvenlik Stratejisi (ABD)

- Kamu kurumları ağlarını tek bir ağ altında güvenli internet bağlantıları ile yönetme
- Kamu kurumları genelinde saldırıları tespit eden sensörler kurma
- Kamu kurumları genelinde saldırı önleme sistemleri kurulumunun sürdürülmesi.
- Ar-Ge çabalarının arttırılmasını koordine etmek ve yönlendirme
- Güvenilen internet bağlantıları ile tek bir ağ kuruluş olarak kamu kurumları hizmetlerinin yönetilmesi.
- Durumsal farkındalığı geliştirmek için mevcut siber merkezleri birbirine bağlama.
- Hükümet çapında karşı siber casusluk planı geliştirilmesi ve uygulanması.
- Sınıflandırılmış ağların güvenliğini arttırma.
- Siber eğitim çalışmalarını genişletme.
- Kalıcı bir "sıçrama-ilerleme" teknolojisi, stratejiler ve programlar tanımlayınız ve geliştiriniz.
- Kalıcı ve caydırıcılık stratejileri ve programları tanımlama ve geliştirme.
- Küresel tedarik zinciri ve risk yönetimi için çok yönlü yaklaşımlar geliştirme.
- Kritik altyapı alanları içine alan ve devletin sorumluluklarını tanımlayan genişletilmiş siber güvenlik çalışmaları yapma

Kaynak: http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf

Siber Güvenlik Stratejisi (Hindistan)

- Güvenlik Politikası, Uyum ve Güvence (Yasal Çerçeve)
- Güvenlik Olayı – Erken Uyarı ve Müdahale
- Kapasite geliştirme
- Dijital Adli Tıp Merkezleri Kurma
- Araştırma ve Geliştirme
- Uluslararası İşbirliği

Siber Güvenlik Stratejisi (Almanya)

Stratejik Hedefler ve Ölçütler

- Kritik Bilgi Altyapılarını Koruma
- Almanya BT Sistemleri Güvenliğini Sağlama
- Kamu Yönetiminde BT Güvenliğin Güçlendirilmesi
- Ulusal Siber Müdahale Merkezi
- Ulusal Siber Güvenlik Konseyi
- Siber Güvenlik İçin Etkili Suç Kontrolü
- Avrupa Ve Dünya Çapında Siber Güvenliği Sağlamak İçin Etkin Koordinasyon
- Güvenilir Ve Sağlam Bilgi Teknolojisi Kullanımı
- Federal Kurumlardaki Personellerin Eğitimi Ve Gelişimi
- Siber Saldırılara Müdahale Araçları

Siber Güvenlik Stratejisi (Hollanda)

- Bağlama ve güçlendirme girişimleri
- Kamu-Özel Ortaklığı
- Bireysel sorumluluk
- Departmanlar arasındaki sorumluluk Bölümü
- Aktif uluslararası işbirliği
- Alınması gereken önlemler orantılı olmalıdır
- Öz-denetim

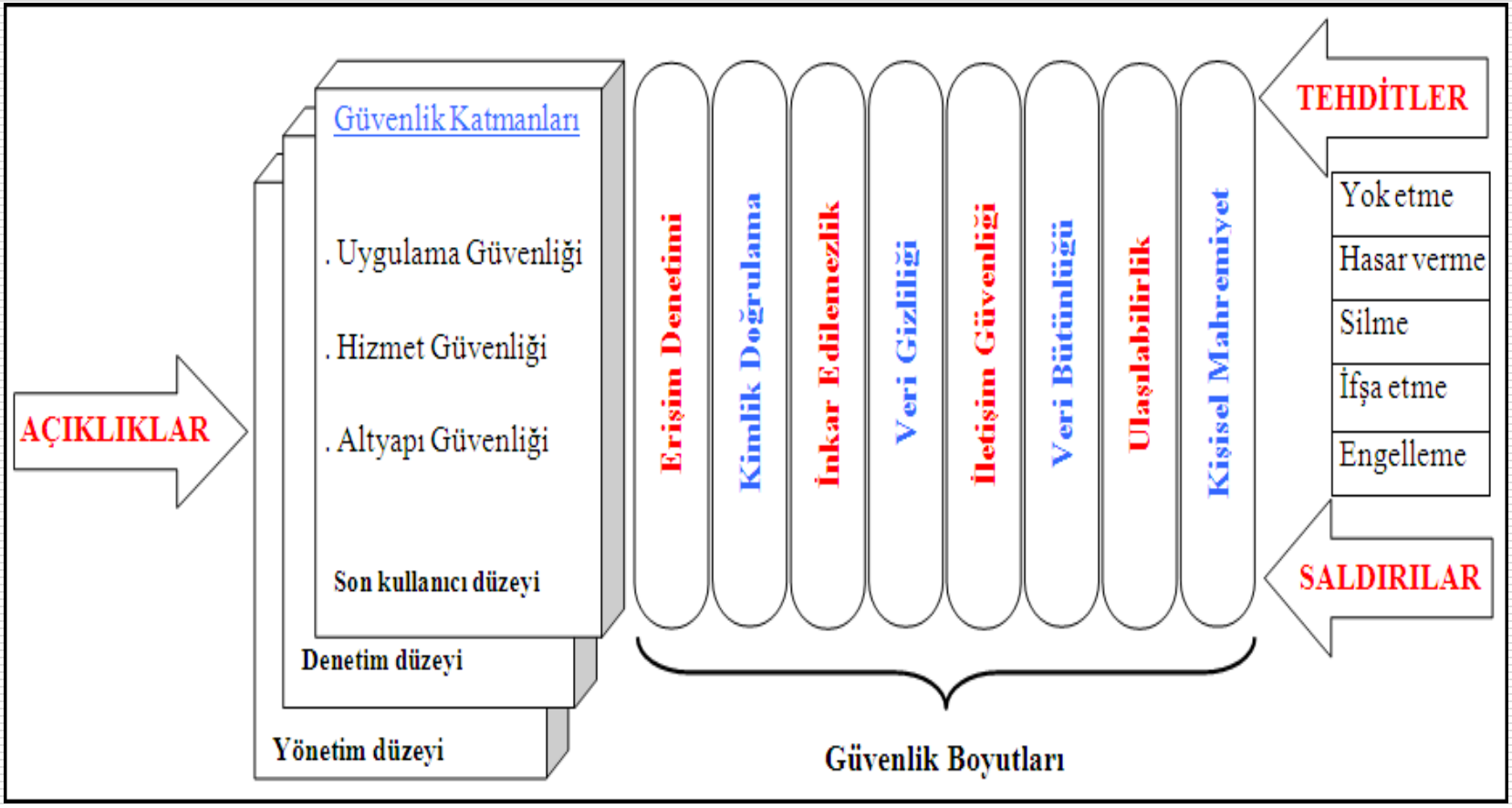
Sonuç

Neler Yapılmalı ???

Bilgi güvenliği konusu, salt teknik – mühendislik bir konu olmayıp, farklı boyutları bulunmaktadır

- ✓ Yasal boşluk giderilmeli (1999'dan beri sürüncemede)
- ✓ Yetkili kurum tespit edilmeli
- ✓ Ulusal Strateji hazırlanmalı
- ✓ Düzenleyici çerçeve oluşturulmalı
- ✓ Farkındalık oluşturulmalı
- ✓ Eğitim müfredatına ilave edilmeli
- ✓ ……

Siber Güvenlik

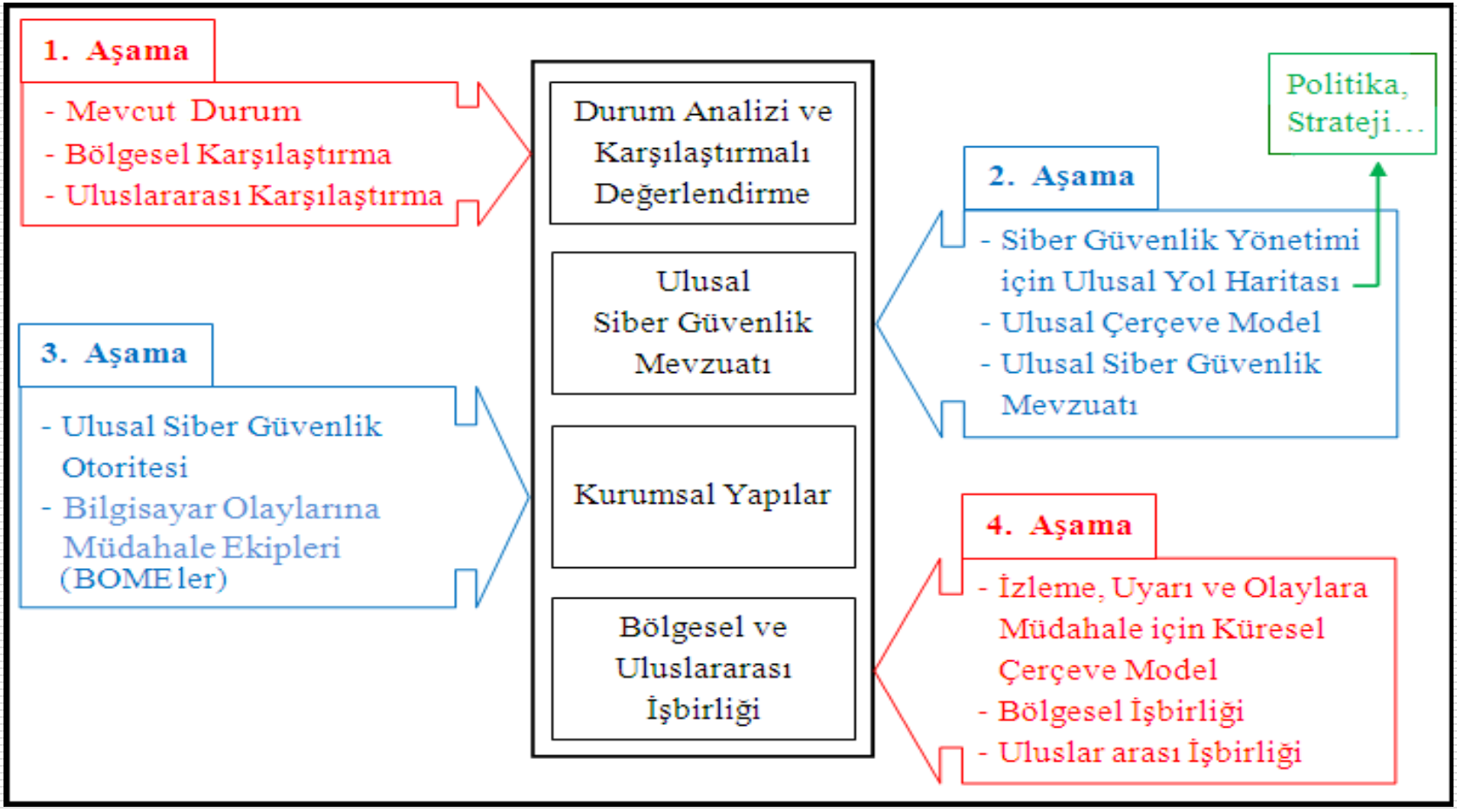


Kaynak: ITU X.1205

Temel İlkeler

1. Temel hak ve hürriyetlerinin korunması
2. Demokratik toplum düzeninin gereklerine uyulması
3. Ölçülülük İlkesine uyulması
4. Karar alma süreçlerine tüm paydaşların katılımının sağlanması
5. Bütüncül bir yaklaşımla hukuki, teknik, idari, ekonomik, politik ve sosyal boyutların ele alınması
6. Güvenlik ile kullanılabilirlik arasında denge kurulması
7. Diğer ülke mevzuatlarının göz önünde bulundurulması ve mümkün olabildiğince uyumluluğun sağlanması
8. Uluslar arası işbirliğinin sağlanması

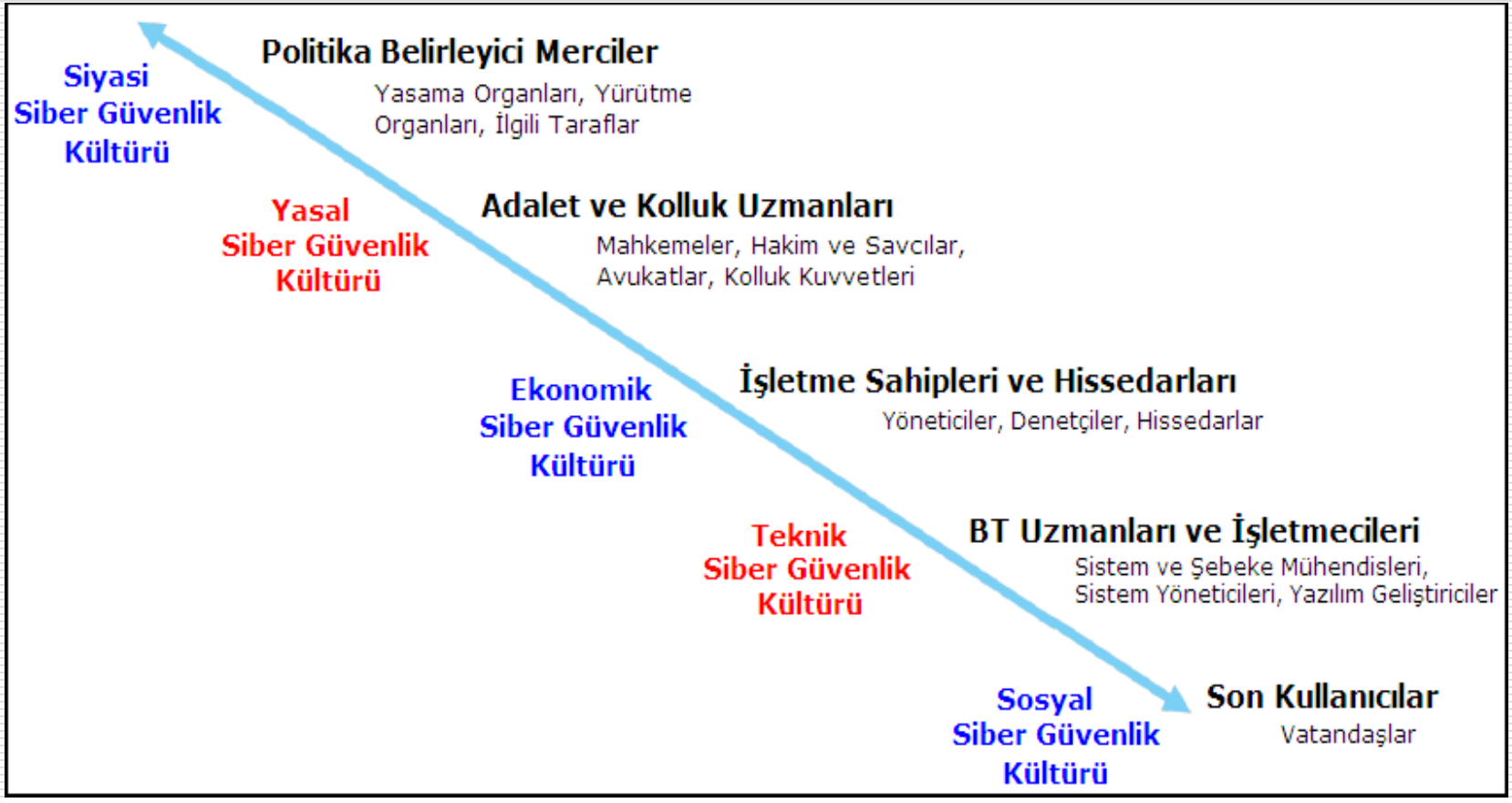
Yöntem



Kaynak: ITU

Siber Güvenlik Adımları

Siber Güvenlik Kültürünün Oluşturulması



Kaynak: ITU

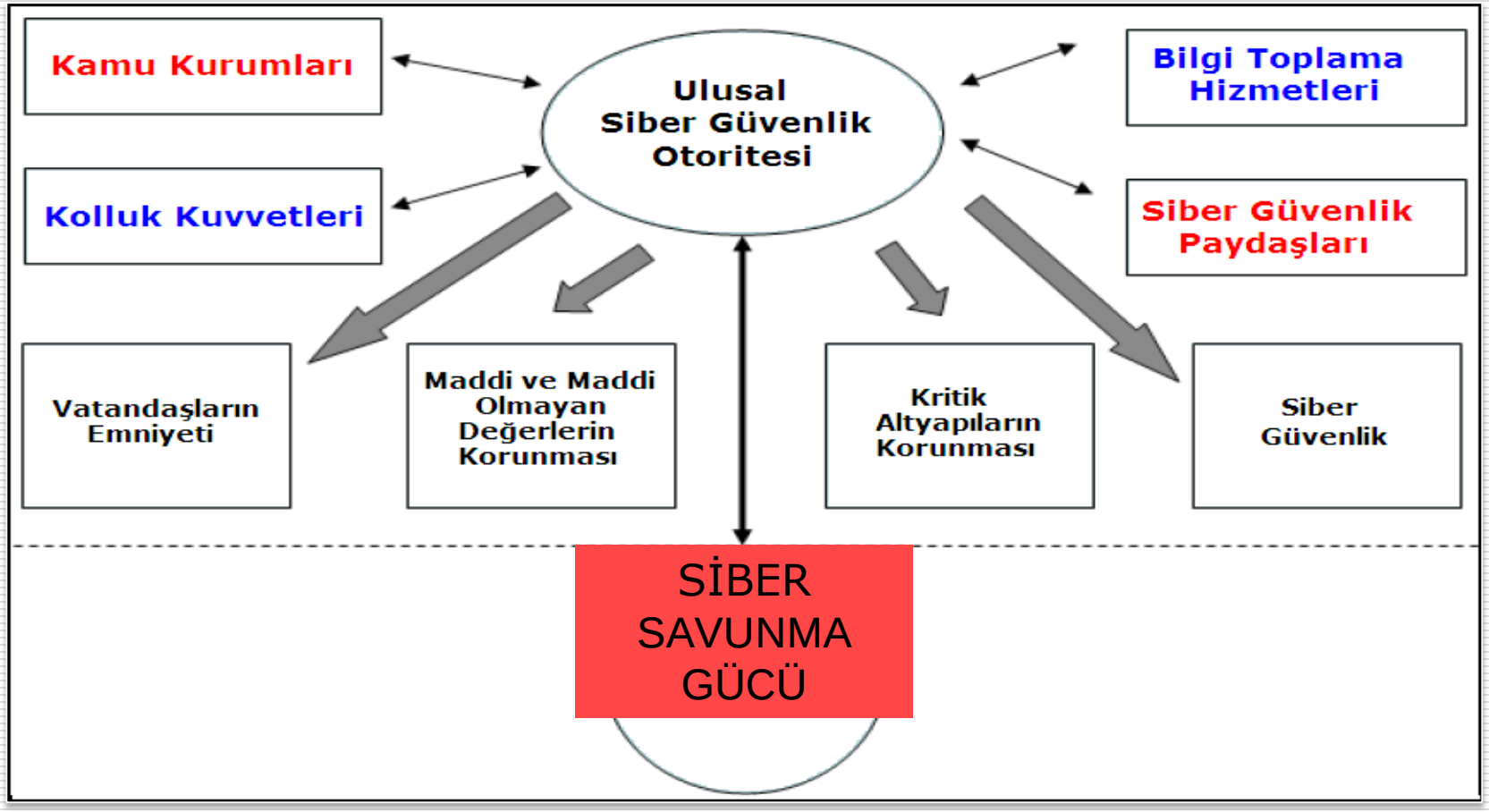
Farkındalığın Artırılması

- Güvenlik zincirinde en zayıf halkası bireyler olduğundan bireylere ve KOBİ'lere öncelik verilmesi
- Kullanıcılara yönelik siber güvenlik farkındalığı programları sunulması
- Özel şirketlerde güvenlik kültürü geliştirilmesinin teşvik edilmesi
- Sivil topluma yönelik destek programları sunulması (Ebeveynlere yönelik dersler, eğitimcilere yönelik destek malzemeleri, çocuklara yönelik gelişim kitapları veya oyunlar gibi)
- Kapsamlı bir ulusal farkındalık programının tesis edilmesi (Personelin eğitilmesi, yaygın kabul gören güvenlik sertifikasyonlarının alınması gibi)
- İnternet kullanıcılarının kişisel mahremiyet ve siber ortamdaki kimliğin sınırları hakkında eğitilmesi

Ulusal Kapasitenin Geliştirilmesi

- Karar vericiler, adli merciler, kolluk kuvvetleri ve BİT üreticilerinin ve hizmet sağlayıcılarının siber güvenlik konusunda eğitim, bilinç düzeyi, teknik ve idari becerilerinin arttırılması
- Siber güvenlik konusunda bilim ve teknoloji, araştırma ve geliştirme programları ve projeleri geliştirilmesi
- BİT yazılımlarının ve donanımlarının güvenlik kapasitesinin güçlendirilmesi
- Kritik bilgi ve altyapılar başta olmak üzere kamuya ait BİS için bir siber güvenlik planı (risk yönetimi, acil durum yönetimi) oluşturulması
- Siber güvenlik ile ilgili olaylara medyada yer verilmesinin sağlanması
- Siber güvenlik konusunda eğitim programları, çalıştaylar, konferanslar, toplantılar gibi etkinliklerin düzenlenmesi

Ulusal Güvenlik Otoritesi



Ulusal Güvenlik Otoritesi
(Ulusal Koordinasyon Kurulu)

- Ulusal siber güvenlik politikasının tanımlanması
- Ulusal siber güvenlik girişimleri için önceliklerin belirlenmesi
- Siber güvenlik faaliyetlerinin ulusal seviyede koordine edilmesi
- Siber güvenlik sorunlarını ele almak üzere paydaşların ve kamu-özel sektör ilişkilerinin belirlenmesi
- Bölgesel ve uluslar arası taraf, kurum ve kuruluşlarla işbirliği yapılması
- Kamuya ait BİS' in ve BİŞ' in izlenmesi ve risk değerlendirmesi
- Siber güvenlik ile ilgili uluslar arası standartların uygulanması
- Bilgi ve iletişim altyapılarının, hizmetlerinin veya işletmecilerinin sertifikasyonu