



SİBER GÜVENLİK YÖNETİMİ, 11.3.2023

Ahmet PEKEL

- ◇ **1982-1986 ODTÜ, Bilgisayar Mühendisliği**
- ◇ **1986-1987 ASELSAN, Yazılım Mühendisi**
- ◇ **1987-1988 MSB, Programcı Subay**
- ◇ **1988-1989 ASELSAN, Yazılım Mühendisi**
- ◇ **1989-1999 TCMB, Sistem Programcısı,
Uzman Çözümleyici/Programcı,
Sistem Uzman Yrd., Sistem Uzmanı**
- ◇ **1999-2004 TCMB, Sistem Teknik Destek Yönetici Yardımcısı**
- ◇ **2008-2009 TBD, Ankara Şb. Kurucu Üyesi**
- ◇ **2009-2011 TBD, Ankara Şb. Yk. Üyesi**
- ◇ **2013-2014 TMMOB BMO, Mesleki Yeterlilik Komisyonu Üyesi**
- ◇ **2015-2017 TBD, Yk. Üyesi**
- ◇ **2017-2019 TBD / İcra Kurulu Üyesi (Bilişimde Özenli Türkçe
Çalışmalarından Sorumlu)**
- ◇ **2004-2019 TCMB, Bilişim Güvenliği ve Kalite Denetimi Müdürü,
Bilişim Güvenliği ve Kalite Yönetimi Müdürü,
Bilişim Teknolojileri Güvenlik Direktörü**
- ❖ **2020-2022 TMMOB BMO Onur Kurulu Üyesi**
- ❖ **2017- TBD, Bilişimde Özenli Türkçe Ç.Topluluğu Bşk. Yrd.**
- ◇ **2019- Siber Güvenlik Yönetim Danışmanı**
- ❖ **2021- TBD Yayın Kurulu Başkanı**
- ❖ **2021- TOBB Yazılım Sektörü Meclis Danışmanı**
- ❖ **2022- TMMOB BMO Kamu Bilişim Politikaları Kom. Başkanı**

Ahmet Pikel

<https://pekelahmet.com>
a.pikel@pekelahmet.com

KONU BAŞLIKLARI

Dünya genelinde siber saldırı risklerine ilişkin beklentiler

Siber saldırıların ardındaki amaçlar

Siber saldırılarda kullanılan yöntemler

Siber saldırıların hedefleri

Siber güvenliğe ilişkin düzenlemeler

Siber güvenlik yönetimi

Siber güvenliğin geleceği

SİBER SALDIRI RİSKLERİ

```
or object to mirror_mod.mirror_object
operation == "MIRROR_X":
    mirror_mod.use_x = True
    mirror_mod.use_y = False
    mirror_mod.use_z = False
operation == "MIRROR_Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

#selection at the end -add
mirror_ob.select= 1
modifier_ob.select=1
context.scene.objects.active
("Selected" + str(modifier_ob.name))
mirror_ob.select = 0
bpy.context.selected_objects
data.objects[one.name].select

print("please select exactly one object")

-- OPERATOR CLASSES -----

bpy.types.Operator):
    X mirror to the selected
    object.mirror_mirror_x"
    mirror X"
```


DÜNYA GENELİNDE SİBER SALDIRI RİSKLERİNE İLİŞKİN BEKLENTİLER

Dünya Ekonomik Forumu verilerine göre siber saldırılar, gerçekleşmesi olası küresel riskler arasında yer alıyor.

Bilişim teknolojileri kullanılarak gerçekleştirilen veri sahtekarlığı ve hırsızlığı da olası küresel riskler arasında yer almakta.

Etkileri açısından doğal olaylar, su sıkıntısı, küresel ısınma, yıkıcı silahlar daha öncelikli görülmekle birlikte, siber saldırıların çok düşükten çok yıkıcı zararlara kadar son derece etkili olabileceği öngörülmüyor.

NEDEN SİBER GÜVENLİK?



Siber uzaya katılan kişi ve aygıt sayısı hızla artıyor.

Bugün, Dünya nüfusunun yarısından fazlası İnternet kullanıcısı.

Son 20 yılda İnternet kullanıcı sayısındaki artış yüzde 1000'in üzerinde.

İnternete bağlı aygıt (Nesnelerin İnterneti: IoT - Internet of Things) sayısı 100 milyara doğru yaklaşmakta.

Dünya genelinde her gün bir milyona yakın yeni zararlı yazılım saldırısı meydana geliyor.

Siber saldırıların Dünya ekonomisine maliyeti trilyon Dolarlarla açıklanmaya başlandı.

Güvenlik ihlallerinin yarısından çoğu doğrudan doğruya kişisel verilerle ilgili.

Siber Tehdit Haritaları

- ◇ <https://www.imperva.com/cyber-threat-attack-map/>
- ◇ <https://threatmap.fortiguard.com/>
- ◇ <https://cybermap.kaspersky.com/>
- ◇ <https://www.fireeye.com/cyber-map/threat-map.html>



SİBER SALDIRILAR: Nedenler, Aktörler, Sonuçlar

Siber saldırıların ardında; politik, ekonomik ve/veya jeopolitik nedenler olabilir.

Saldırıları, devlet ya da devlet dışı aktörler tarafından başlatılabilir.

Siber saldırılar, toplum düzenini bozabilecek düzeyde bir etki oluşturabilir, itibar ve inandırıcılık kaybına neden olabilir.

SİBER SALDIRILAR: Amaçlar

1

Dünya genelinde gerçekleşen siber saldırıların yüzde 88'ine yakını siber suç kapsamında değerlendirilmektedir.

2

Saldırıların yüzde 8'e yakını siber haber alma çalışmalarıyla ilişkilendirilmektedir.

3

Çok az bir bölümü ise (yüzde 1 düzeylerinde) siber savaş kapsamında ele alınmaktadır.

SİBER SALDIRI YÖNTEMLERİ

- ◆ **Kötücül yazılımlar (malware)**
- ◆ **Sistem ya da yazılım açıklıklarını sömürme**
- ◆ **Kullanıcı hesabı ele geçirme**
- ◆ **Hedefli saldırılar**
- ◆ **Kötücül kod yerleştirme**
- ◆ **Yanlış yapılandırılmış sistemler**
- ◆ **Kötücül istenmeyen (spam) iletiler**
- ◆ **Sahte sosyal hesaplar**
- ◆ **Kötücül reklam kodları**

SİBER SALDIRI HEDEFLERİ

- ◊ Sanayi kuruluşları
- ◊ Bireyler
- ◊ Kamu
- ◊ Bilim-Teknik
- ◊ Sağlık
- ◊ Eğitim
- ◊ Destek hizmetleri

- ◊ Finans ve sigortacılık
- ◊ Konaklama ve yiyecek
- ◊ Satış ve kiralama hizmetleri
- ◊ Sanat ve eğlence
- ◊ İmalât
- ◊ Ödeme Sistemleri
- ◊ Emlâk
- ◊ Bilgi ve İletişim Teknolojileri



Kritik Altyapılar

**Siber savaşlarda en çok yeğlenen saldırı hedefleri kritik altyapılar;
ülkenin yaşamsal kaynakları...**

savunma

enerji

ulaşım

finans

sağlık

iletişim
altyapıları

su
yönetimi

SİBER GÜVENLİĞE İLİŞKİN DÜZENLEMELER ve ÖNEMİ

```
object to mirror  
mirror_mod.mirror_object
```

```
operation == "MIRROR_X":  
    mirror_mod.use_x = True  
    mirror_mod.use_y = False  
    mirror_mod.use_z = False  
operation == "MIRROR_Y":  
    mirror_mod.use_x = False  
    mirror_mod.use_y = True  
    mirror_mod.use_z = False  
operation == "MIRROR_Z":  
    mirror_mod.use_x = False  
    mirror_mod.use_y = False  
    mirror_mod.use_z = True
```

```
selection at the end -add  
mirror_ob.select= 1  
mirror_ob.select=1  
context.scene.objects.active  
("Selected" + str(modifier))  
mirror_ob.select = 0  
= bpy.context.selected_objects  
data.objects[one.name].select  
print("please select exactly")
```

```
-- OPERATOR CLASSES --
```

```
types.Operator):  
    X mirror to the selected  
    object.mirror_mirror_x"  
    mirror X"
```

An abstract graphic on the left side of the slide. It features a dark blue background with a network of white lines connecting various points. Some points are highlighted with small white circles. Overlaid on this network are several translucent, overlapping triangles in shades of blue and purple. Binary code (0s and 1s) is scattered across the image, appearing as if it's floating or part of the network. In the bottom right corner of the graphic area, there's a small grid with numbers 10, 20, 30, and 40 along its axes.

Siber saldırılara karşı hazırlıklı olma gereksinimi

Siber Uzay'da;

◆Sınırlar yok!

◆Kural yok!

◆Otorite yok!

◆Karmaşa ve belirsizlik var!

Siber saldırılara karşı hazırlıklı olma gereksinimi

- ❖ Siber saldırganlar kendilerini çok hızlı yenileyip, savunma durumundaki kişilerden daha hızlı davranabilmekte; bunu çok düşük bir maliyetle gerçekleştirebilmektedirler.
- ❖ Dünyanın herhangi bir yerinde yaşanan siber olaydan tüm ülkeler etkilenebilmektedir.
- ❖ Siber saldırılara karşı her ülkenin, her kurumun hazırlıkları farklı seviyelerdedir; güvenlik ve inandırıcılık önemli olduğundan işbirliği içinde olunan ülkelerle ortak seviyelerin oluşturulması gerekmektedir.
- ❖ Ekonomik ve sosyal faaliyetlerin sürdürülebilmesi için uluslararası düzeyde ortak güvenlik ölçütlerine göre hazırlık, planlama, uygulama ve bilgi paylaşımı gereksinimi vardır.

Düzenlemeler ve Amaçları

- ◊ Siber güvenlik yeteneklerini geliştirmek
- ◊ Olay bildirme altyapısını oluşturmak
- ◊ Kriz yönetimi
- ◊ Risk yönetimi
- ◊ Veri koruma
- ◊ Denetleme ve değerlendirme
- ◊ İşbirliği olanaklarını geliştirme (eğitimler, tatbikatlar vb.)

Düzenlemeler ve Amaçları



Ulusal Siber Güvenlik Stratejileri

- ◊ Siber Güvenlik Ulusal Güvenliğin önemli bir bileşeni.
- ◊ 7x24 iletişim gerektiriyor.
- ◊ Ulusal stratejiler: 2013-2014, 2016-2019, 2020-2023 (kritik altyapılar, yeni teknolojilerin güvenliği, yerli ve milli teknolojilerin geliştirilmesi)
- ◊ Kovid-19'da en çok: uzaktan erişim, görüntülü toplantı, e-ticaret, bankacılık uygulamaları kullanıldı; sosyal yaşam bilişim ortamlarına taşındı, ortalama saldırıları arttı.
- ◊ Yapay zekâ, nesnelerin interneti, blok zincir, 5G- & 6G, davranışların interneti gibi konular ön plana çıktı.

Kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerin bilgi ve iletişim güvenliği

- ❖ 06.07.2019 tarih ve 30823 sayılı Resmi Gazete’de Bilgi ve İletişim Güvenliği Tedbirleri konulu 2019/12 sayılı Cumhurbaşkanlığı Genelgesi yayımlanmıştır. Yayımlanan Genelge doğrultusunda Cumhurbaşkanlığı Dijital Dönüşüm Ofisi koordinasyonunda, paydaşların katılımıyla Bilgi ve İletişim Güvenliği Rehberi hazırlanmıştır (Temmuz 2020). Ardından yayımlanan Bilgi ve İletişim Güvenliği Denetim Rehberiyle (Ekim 2021) belirtilen önlemlerin ne zaman ve nasıl alınacağı, alınmış önlemlerin nasıl denetleneceği belirlenmiştir. Uyum süreci olarak yayımlandığı tarihten (27 Temmuz 2020) 27 Temmuz 2022’ye dek geçecek süre (24 ay) öngörülmüştür. 04.01.2023 tarihinde Bilgi ve İletişim Güvenliği Uyum ve Denetim İzleme Sistemi (BİGDES) devreye alınmıştır.

Ülkemizde Siber Güvenlik Sorumluluğu

- ◊ Strateji: Ulaştırma ve Altyapı Bakanlığı
- ◊ Saldırı engelleme, caydırıcılık: BTK (USOM, SOME)
- ◊ Siber güvenliğin artırılması, yeni projelerin üretilmesi (DDO)

Ülkemizdeki bilgi ve iletişim alanlarını ilgilendiren düzenlemeler

- 5846 sayılı Fikir ve Sanat Eserleri Kanunu (2001)
- 5070 sayılı Elektronik İmza Kanunu (2004)
- Türk Ceza Kanunu'ndaki “Bilişim Alanında Suçlar” Hk. Hükümler (2005)
- 5651 sayılı İnternet Yayınları ve Suçları Hk. Kanun (2007)
- 5809 sayılı Elektronik Haberleşme Kanunu (2008)
- 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun (2014)
- 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hk. Kanun (2014)
- 6698 Kişisel Verilerin Korunması Kanunu (2016)
- Uluslararası yükümlülükler
- İlgili yönetmelikler

6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK) Veri sorumluları tarafından alınması gereken **idari önlemler**

- ◆ Kişisel Veri İşleme Envanterinin Hazırlanması
- ◆ Kurumsal Politikaların (Erişim, Bilgi Güvenliği, Kullanım, Saklama ve İmha vb.) Oluşturulması
- ◆ Sözleşmelerin (Veri Sorumlusu - Veri Sorumlusu, Veri Sorumlusu - Veri İşleyen Arasında) Güncellenmesi
- ◆ Gizlilik Taahhütnamelerinin Güncellenmesi
- ◆ Kurum İçi Periyodik ve/veya Rastgele Denetimlerin Planlanması
- ◆ Risk Analizlerinin Yapılması
- ◆ İş Sözleşmesi, Disiplin Yönetmeliği (Kanuna Uygun Hükümler İlave Edilmesi) Gibi Belgelerin Güncellenmesi
- ◆ Kurumsal İletişimin (Kriz Yönetimi, Kurul ve İlgili Kişiyi Bilgilendirme Süreçleri, İtibar Yönetimi vb.) Güçlendirilmesi
- ◆ Eğitim ve Farkındalık Faaliyetlerinin (Bilgi Güvenliği ve Kanun) Gerçekleştirilmesi
- ◆ Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) Bildirim Yapılması

6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK) Veri sorumluları tarafından alınabilecek **teknik önlemler**

- ◆ Yetki Matrisi
- ◆ Yetki Kontrol Erişim Logları
- ◆ Kullanıcı Hesap Yönetimi Altyapısı
- ◆ Ağ Güvenliği Altyapısı
- ◆ Uygulama Güvenliği Altyapısı
- ◆ Şifreleme Altyapısı
- ◆ Sızma Testi
- ◆ Saldırı Tespit ve Önleme Sistemleri
- ◆ Log Kayıtları
- ◆ Veri Maskeleyme
- ◆ Veri Kaybı Önleme Yazılımları
- ◆ Yedekleme
- ◆ Güvenlik Duvarları
- ◆ Güncel Anti-Virüs Sistemleri
- ◆ Silme, Yok Etme veya Anonim Hale Getirme
- ◆ Anahtar Yönetimi

KVKK Kapsamında DUYURULMUŞ İhlal Örneği ve Alınabilecek Önlemler



- ◇ ...'da yürütülen veri sızıntısı önleme çalışmaları kapsamında bir ... çalışanın ekinde ... sorgularını içeren e-postaları ... dışı kullanıcılara ilettiğinin belirlendiği,
- ◇ ... tarafından yapılan ön incelemede kişinin görevini kötüye kullanarak elde ettiği raporları para karşılığı üçüncü taraflara aktardığının tespit edildiği,
- ◇ İhlalden etkilenen verilerin kimlik ve finans bilgileri olduğu,

Çözüm:

- ◇ Bilgi Güvenliği Politikası Yayınlanması ve Çalışanlara Duyurulması
- ◇ İşlem Kısıtlama (Gereksinim kadar yetkilendirme)
- ◇ İşlem Kaydı Tutma (Loglama)
- ◇ Veri Sızıntısı Önleme Sistemi (Kayıt, Uyarı, İzleme, Önleme)
- ◇ Kullanıcı Bilinçlendirme Çalışması

Uluslararası kabul görmüş siber güvenlik standartları

- ◆ En iyi uygulamalara göre geliştirilmiştir
- ◆ Paydaşlar arasında ortak bir dil oluşmasına yardımcı olur
- ◆ Siber saldırıların yaratabileceği zararlardan en az maliyetle çıkılmasına olanak tanır

Uluslararası kabul görmüş siber güvenlik standartları/denetim çerçeveleri

NIST - National
Institute of
Standards and
Technology

ISO - International
Organization for
Standardization

IEC - International
Electrotechnical
Commission

SANS - SysAdmin,
Audit, Network and
Security

CSC - Computer
Sciences
Corporation

COBIT - Control
Objectives for
Information and
Related Technologies

SİBER GÜVENLİK YÖNETİMİ

```
or object to mirror_mod.mirror_object
operation == "MIRROR_X":
    mirror_mod.use_x = True
    mirror_mod.use_y = False
    mirror_mod.use_z = False
operation == "MIRROR_Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

#selection at the end -add
mirror_ob.select= 1
mirror_ob.select=1
context.scene.objects.active
("Selected" + str(modifier))
mirror_ob.select = 0
bpy.context.selected_objects
data.objects[one.name].select

print("please select exactly")

-- OPERATOR CLASSES -----

types.Operator):
    X mirror to the selected
    object.mirror_mirror_x"
    mirror X"
```

Siber güvenlik
sayısal
dönüşümün en
önemli
bileşenlerinden
biridir

Siber güvenlik bilişim
teknolojileri süreçlerini
yatay kesen temel
süreçlerdendir



ALTYAPI
TASARIM



EĞİTİM



UYGULAMA



İZLEME



İYİLEŞTİRME

Siber güvenlik yönetimi bir süreç yönetimidir

- ◊ Siber Güvenlik Stratejisi
- ◊ Siber Güvenlik Politikaları
- ◊ İK Politikaları
- ◊ Teknoloji Politikaları
- ◊ Risk Yönetimi
 - ◊ Önceliklerin Belirlenmesi
 - ◊ Önlemlerin Geliştirilmesi
 - ◊ Önlemlerin Düzenli Olarak Sınanması
- ◊ Bütçe ve Finansman
- ◊ Denetim

*“Güvenlik bir kalite hedefidir.
Sürecin olgunluğu güvenliğin
yetkinliğini belirler.”*

Siber Güvenlik Alanları

- ◊ Bilgi Güvenliği Yönetiřimi
- ◊ Bilgi Güvenlięi Mimarisi
- ◊ Siber Güvenlik Mühendislięi
- ◊ Siber Güvenlik Olay İzleme ve Önleme
- ◊ Tersine Mühendislik/Zararlı Yazılım Çözümleme
- ◊ Siber Bilgi Toplama (İstihbarat)
- ◊ Siber Güvenlik Sızma Testleri
- ◊ Şifreleme (Crypthology)
- ◊ Mobil Güvenlik
- ◊ Kimlik ve Eriřim Yönetimi
- ◊ Bilgi Güvenlięi Risk Yönetimi
- ◊ Adli Biliřim
- ◊ Siber Güvenlik İçin İnsan Kaynaęı Yetiřtirme
- ◊ Siber Güvenlik Farkındalık Geliřtirme
- ◊ Ulusal ve Uluslararası Düzenlemelere, Standartlara ve Denetim Çerçeveslerine Uyum

Temel Gvenlik İlkeleri

Gvenlik Hedeflerinin İř Hedefleriyle Uyumluluęu

Uygun ve Gncel Teknoloji

Derinlemesine Savunma

Gvenlik Temelli Tasarım

Kiřisel Gizlilik Temelli Tasarım

Bilmesi Gereken İlkesi

En Az Yetki Dzeyinde Çalıřma

Saldırı Yzeyinin Azaltılması

En Zayıf Halkanın Belirlenmesi

Gvenlik Ynetiminin Yetkin Çalıřanlarca Yrtlmesi



Saldırı
yüzeyini
azaltmanın
5 yolu:

Altyapıdaki karmaşıklığın ortadan kaldırılması

Güvenlik açıklarının saptanması, önlem alınması

Ağın bölütlenmesi, birbirinden yalıtılması

Risklerin önceliklendirilmesi

Gereksiz bağlantı noktalarının kapatılması



Siber saldırılarda en çok
bireyler hedef alınıyor!

Akılda tutulması gerekenler...

Güçlü Parola

Önemli Bilgilerin Düzenli
Olarak Yedeklenmesi

Yazılımların Güncel Tutulması

Şüpheli Bağlantıların
Açılmaması

Sanal Ortam Hesaplarının
Yönetilmesi



SİBER GÜVENLİĞİN GELECEĞİ

```
for object to mirror  
mirror_mod.mirror_object =  
operation == "MIRROR_X":  
mirror_mod.use_x = True  
mirror_mod.use_y = False  
mirror_mod.use_z = False  
operation == "MIRROR_Y":  
mirror_mod.use_x = False  
mirror_mod.use_y = True  
mirror_mod.use_z = False  
operation == "MIRROR_Z":  
mirror_mod.use_x = False  
mirror_mod.use_y = False  
mirror_mod.use_z = True
```

```
selection at the end -add  
mirror_ob.select= 1  
mirror_ob.select=1  
context.scene.objects.active  
("Selected" + str(modifier))  
mirror_ob.select = 0  
bpy.context.selected_objects  
data.objects[one.name].select  
print("please select exactly")
```

-- OPERATOR CLASSES --

```
bpy.types.Operator):  
X mirror to the selected  
object.mirror_mirror_x"  
mirror X"
```

Teknolojik gelişmeler (örnekler)

- ◇ ...
- ◇ Bulut Bilişim 2009
- ◇ İnternet TV 2011
- ◇ Kendi Cihazını Getir (BYOD) 2012
- ◇ Büyük Veri 2013
- ◇ Nesnelerin İnterneti 2014
- ◇ Otonom Araçlar 2015
- ◇ ...

”Siber güvenlikte yarın, bugünden farklı olacak...”



Nesnelerin İnterneti (IoT): DDOS saldırılarının etkisini artırmak için yeni hedef



IoT teknolojilerinin belli bir olgunluğa eriştiği yıl 2014'dür.

Çoğunlukla güvenlik açısından güçlendirilmemiş olarak üretildiklerinden, kolay ele geçirilebilmektedir. Bu nedenle IoT cihazları, DDOS atakları için kullanışlı birer silah haline gelmiştir.

Eksik ve hatalı yapılandırılmış sistemler ele geçirilerek DDOS saldırı hacmi artırılabilir (2018'de Github'a yapılan son DDOS atakının boyutu 1.35 Tbps).

Bebek izleme
aygıtları : Düşük
güvenlik
yapılandırması



Çoğu bebek izleme aygıtları (webcam)
video akışını şifrelemediklerinden
kolaylıkla siber saldırganların hedefi
olabilmektedirler.



Yetersiz güvenlikte üretildiklerinden ev
ağına sızmak için birer atlama taşı
olarak da kullanılmaktadır.

“Teknolojideki gelişmeler hem siber savunma şekillerini hem de saldırı yöntemlerini etkileyecek...”

Teknolojik eğilimler

Nicem Bilgisayarlar – Quantum Computing

Sayısal İkizler – Digital Twins

Öbekzincir – Blockchain

Yapay Zekâ Tabanlı Geliştirme – AI Driven Development

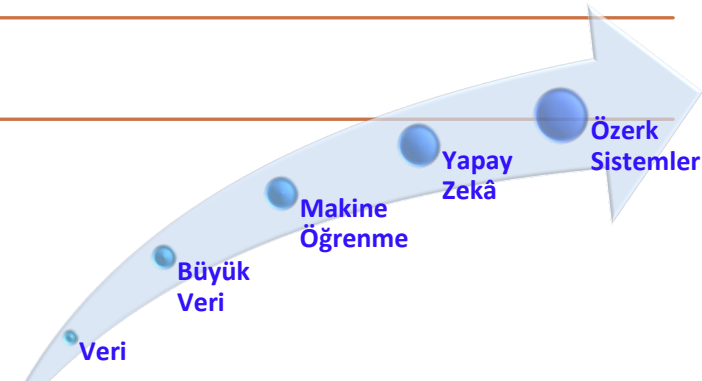
Özerk Nesneler - Autonomous Things

Artırılmış Çözümleme – Augmented Analytics

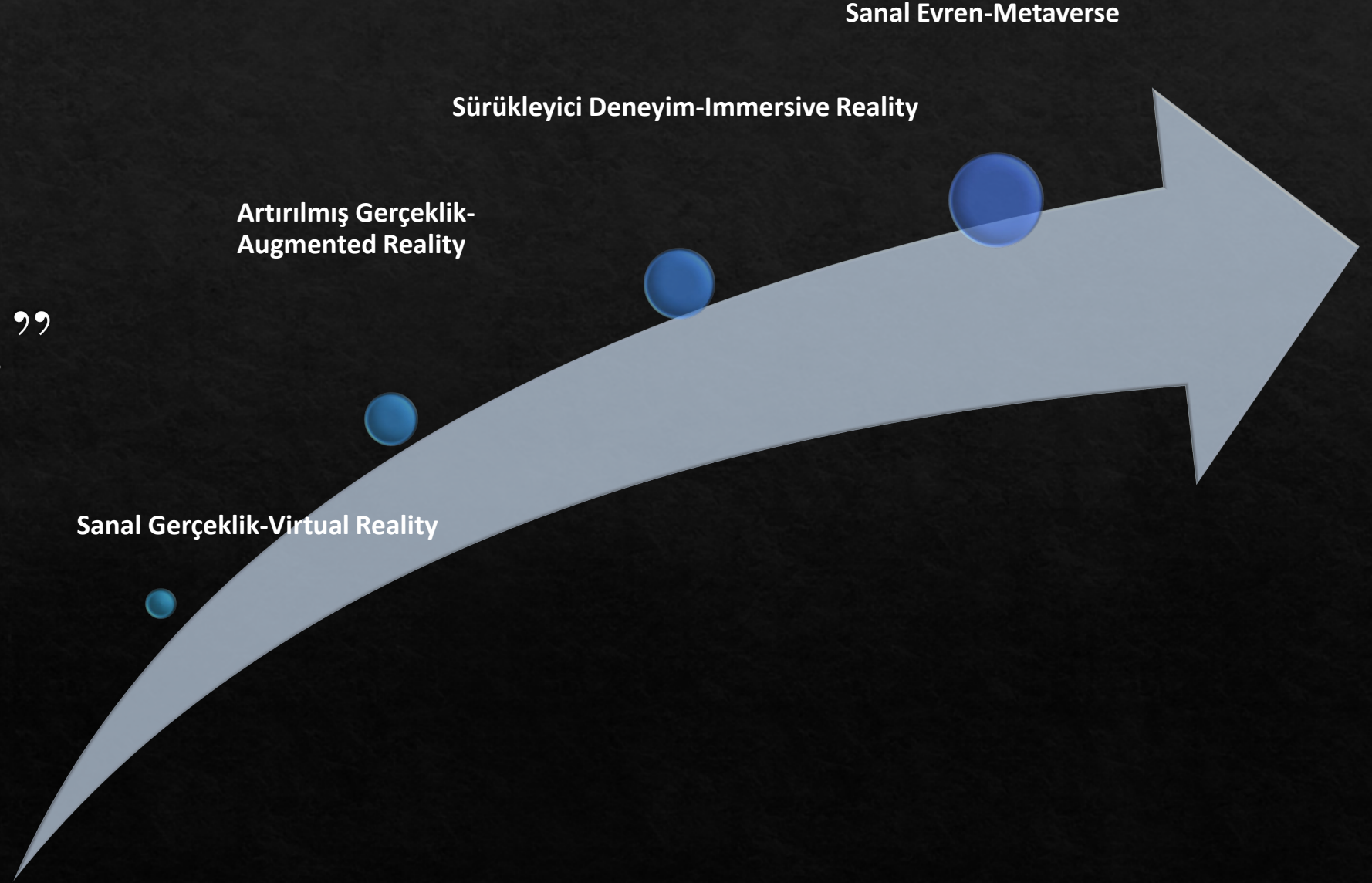
Güçlendirilmiş Uç – Empowered Edge

Sanal Evren – Metaverse

Akıllı Alanlar – Smart Spaces



“Sanal Gerçeklik...”



“Verinin Yolculuđu...”



DAVRANIŞLARIN İNTERNETİ (IoB)

- Özerk sistemler alışkanlıklarımıza ilişkin verileri toplayıp, araçları yönlendirebilecekler.
- Sosyal mühendislik için kimi veriler kullanılabilir
- Davranış Analizi-Yönlendirme-Pazarlama (Adsızlaştırma önemli)

Siber Güvenlik Teknolojilerinde Beklenen Geliřmeler

Yakın Gemiř

İmza Tabanlı Saldırı Önleme Sistemleri (%30)

İnsan müdahalesine bağımlı güvenlik süreçleri

Bugün

Davranış Tabanlı Saldırı Önleme Sistemleri

Büyük Veri Çözümleme (log, dosya, paket) Uygulamaları

Yapay Zekâ Kullanımı

Makine Öğrenme Süreci

Tam Otomasyon

Siber Dayanıklılık

Yakın Gelecek

Siber Güvenlikte Nicem Bilgisayarların Kullanımı

(Kapasite ve Hız Kazanımı)

Siber Güvenlik Uzmanlığı Açığının Kapatılmasında Yapay Zekâdan Yararlanılması

(Güvenlik Verilerinin Hızlı ve Doğru Bir Şekilde Çözümlemesine Yardımcı Olması)

Bulut Uygulamalarının Yaygınlaşması

Teşekkürler



@pekelahmet



<https://pekelahmet.com>