



# TBD KAMU-BİB

Kamu Bilişim Platformu-19

26-29 Ekim 2017



## Dijital Türkiye ve Siber Dünya: Siber Güvenlik 'te Milli Hedeflerimiz

Mustafa AFYONLUOĞLU



Siber Güvenlik, E-Yönetişim ve E-Devlet Kıdemli Uzmanı



#DigitalDevlet

# 2017'DE SİBER DÜNYA

VERİ SIZINTILARI	2014 <sup>(1)</sup>	2015 <sup>(1)</sup>	2016 <sup>(2)</sup>
Sızıntı Sayısı	312	318	1,209
Sızıntı başına Ortalama Veri Kaybı	805	466	927
Toplam Sızan Veri Adedi	348,000,000	428,000,000	1,100,000,000
10 Milyondan fazla kişiyi etkileyen olay sayısı	4	9	15
Son 8 Yılda Sızan Veri Miktarı	7.1 MİLYAR KİMLİK	+ 3 Milyar	+ 0,14 Milyar

FİDYE YAZILIMLAR	2014	2015	2016
Tespit Edilen Fidye Olay Sayısı	0	340,665	463,841
Fidye Yazılım Türü	30	30	101
Ödenen Ortalama Fidye (ABD Doları)	373	294	1,077

ORTALAMA	2017 (Ekim)	2016	
Tarım, Ormanlık ve Balıkçılık	Her 1751 postada 1 tane	Her 1815 postada 1 tane	1. Sırada
<b>Kamu Yönetimi</b>	<b>Her 2147 postada 1 tane</b>	Her 2329 postada 1 tane	<b>4. Sırada</b>
Madencilik	Her 2276 postada 1 tane	Her 2254 postada 1 tane	3. Sırada
Finans, Sigorta ve Kiralama	Her 2420 postada 1 tane	Her 1918 postada 1 tane	2. Sırada
Hizmet Sektörü	Her 3191 postada 1 tane	Her 3091 postada 1 tane	7. Sırada

(1) Nisan 2016 Symantec Corp. Internet Security Threat Report, Vol: 21

(2) 27 Nisan 2017 Symantec Corp. Internet Security Threat Report, Vol: 22

(3) 2017 Eylül Symantec Aylık Saldırı Raporu, [https://www.symantec.com/security\\_response/publications/monthlythreatreport.jsp](https://www.symantec.com/security_response/publications/monthlythreatreport.jsp)



**TBD KAMU-BİB**

Kamu Bilişim Platformu-19

26-29 Ekim 2017

#DİGİTALDEVLET

Dijital Türkiye ve Siber Dünya  
Siber Güvenlikte Milli Hedeflerimiz

# 2017'DE SİBER DÜNYA

Saldırı Grubu	Kısa Adı	Ülke	Kuruluş Yılı	Motivasyonu	Hedef Kategoriler
Sandworm	Quedagh, BE2 APT	Rusya	2014	Casusluk, Sabotaj	Hükümetler, Uluslararası Organizasyonlar, Avrupa, Amerika, Enerji Sektörü
Fritillary	Cozy Bear, APT29, Office Monkeys	Rusya	2010	Casusluk, Hükümet Devirme, Yıkma	Hükümetler, Düşünce Örgütleri, Medya, Avrupa, Amerika
Swallowtail	Fancy Bear, APT28, Sednit	Rusya	2007	Casusluk, Hükümet Devirme, Yıkma	Hükümetler, Avrupa, Amerika
Cadelle	-	İran	2012	Casusluk	Havayolları, İletişim, İran Vatandaşları, Hükümetler, STK'lar
Appleworm	Lazarus	Kuzey Kore	2012	Casusluk, Sabotaj, Hükümet Devirme, Yıkma	Finans Sektörü, Askeriye, Hükümetler, Eğlence sektörü, Elektronik Cihazlar
Housefly	Equation	ABD	2001	Casusluk	Ülke saldırganlarına yönelik hedefler
Strider	Remsec	Batı	2011	Casusluk	Büyükelçilikler, Havayolları, Rusya, Çin, İsveç, Belçika
Suckfly	-	Çin	2014	Casusluk	e-Ticaret, Hükümetler, Teknoloji, Sağlık Sektörü, Finans Sektörü, Gemicilik Sektörü
Buckeye	APT3, UPS, Gothic Panda	Çin	2009	Casusluk	Askeri Alanlar, Savunma Endüstrisi, Medya, Eğitim Sektörü, ABD, İngiltere, Hong Kong
Tick	-	Çin	2006	Casusluk	Teknoloji, Yayıncılık, Japonya, Su Mühendisliği

Dikkat Çekici Etkileri Olan ve **Ülkeler Tarafından Desteklendiği Açıkça Bilinen** Hedef Odaklı Saldırı Grupları

27 Nisan 2017 Symantec Corp. Internet Security Thread Report, Vol: 22



**TBD KAMU-BİB**

Kamu Bilişim Platformu-19

26-29 Ekim 2017

#DigitalDevlet

Dijital Türkiye ve Siber Dünya  
Siber Güvenlikte Milli Hedeflerimiz

# SİBER GÜVENLİK ve MİLLİ GÜVENLİK

**Milli Güvenlik:** Devletin milli varlığına, bekasına ve güvenliğine yönelik tehditlere karşı tedbirler almak için **bölgesel** ve **küresel** ortamın izlenerek **tehdit** ve **fırsat**ların tespit edilmesi ile bu hususlara uygun siyasetin belirlenmesini ve en uygun politikaların uygulanmasını sağlayacak **süreç ve unsurlar** (MGK)\*



\* <http://www.mgk.gov.tr/index.php/milli-guvenlik-kurulu/genel-bilgi>

\*\* <http://www.nato.int/docu/review/2017/Also-in-2017/nato-priority-spending-success-cyber-defence/EN/index.htm>

# Türkiye'de Siber Güvenliğin Kısa Geçmişi

2012

2013

2014

2016

2017

Ekim 2012

Ulusal Siber Güvenlik Çalışmalarının Koordinasyon ve Yönetimine İlişkin Bakanlar Kurulu Kararı

Şubat 2013

TR-CERT Kuruluşu Onaylandı

Aralık 2012

2013-2014 Siber Güvenlik Strateji ve Eylem Planı (SGEP) Bakanlar Kuruluna sunuldu

Mart 2013

2013-2014 SGEP Bakanlar Kurulu'na onaylandı

May 2013

TR- CERT hk. İkincil Düzenlemeler

Haziran 2013

Siber Güvenlik Kurulu (SGK) 2. Toplantısı: 6 kritik altyapının belirlenmesi

Aralık 2013

SGK 3. Toplantısı: FIRST ve TI Üyeliği

Kasım 2013

SOME İkincil Düzenlemeleri

Ağustos 2013

Siber Savunma Komutanlığı kuruldu

Kasım 2014

Sektörel SOME'ler için rehberlerin hazırlanması

Temmuz 2014

Kurumsal SOME'ler için Rehberlerin hazırlanması

Nisan 2016

Kişisel Verileri Koruma Kanunu (#6698) Kabulü ve KVK Kurulu'nun oluşturulması

Ağustos 2016

671 Sayılı KHK ile BTK'nın siber saldırılara korunmada yetkilendirilmesi

Şubat 2016

SGK 4. Toplantısı; 2016-2019 SGEP

Haziran 2017

KVK için ikincil düzenlemeler

Temmuz 2017

Enerji sektöründeki Endüstriyel Kontrol Sistemleri (EKS) için ikincil düzenlemeler



TBD KAMU-BİB

Kamu Bilişim Platformu-19

26-29 Ekim 2017

#DigitalDevlet

Dijital Türkiye ve Siber Dünya  
Siber Güvenlikte Milli Hedeflerimiz

# Siber Güvenlik Yönetişim Modeli



Siber Güvenlik Kurulu



Kurumsal SOME'ler  
(658)\*

Sektörel SOME'ler  
(8)\*

Düzenleyici Denetleyici Kurum

Bakanlık

iik

Kurumsal SOME'ler

Özel Sektör'deki Sektörel SOME'ler

BTK



BDDK



SPK



EPDK



Yerel Yönetimler  
(1397)

Diğer Kurumlar

Kamu Özel

TRD KAMU-BİB  
RSI : İlgili / İlişkili Kurum  
(\* ) 08.05.2017 itibari ile

#DigitalDevlet

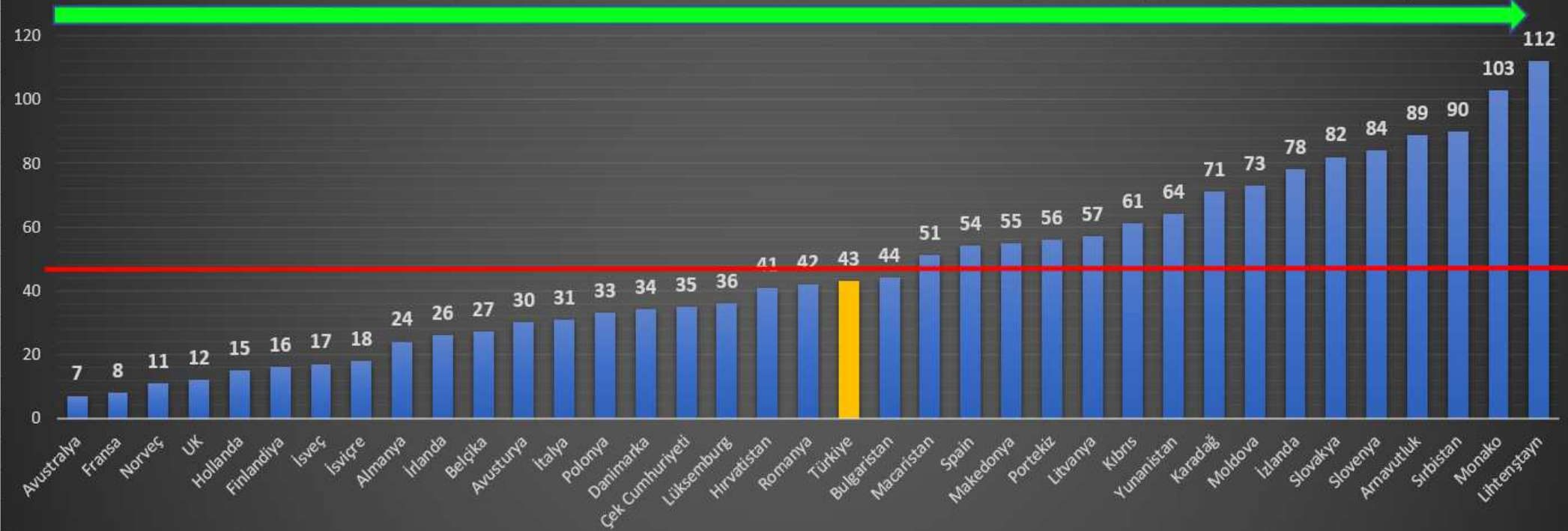
ve Siber Dünya  
Siber Güvenlikte Milli Hedeflerimiz



# Siber Güvenlik – Küresel Ölçümler

193 Ülke

## Küresel Siber Güvenlik Endeksi - Avrupa 2017 (Ülke Sıralamaları)



TBD KAMU-BİB

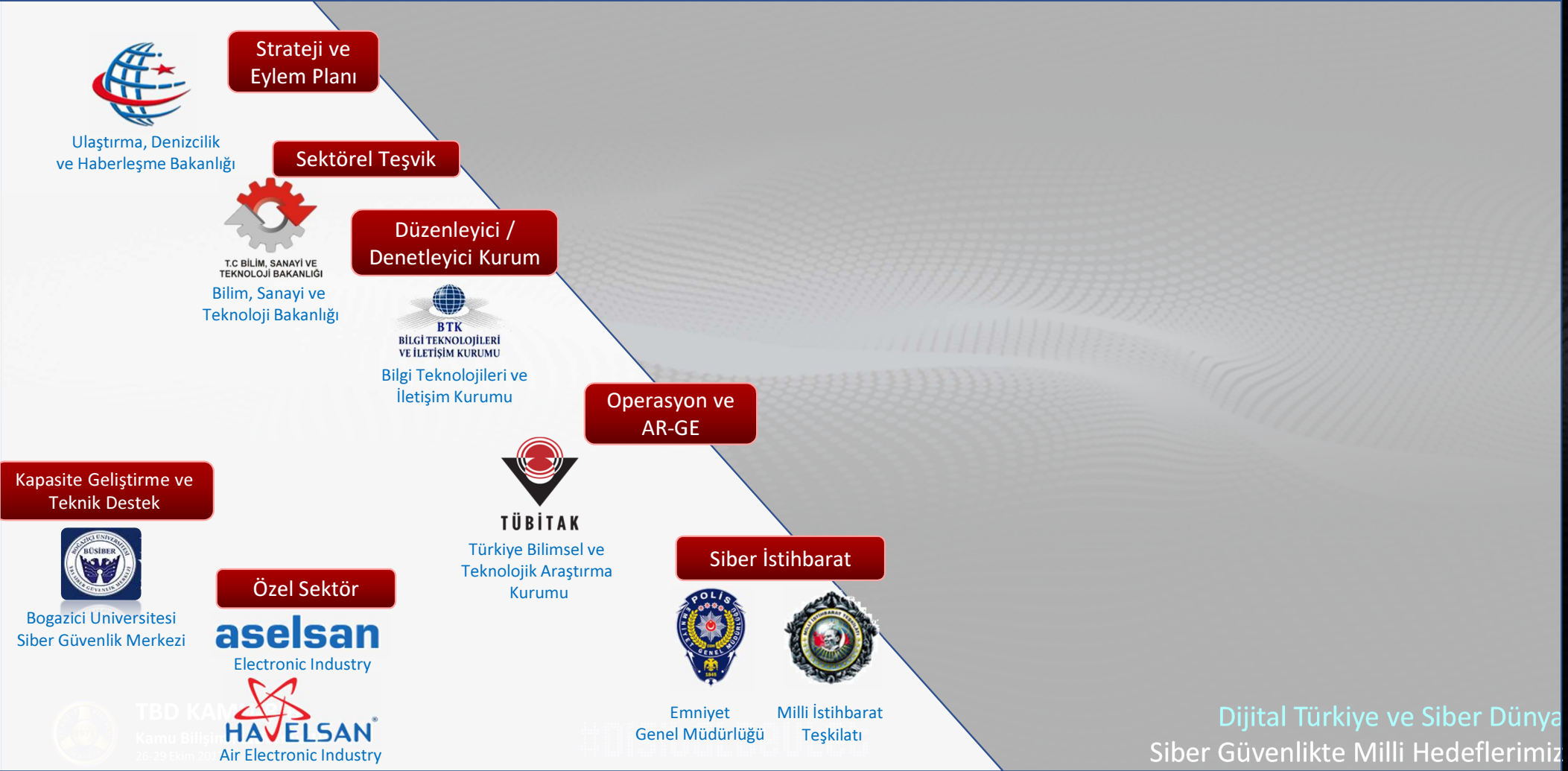
Kamu Bilişim Platformu-19

26-29 Ekim 2017

#DigitalDevlet

Dijital Türkiye ve Siber Dünya  
Siber Güvenlikte Milli Hedeflerimiz

# Siber Güvenlik Üstyapısı Yakın Gelecek Planları





# Siber Güvenlik Üstyapısı Yakın Gelecek Planları



## Siber güvenliğe tek çatı emri

16 Şubat 2017 - 22:49 | Son Güncelleme : 17 Şubat 2017 - 10:3

**CUMHURBAŞKANLIĞI, siber güvenlik alanında farklı kurumlarda yürütülen çalışmalarını tek çatı altında toplamak için çalışma başlattı.**

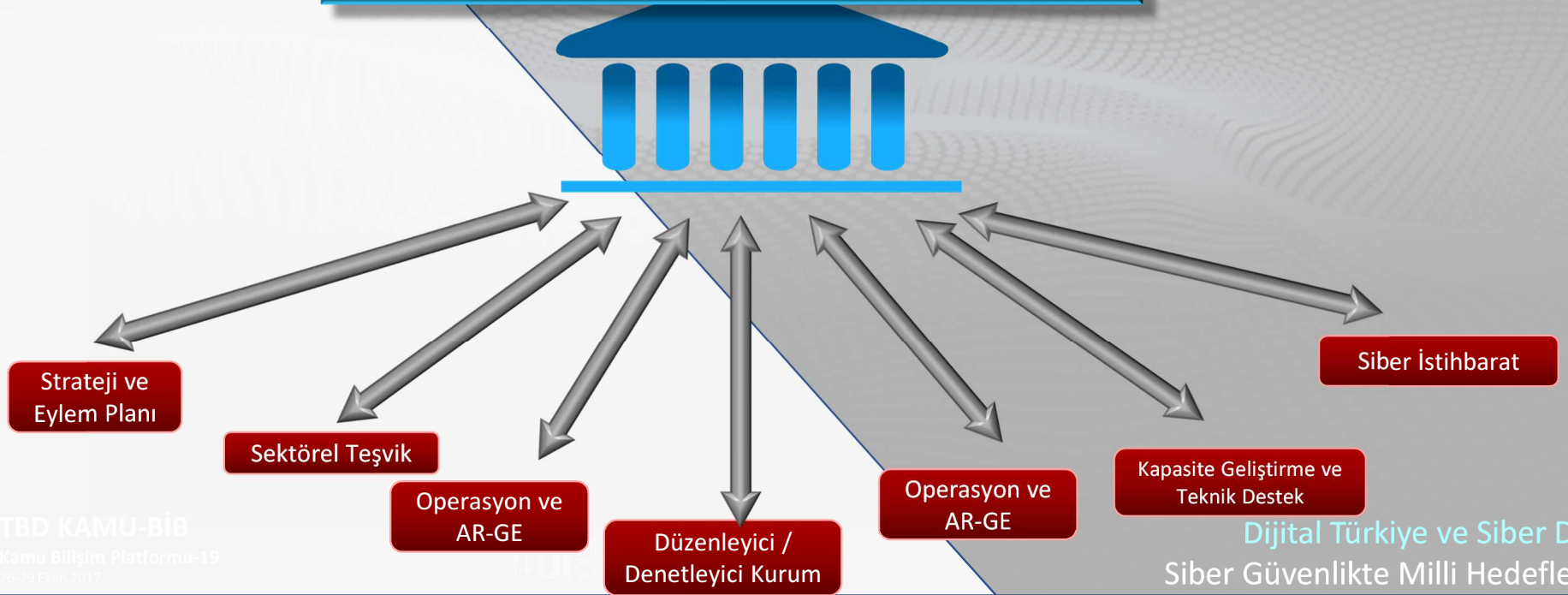


Cumhurbaşkanı Tayyip Erdoğan'ın talimatıyla başlatılan çalışmalar kapsamında, siber güvenlik altyapısının yerleştirilmesi, durum analizi yapılması ve alınması gereken tedbirler ortaya konulacak. Cumhurbaşkanı Erdoğan, FETÖ'nün 15 Temmuz darbe girişiminin ardından kurmaylarına siber güvenlik altyapısının incelenmesi için talimat verdi. Devlet Denetleme Kurulu ve Erdoğan'ın teknoloji kurmaylarının yer aldığı çalışma kapsamında Bilim, Sanayi ve Teknoloji Bakanlığı, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu ile TÜBİTAK gibi kurumlarda ayrı ayrı yapılan siber güvenlik çalışmalarının tek çatı altında birleştirilmesi planlanıyor.

<http://www.hurriyet.com.tr/siber-guvenlige-tek-cati-emri-40368316>

# Siber Güvenlik Üstyapısı Yakın Gelecek Planları

- ✓ Siber güvenlikte en üst seviye **Koordinasyon**
- ✓ **Milli Çözümler** 'e en yüksek destek (Donanım/Yazılım)
- ✓ Nitelikli insan kaynağı **Kapasite Geliştirme**



# Yakın Dönem Tamamlanan Çalışmalar

**Kişisel Verileri Koruma Kurulu'nun**  
Oluşturulması  
30 Ocak 2017



**Ulusal E-Posta Sistemi** duyuruldu  
07 Ağustos 2017

## **Kamu Güvenli Ağı**

Mevzuat: 21 Haziran 2017  
Dahil Olan Kurumlar: % 23  
Hedef: Aralık 2018



## **E-Devlet ve Siber Güvenlik CIO Kurulu**

Başkan : Başbakanlık Müsteşarı  
Katılımcılar: Her Bakanlığın İlgili Müsteşar Yardımcısı  
Periyot : Düzenli olarak, her ay (Mart 2017'den bu yana)  
Amaç : Üst Seviye İzleme ve Koordinasyon

<http://www.hurriyet.com.tr/milli-e-posta-sistemi-geliyor-40542359>  
<http://www.edevlet.gov.tr/wp-content/uploads/2017/08/03.08.2017-e-Devlet-Koordinasyon.pdf>  
<http://www.edevlet.gov.tr/2017/08/04/agustos-ayi-e-devlet-koordinasyon-toplantisi-gerceklestirildi/>

**Dijital Türkiye ve Siber Dünya**  
Siber Güvenlikte Milli Hedeflerimiz

# Yakın Dönem Tamamlanan Çalışmalar

**Kamu Entegre Veri Merkezi**  
(Fizibilite Aşamasında)



**Havelsan**  
**Siber Savunma Teknoloji Merkezi**  
(SİSATEM)  
23 Mart 2016



**STM Siber Füzyon Merkezi**  
17 Mayıs 2016

**TSK Siber Savunma Komutanlığı**  
Siber Savunma Operasyon Merkezi  
11 Temmuz 2017



**TBD KAMU-BİB**

Kamu Bilişim Platformu-19  
26-29 Ekim 2017

#DigitalDevlet

Dijital Türkiye ve Siber Dünya  
Siber Güvenlikte Milli Hedeflerimiz

# Yakın Dönem Hedeflenen Çalışmalar

## Tüm Kamu Kurumlarında ISO 27001 Sertifikasyonu

Hedef: 31 Aralık 2018



## Siber Güvenlik Uzmanı Yetiştirilmesi

Hedef: 31 Aralık 2018

## Tüm Kamu Kurumlarından Siber Güvenlik Testleri

Hedef: 31 Aralık 2017

**Kapsam:** Sistem ve Network Penetrasyon Testleri  
Kaynak Kod Analizi, DDoS, Sosyal Mühendislik ...



**TBD KAMU-BİB**

Kamu Bilişim Platformu-19

26-29 Ekim 2017

#DigitalDevlet

Dijital Türkiye ve Siber Dünya  
Siber Güvenlikte Milli Hedeflerimiz

# E-DEVLET'TEN SİBER GÜVENLİK'E EKOSİSTEM

## SİBER TEHDİT

## HEDEF

## ELEKTRONİK YAPILAR

## YÖNETİM



## BİLGİ İŞLEM DAİRE BAŞKANLIKLARI



TBD KAMU-BİB

Kamu Bilişim Platformu-19

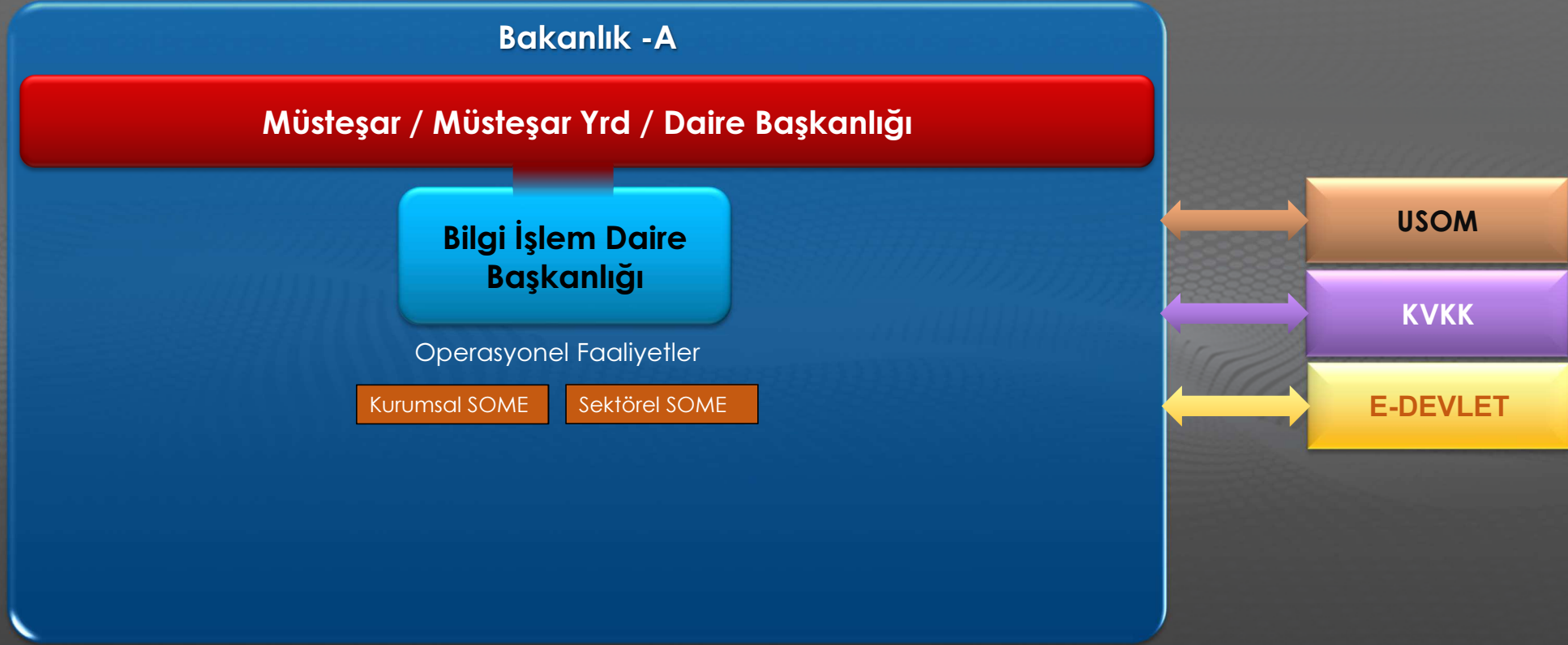
26-29 Ekim 2017

#DigitalDevlet

Dijital Türkiye ve Siber Dünya  
Siber Güvenlikte Milli Hedeflerimiz

# BÜTÜNCÜL, ETKİN ve YETKİN İDARİ YAPI

## MEVCUT DURUM



TBD KAMU-BİB

Kamu Bilişim Platformu-19

26-29 Ekim 2017

#DigitalDevlet

Dijital Türkiye ve Siber Dünya  
Siber Güvenlikte Milli Hedeflerimiz

# BÜTÜNCÜL, ETKİN ve YETKİN İDARİ YAPI

## ÖNERİLEN İDARİ MODEL



TBD KAMU-BİB

Kamu Bilişim Platformu-19

26-29 Ekim 2017

#DigitalDevlet

Dijital Türkiye ve Siber Dünya  
Siber Güvenlikte Milli Hedeflerimiz



# «MİLLİ» SİBER GÜVENLİK

- Yazılımların **tam kaynak kodu** olmalı:
  - AKK şart değil (source-available / shared-source) ama kaynak koduna sahip olunmayan karakutu bileşen içermemeli
- **Milli özel sektör** tarafından hazırlanmalı:
  - Devlet sadece **altyapı** ve **ARGE**'yi hazırlamalı
  - Yazılım geliştirmede **devlet özel sektörle rekabet yapmamalı**:
    - Devlet, yazılım geliştirme yerine bunlara altlık olacak **çerçeveler**, kütüphaneler ve ulusal **AR-GE** çalışmalarını gerçekleştirmeli, standartları belirlemeli
    - Milli özel sektör bunları kullanarak **sektörel** (sağlık, eğitim, ...) ve **yatay** (EBYS) yazılımlar geliştirmeli
    - 8227 sayılı Kamu İhale Kanunu **İstisnalar** - 3. maddesi, özel sektördeki **rekabeti** destekleyecek şekilde yeniden ele alınmalı
    - Sektör **seviyelendirilerek** kategorilere ayrılmalı
    - **Kamudaki pazar** bu kategorilerin gelişmesini sağlamalı
- **Sürdürülebilir** modeli olmalı:
  - Sadece AR-GE teşvikleri ile yalnız bırakılmamış **ürün haline gelmiş çözümler**
- **Teknik, idari, mali ve hukuki** açıdan devlet tarafından desteklenmeli



**MİLLİ ÜRÜN**'lerin kamuda **ulusal politika** olarak istisnasız kullanılması

### «ÖNCE BİZ KULLANACAĞIZ !»

Kamuda **Yaygınlaştırma Politikası**:

- Akreditasyon ve sertifikasyon ile kamu alımlarında «**Şirket Derecelendirme**»
- Teşvik Modeli: **ARGE** → Başarılı çalışmalarda «**Ürünleştirme**» → Pilot Uygulamalar → Destek ve Geliştirme Altyapısı → Kamuda Konumlandırma
- Birinci katman mevcut ürünler, ikinci katmanlar **milli ürünler**
- Geçiş ve olgunlaşma sürecinden sonra her iki katmanda milli ürün kullanımı
- Her segment için en az iki **milli çözüm politikası**
- **Bölgesel Yaygınlaştırma**



# TBD KAMU-BİB

Kamu Bilişim Platformu-19

26-29 Ekim 2017



## Teşekkür Ederim

**Dijital Türkiye ve  
Siber Dünya:  
Siber Güvenlik 'te  
Milli Hedeflerimiz**

**Mustafa AFYONLUOĞLU**

Siber Güvenlik, E-Yönetişim ve E-Devlet Kıdemli Uzmanı

**E-Posta:** [afyonluoglu@gmail.com](mailto:afyonluoglu@gmail.com)

**Web:** [afyonluoglu.org](http://afyonluoglu.org)

**LinkedIn:** <http://linkedin.com/in/afyonluoglu>

**Twitter:** <http://twitter.com/#!/afyonluoglu>



#DİJİTALDEVLET