Türkiye'de ve Dünyada

Siber Güvenlik

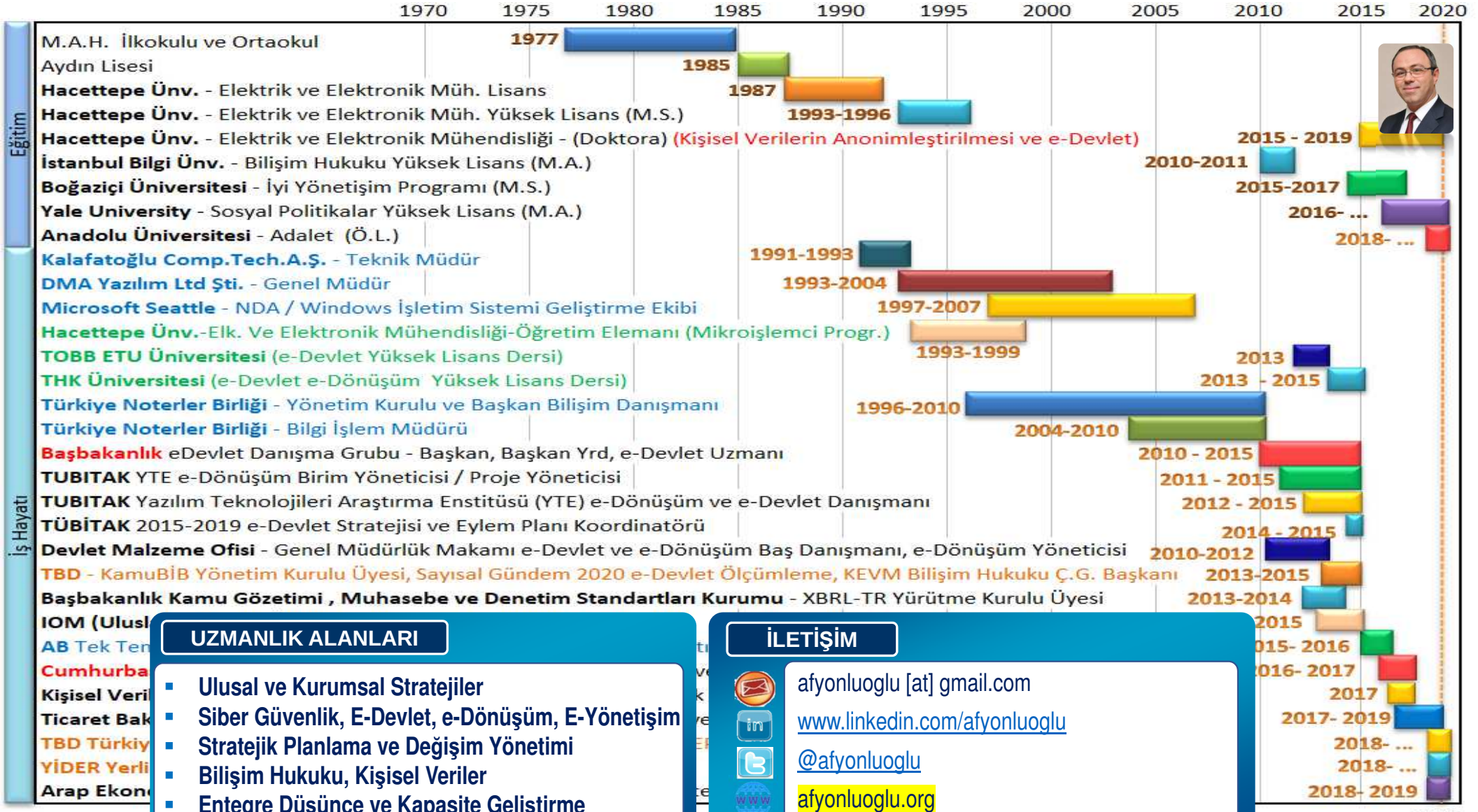
Kamu Sektöründe İnovasyon

ARGÜDEN
GOVERNANCE
ACADEMY

Good Governance for
Quality of Life

MUSTAFA AFYONLUOĞLU

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



UZMANLIK ALANLARI

- Ulusal ve Kurumsal Stratejiler
- Siber Güvenlik, E-Devlet, e-Dönüşüm, E-Yönetişim
- Stratejik Planlama ve Değişim Yönetimi
- Bilişim Hukuku, Kişisel Veriler
- Entegre Düşünce ve Kapasite Geliştirme

İLETİŞİM

afyonluoglu [at] gmail.com

www.linkedin.com/afyonluoglu

@afyonluoglu

afyonluoglu.org

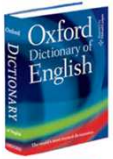
Gündem


Tanımlar ve Kapsam
1
Kritik Altyapılar ve Siber Güvenlik
2
Siber Güvenlik ve Yönetişim
3
Siber Güvenlik Stratejileri
4
Siber Güvenlik ve Mevzuat
5
Siber Güvenlik için Kaynaklar
6

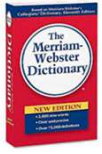
Gündem


Tanımlar ve Kapsam
1
Kritik Altyapılar ve Siber Güvenlik
2
Siber Güvenlik ve Yönetişim
3
Siber Güvenlik Stratejileri
4
Siber Güvenlik ve Mevzuat
5
Siber Güvenlik için Kaynaklar
6

Siber Güvenlik Tanımı



The Oxford Dictionaries : Elektronik verilerin suçlular tarafından veya yetkisiz kullanımına karşı korunma durumu veya bunu başarmak için alınan önlemler



The Merriam – Webster **:** Bilgisayar veya bilgisayar sistemini (Internet'te olduğu gibi) yetkisiz erişime veya saldırıya karşı korumak için alınan önlemler

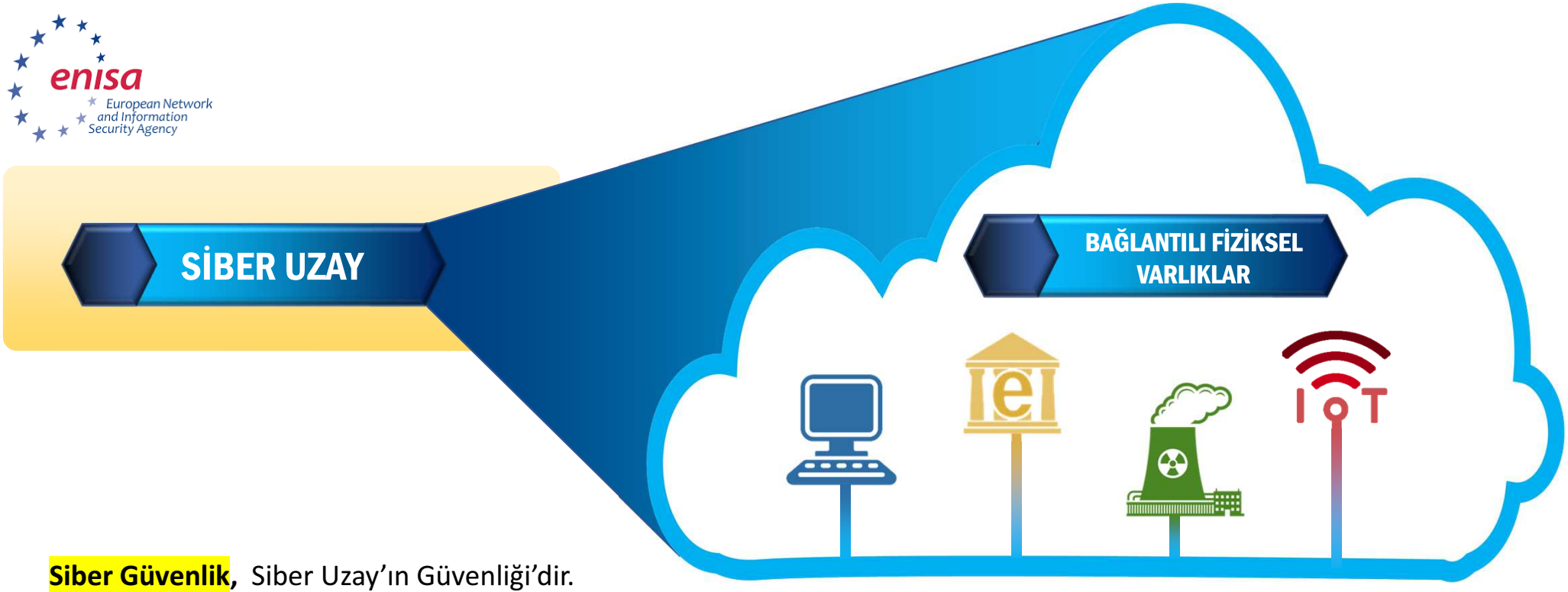
Cisco **:** Siber güvenlik, sistemleri, ağları ve programları, hassas bilgilere erişmeye, onları değiştirmeye veya yok etmeye yönelik dijital saldırılardan koruma pratiğidir.

ISO : Bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin siber uzayda korunması
CIA : Confidentiality, Integrity, Availability
KGB: Kullanılabilirlik, Gizlilik, Bütünlük *(TSE ISO/IEC-27001: Bilgi Güvenliği Yön.Sistemi)*

ITU : Siber çevreyi, organizasyonu ve kullanıcının varlıklarını korumak için kullanılabilecek araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, kılavuzlar, risk yönetimi yaklaşımları, eylemler, eğitim, en iyi uygulamalar, güvence ve teknolojiler bütünü

NIST : Siber alanı siber saldırılardan koruma veya korunma yeteneği

Siber Güvenlik Tanımı

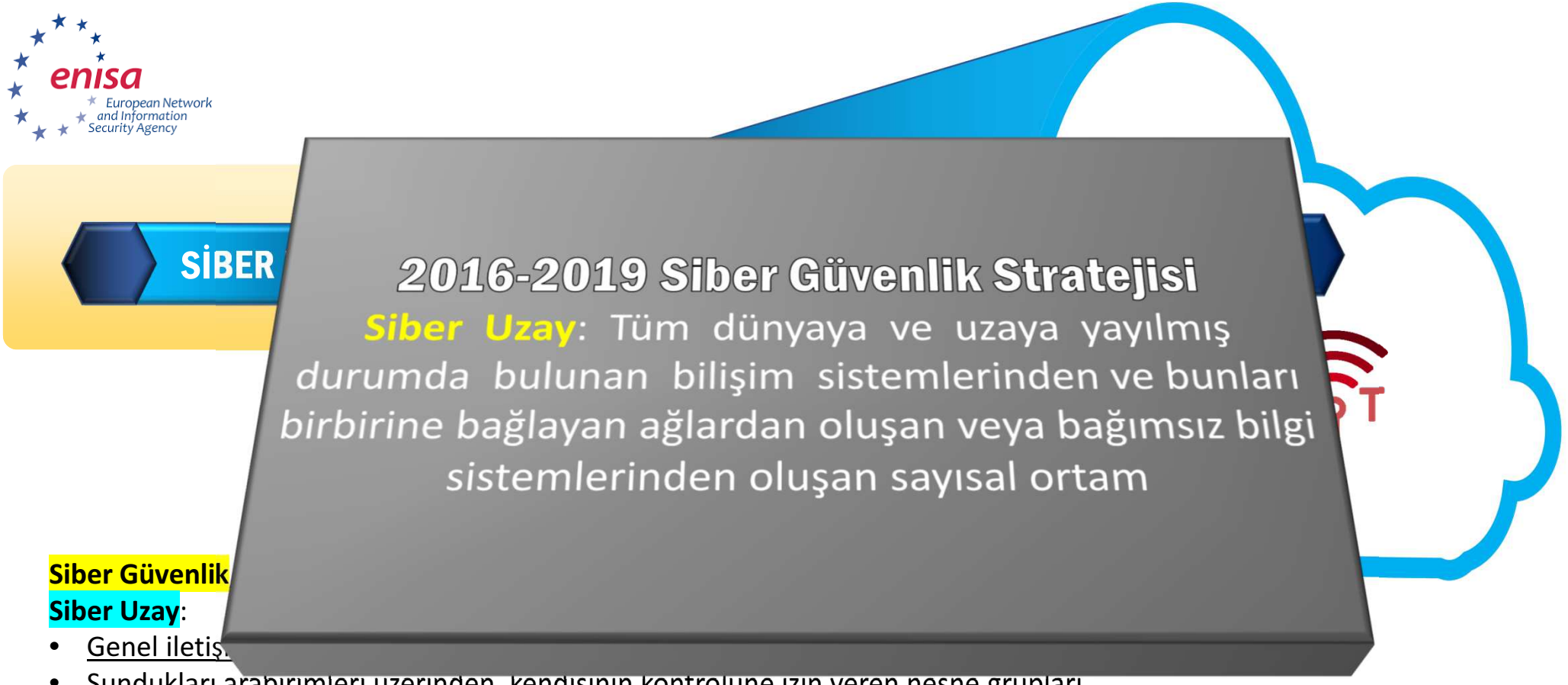


Siber Güvenlik, Siber Uzay'ın Güvenliği'dir.

Siber Uzay:

- Genel iletişim ağı üzerinden erişilebilen nesneler ve aralarındaki bağlantılar ve ilişkiler,
- Sundukları arabirimleri üzerinden kendisinin kontrolüne izin veren nesne grupları
- Uzaktan erişilebilen ve/veya yönetilebilen veriler

Siber Güvenlik Tanımı



Siber Güvenlik

Siber Uzay:

- Genel iletiş
- Sundukları arabirimleri üzerinden kendisinin kontrolüne izin veren nesne grupları
- Uzaktan erişilebilen ve/veya yönetilebilen veriler

Siber Güvenlik Tanımı

ENISA 2015 Aralık: «Definition of Cybersecurity : Gaps and overlaps in standardisation»

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 fırsatların 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

- **Şubat 2016**: Avrupa Birliği ile siber savunma işbirliği konusunda Teknik Düzenleme imzalandı.
- **Temmuz 2016**: Kara, Hava, Deniz ve Uzay'dan sonra **Siber Alan** 5. operasyonel alanıdır.
- **Aralık 2016**: **Siber savunma**, NATO'nun toplu savunma alanındaki temel görevlerinden biridir.
  - Uluslararası hukuk siber alanda da uygulanmalıdır.
  - NATO, **siber eğitim** ve tatbikat yeteneklerini geliştirecektir.

Gündem


Tanımlar ve Kapsam
1
Kritik Altyapılar ve Siber Güvenlik
2
Siber Güvenlik ve Yönetişim
3
Siber Güvenlik Stratejileri
4
Siber Güvenlik ve Mevzuat
5
Siber Güvenlik için Kaynaklar
6

Kritik Altyapılar

TÜRKİYE'DE KRİTİK ALTYAPILAR

20/06/2013 tarih, 2 sayılı Siber Güvenlik Kurulu kararı
2016-2019 Siber Güvenlik Stratejisi

KRİTİK ALTYAPILAR

İşlediği bilgi/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda,

- **Can kaybına,**
- **Büyük ölçekli ekonomik zarara,**
- **Ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek**

bilişim sistemlerini barındıran altyapılar

DÜNYADAKİ KRİTİK ALTYAPI YAKLAŞIMLARI

ABD Başkanlık Politikası Yönergesi: Kritik Altyapı Güvenliği ve Esnekliği

- ENERJİ
- FİNANSAL SERVİSLER
- HABERLEŞME
- ULAŞIM SİSTEMLERİ
- SU YÖNETİMİ
- KRİTİK KAMU HİZMETLERİ
- BİLGİ TEKNOLOJİLERİ
- SAĞLIK ve HALK SAĞLIĞI
- TİCARİ TESİSLER
- GIDA ve TARIM
- ACİL SERVİSLER
- SAVUNMA SANAYİ
- BARAJLAR
- KRİTİK İMALAT
- KİMYA ENDÜSTRİSİ
- NÜKLEER REAKTÖRLER ve ATIKLAR

PPD 21: Presidential Policy Directive 21 -Critical Infrastructure Security and Resilience: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

DÜNYADAKİ KRİTİK ALTYAPI YAKLAŞIMLARI

Kanada 2014-2017 Kritik Altyapılar Eylem Planı (Şubat 2013)

- ENERJİ ve UTILITY HİZMETLER (Su, doğalgaz, ısınma vd.)
- FİNANSAL SERVİSLER
- BİLGİ ve İLETİŞİM TEKNOLOJİLERİ
- ULAŞIM SİSTEMLERİ
- SU YÖNETİMİ
- KRİTİK KAMU HİZMETLERİ
- KRİTİK İMALAT
- SAĞLIK
- GIDA
- KAMU GÜVENLİĞİ

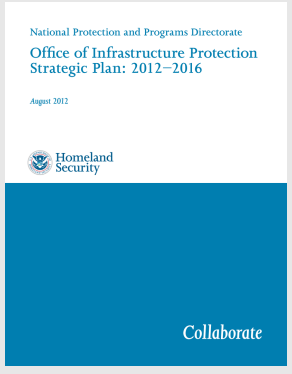
DÜNYADAKİ KRİTİK ALTYAPI YAKLAŞIMLARI

Avrupa Birliği - Kritik Altyapılar Koruma Avrupa Programı - EPCIP (Aralık 2006)

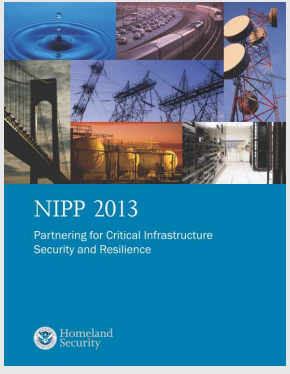
- ENERJİ
- FİNANSAL SERVİSLER
- BİLGİ ve İLETİŞİM TEKNOLOJİLERİ
- ULAŞIM SİSTEMLERİ
- SU YÖNETİMİ
- ARAŞTIRMA FAALİYETLERİ
- KİMYA ENDÜSTRİSİ
- SAĞLIK
- GIDA
- UZAY
- NÜKLEER ENDÜSTRİ

http://europa.eu/rapid/press-release_MEMO-06-477_en.pdf

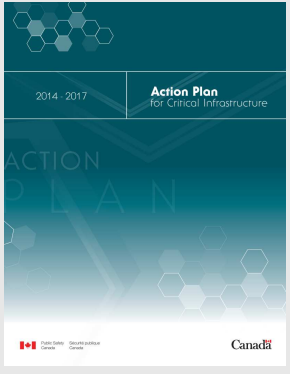
Kritik Altyapılar Strateji ve Eylem Planı



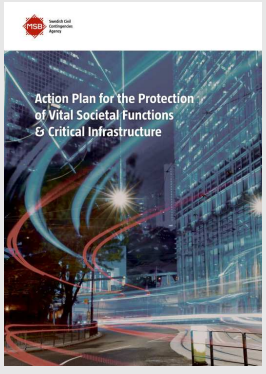
ABD 2012-2016



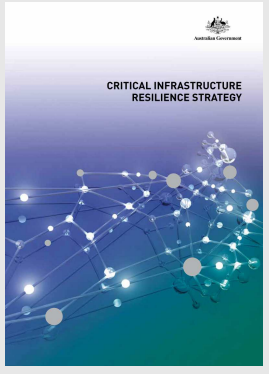
ABD 2013-2017



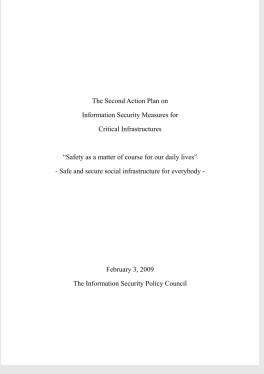
Kanada 2014-2017



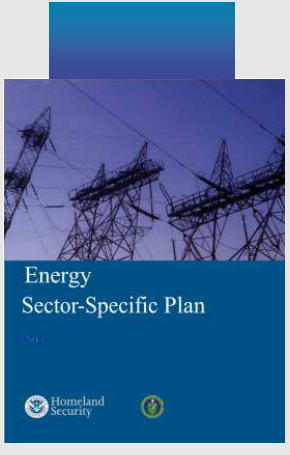
İsveç 2014

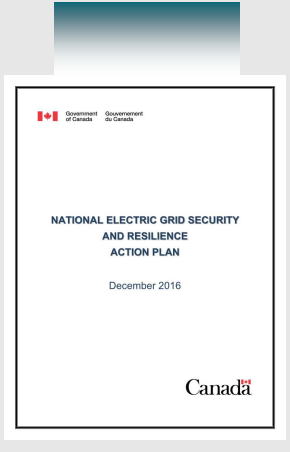


Avustralya 2010



Japonya 2009

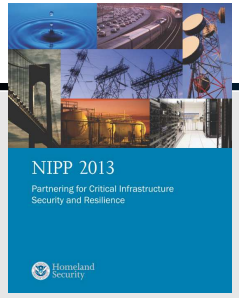


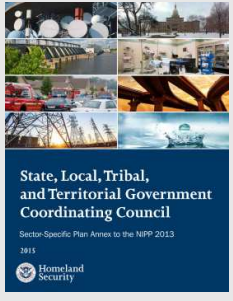


OECD 2008

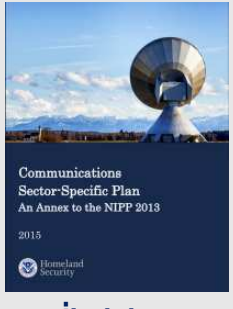
http://afyonluoglu.org/siberguvenlik/kritik-altyapilar4/

Kritik Altyapılar Stratejisi ile Bütün - Sektöre Özel Planlar

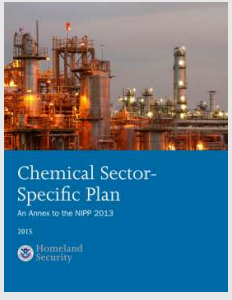




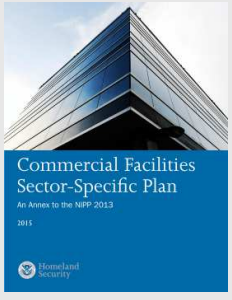
Koordinasyon



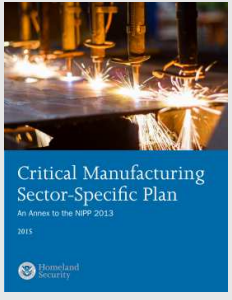
İletişim



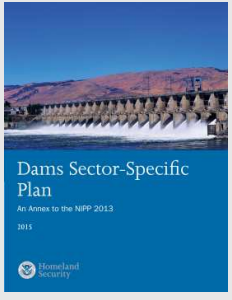
Kimya



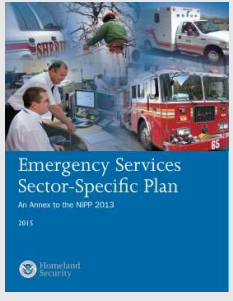
Ticaret



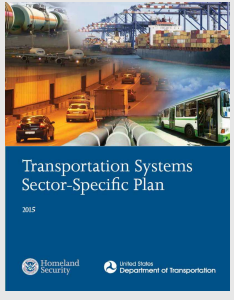
Kritik Üretim



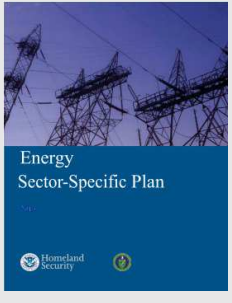
Barajlar



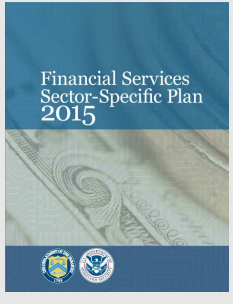
Acil Durum



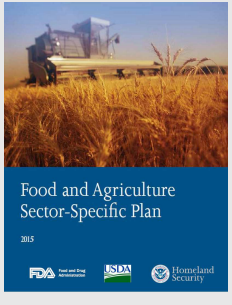
Ulaşım



Enerji

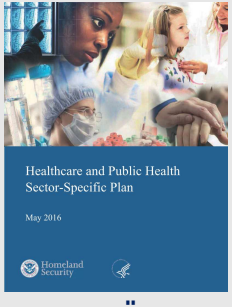


Finans

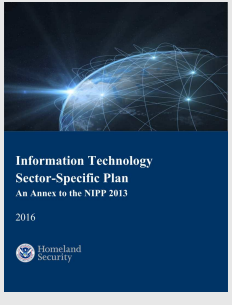


Gıda ve Tarım

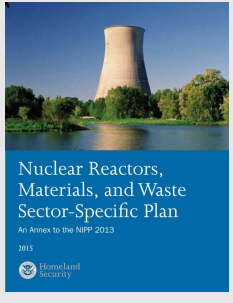
Kamu Hizmetleri



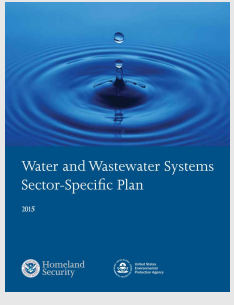
Kritik Üretim



Bilgi Teknolojileri



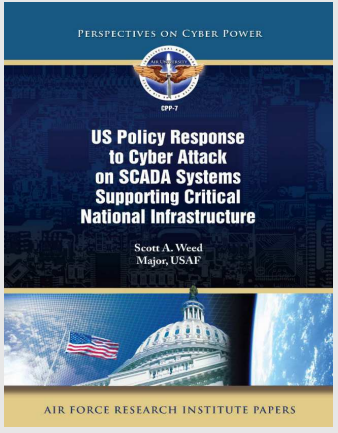
Nükleer Reaktörler ve Atıklar



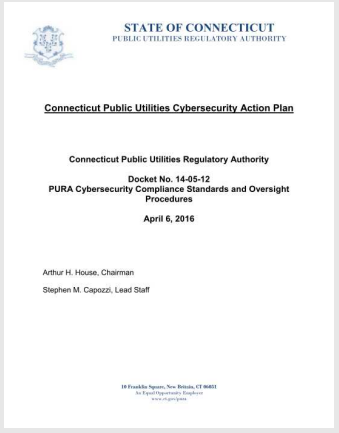
Su Yönetimi

http://afyonluoglu.org/siberguvenlik/kritik-altyapilar5/

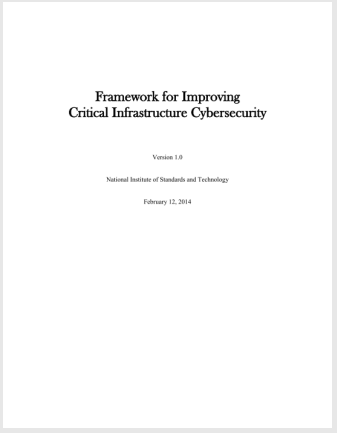
Kritik Altyapılara İlişkin Rehberler, Standartlar ve Çerçeveler



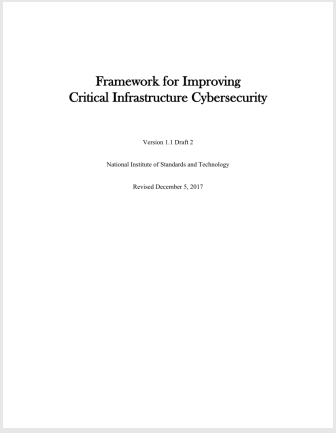
2017 US Policy Response to Cyber Attack on SCADA Systems



2016 USA-Public Utilities CyberSecurity Compliance Standards



NIST Siber Güvenlik Kritik Altyapı Çerçevesi



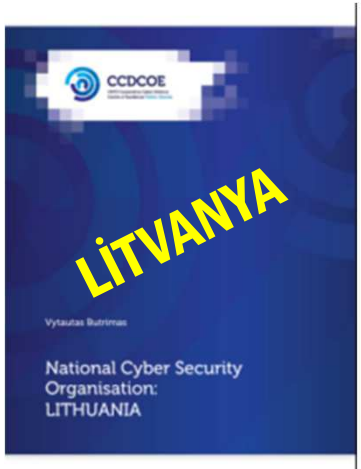
NIST CSF 1.1 (16 Nisan 2018)

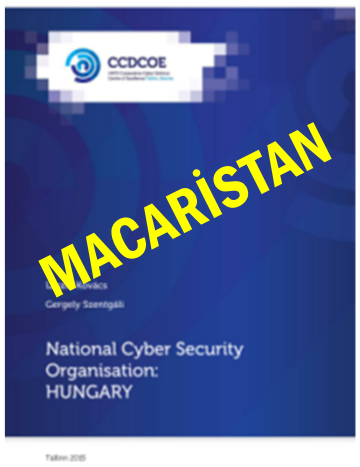
http://afyonluoglu.org/siberguvenlik/kritik-altyapilar8/
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

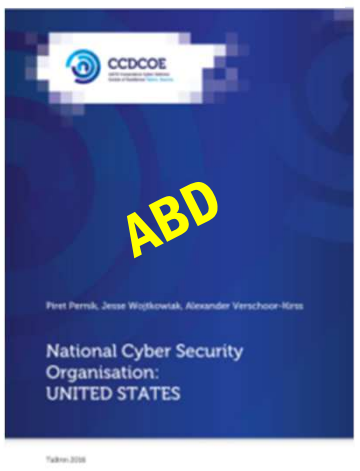
Gündem


Tanımlar ve Kapsam
1
Kritik Altyapılar ve Siber Güvenlik
2
Siber Güvenlik ve Yönetişim
3
Siber Güvenlik Stratejileri
4
Siber Güvenlik ve Mevzuat
5
Siber Güvenlik için Kaynaklar
6

NATO Üye Ülkelerin Siber Güvenlik Organizasyonel Yapıları



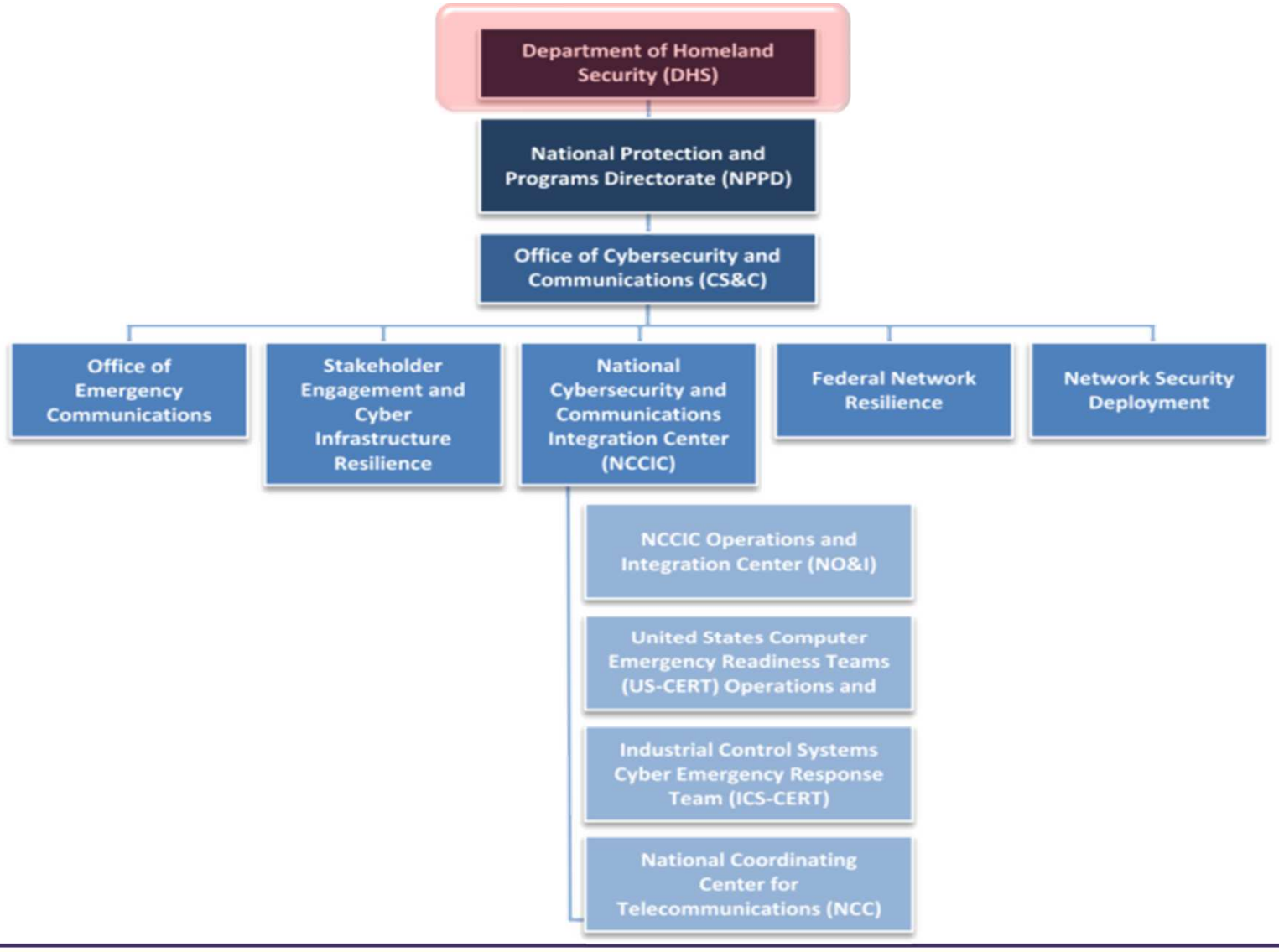




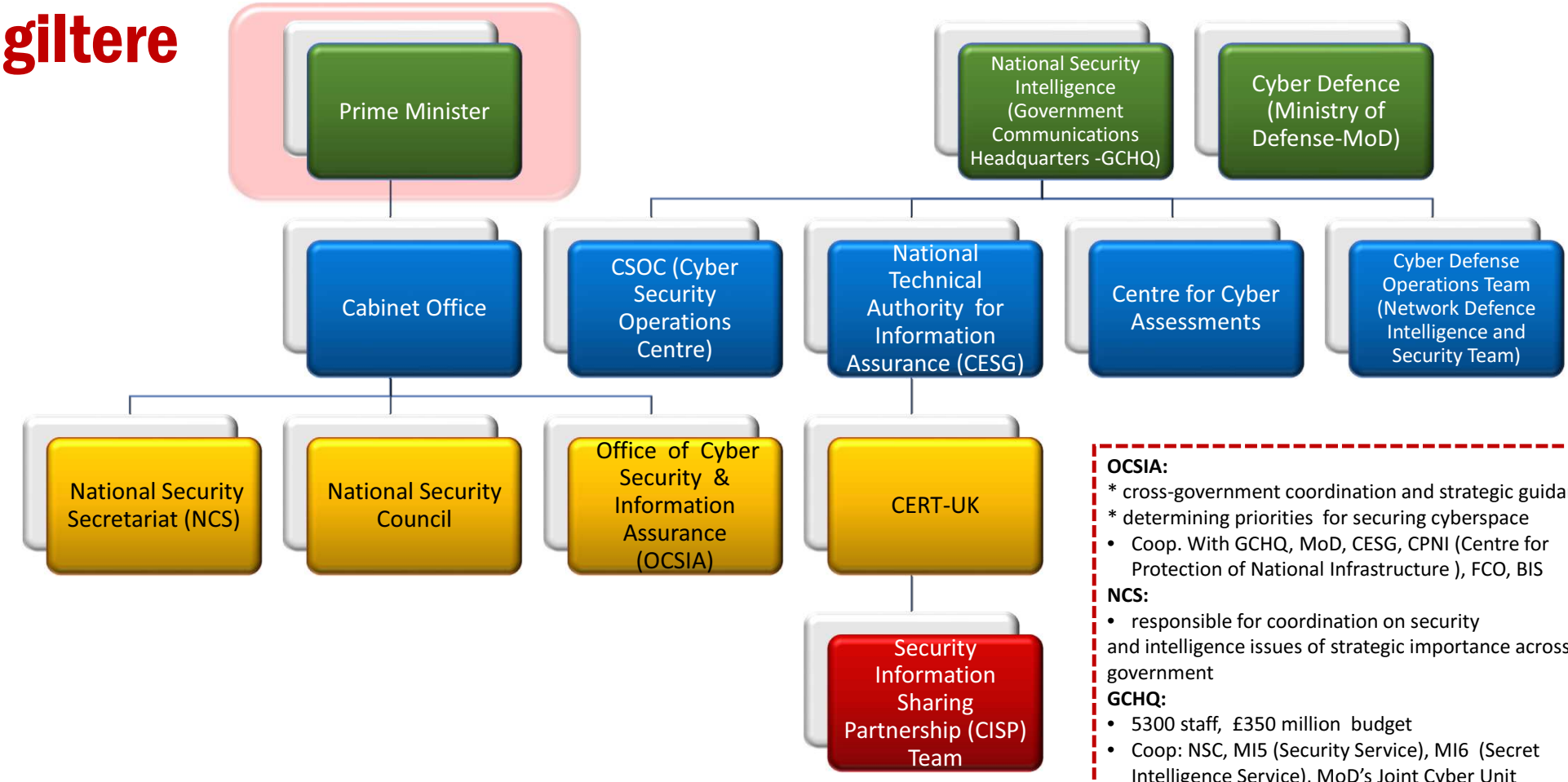
Siber Güvenlik: İdeal Ulusal Model Nasıl Olmalı?

Seviye	Hedef	Bileşenler
Politik Seviye	ÜST SEVİYE TEMSİLİYET	En üst seviyedeki siyasi lider tarafından sahiplenme
Stratejik Seviye	POLİTİKA BELİRLEME YÖNETİŞİM	• Ulusal Politikaların Belirlenmesi, Uygulama ve İzleme • Özel sektör, Üniversite, STK ve Kamu Yönetişimi • Kaynak Planlama
Operasyonel Seviye	PAYDAŞLAR ARASI İŞBİRLİĞİ	• Üst Kurullar ile İşbirliği • CIO Kurulu • Denetim
Taktik Seviye	KOORDİNASYON	• Ulusal Siber Olaylara Müdahale Merkezi • Siber Güvenlik Teknoloji Merkezi • Siber Ordu ve Siber Savunma • Siber İstihbarat
Teknik Seviye	TEKNİK BİLEŞENLER	• SOME • Siber Veri Analizi • Siber İnovasyon Merkezi • Siber Kapasite Geliştirme Merkezi • Standartlar • Rehberler • Siber Takımlar • AR-GE

ABD


Department of Homeland Security (DHS)
National Protection and Programs Directorate (NPPD)
Office of Cybersecurity and Communications (CS&C)
Office of Emergency Communications
Stakeholder Engagement and Cyber Infrastructure Resilience
National Cybersecurity and Communications Integration Center (NCCIC)
Federal Network Resilience
Network Security Deployment
NCCIC Operations and Integration Center (NO&I)
United States Computer Emergency Readiness Teams (US-CERT) Operations and
Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
National Coordinating Center for Telecommunications (NCC)

İngiltere



OCSIA:
* cross-government coordination and strategic guidance
* determining priorities for securing cyberspace
- Coop. With GCHQ, MoD, CESG, CPNI (Centre for Protection of National Infrastructure), FCO, BIS

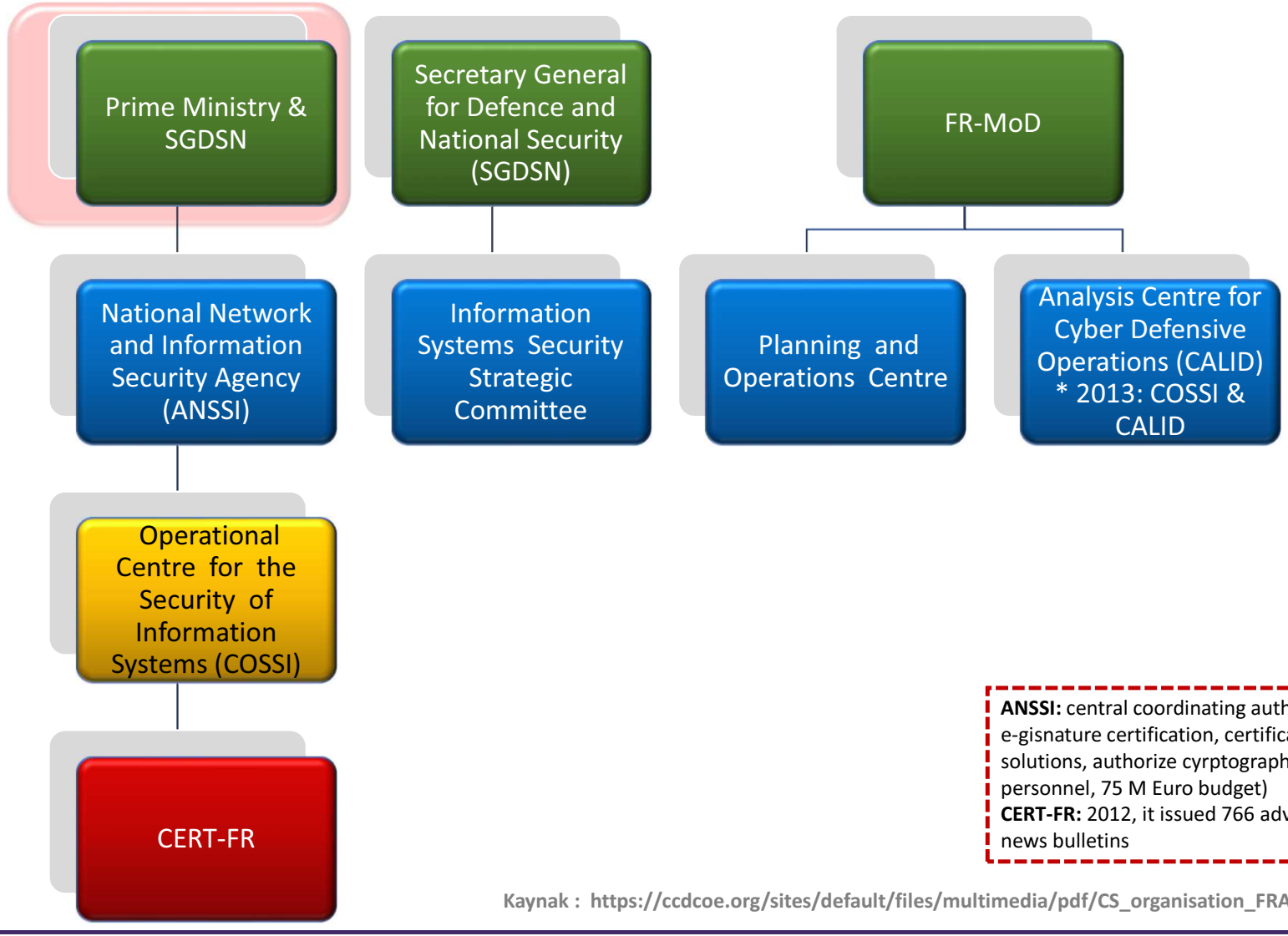
NCS:
- responsible for coordination on security and intelligence issues of strategic importance across government

GCHQ:
- 5300 staff, £350 million budget
- Coop: NSC, MI5 (Security Service), MI6 (Secret Intelligence Service), MoD's Joint Cyber Unit

MI5:
* counter-espionage, counter-intelligence, counter-proliferation, cyber and protective security

Kaynak : https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_UK_032015_0.pdf

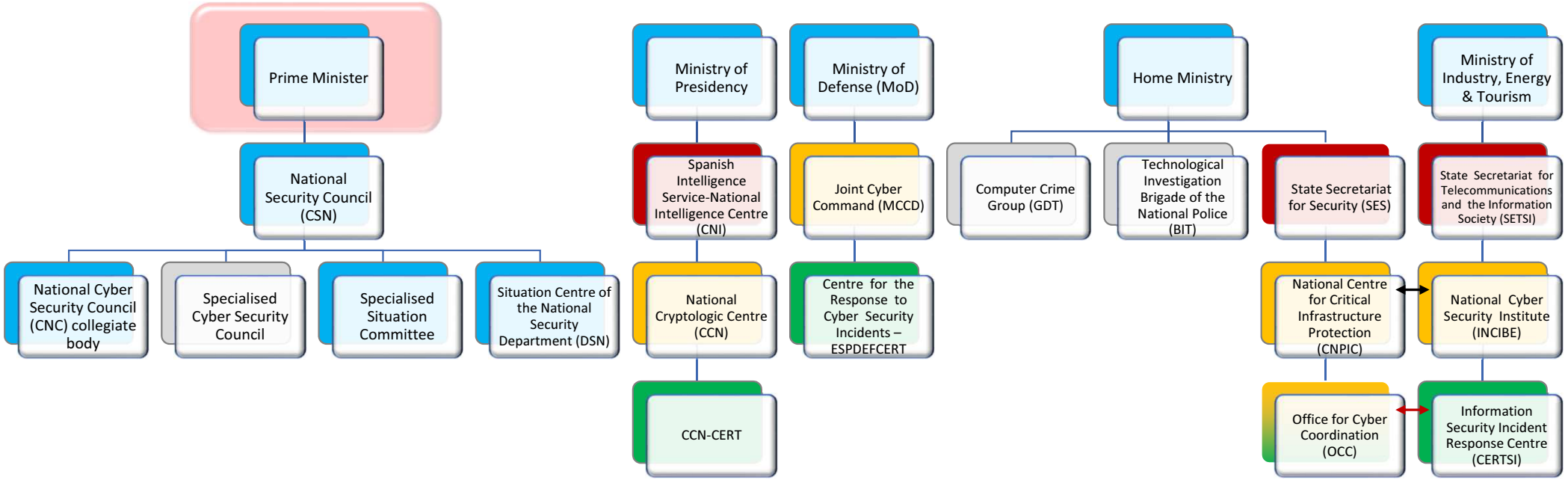
Fransa



ANSSI: central coordinating authority for cyber security, e-gisnature certification, certification of security solutions, authorize cyrptographic services (500 personnel, 75 M Euro budget)
CERT-FR: 2012, it issued 766 advices, 10 alerts and 52 news bulletins

Kaynak : https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_FRANCE_032015_0.pdf

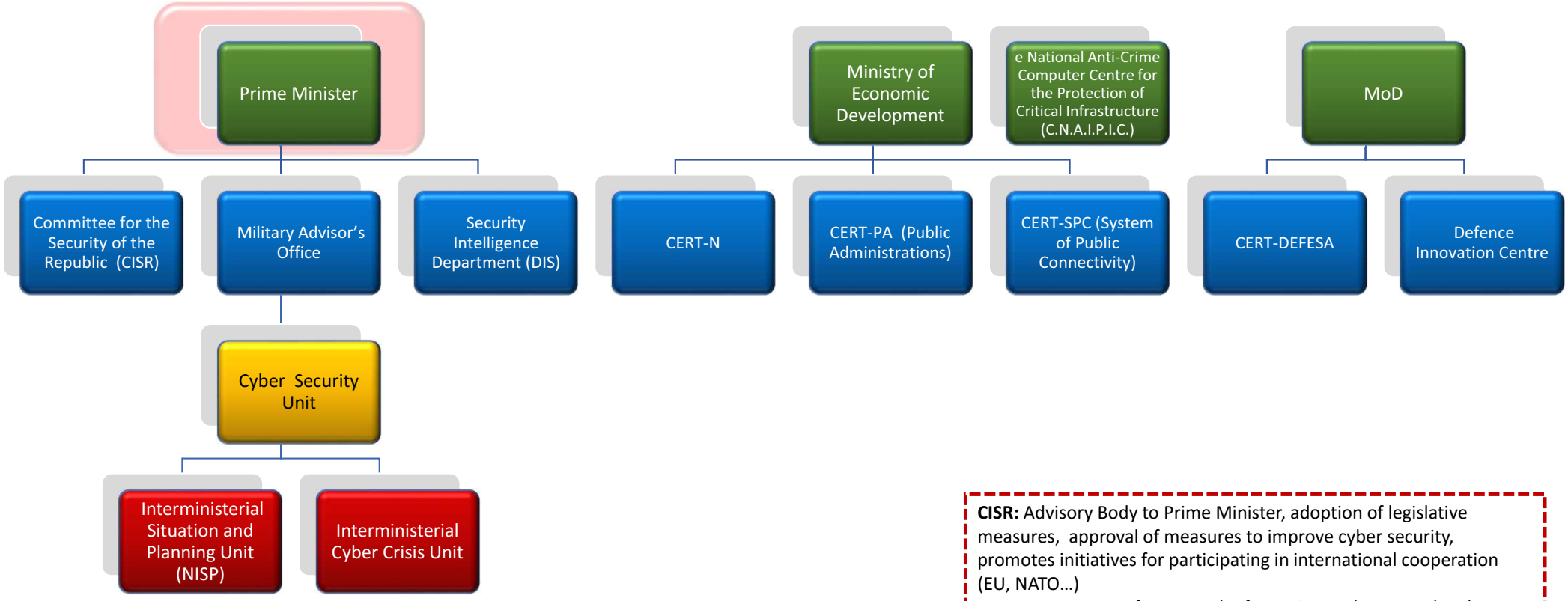
İspanya



DSN: Technical Secreteriat
SARA: System of Application and Networks for Administrations: Government & EU Network
EWS: Early-Warning System, part of SARA
CARMEN: Centre for Record Analysis and Event Mining
PILAR: Logic Computer Procedure for Risk Analysis
LUCIA: Unified List for the Coordination of Incidents and Threats
CCN-CERT provides online courses

Kaynak : https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_SPAIN_092016.pdf

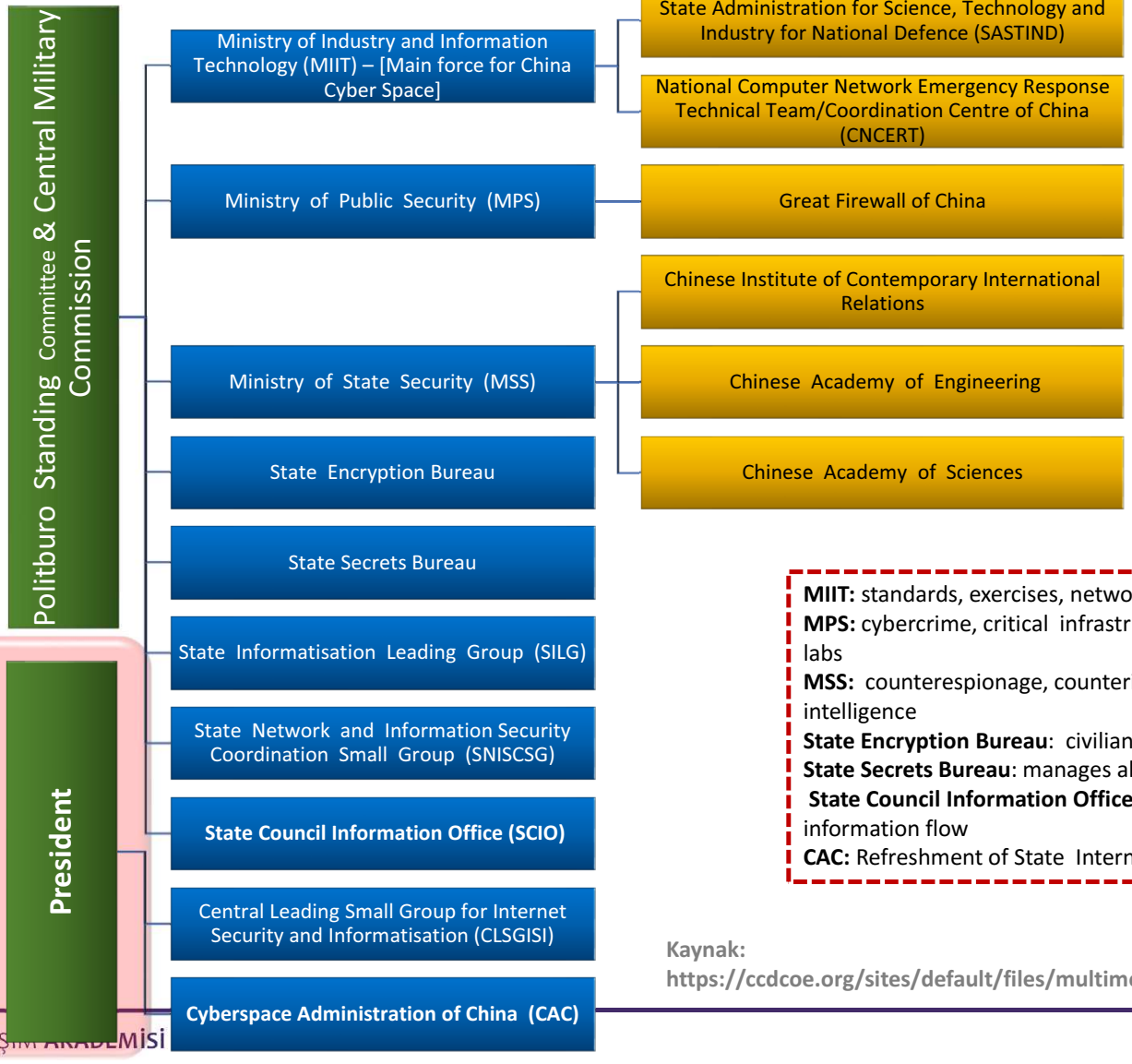
İtalya



CISR: Advisory Body to Prime Minister, adoption of legislative measures, approval of measures to improve cyber security, promotes initiatives for participating in international cooperation (EU, NATO…)
DIS: Coop - Agency for Internal Information and Security (AISI), Agency for External Information and Security (AISE), Cyber Security Unit
CERT-DIFESA: Coop NATO-NCIRC

Kaynak : https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_ITALY_032015_0.pdf

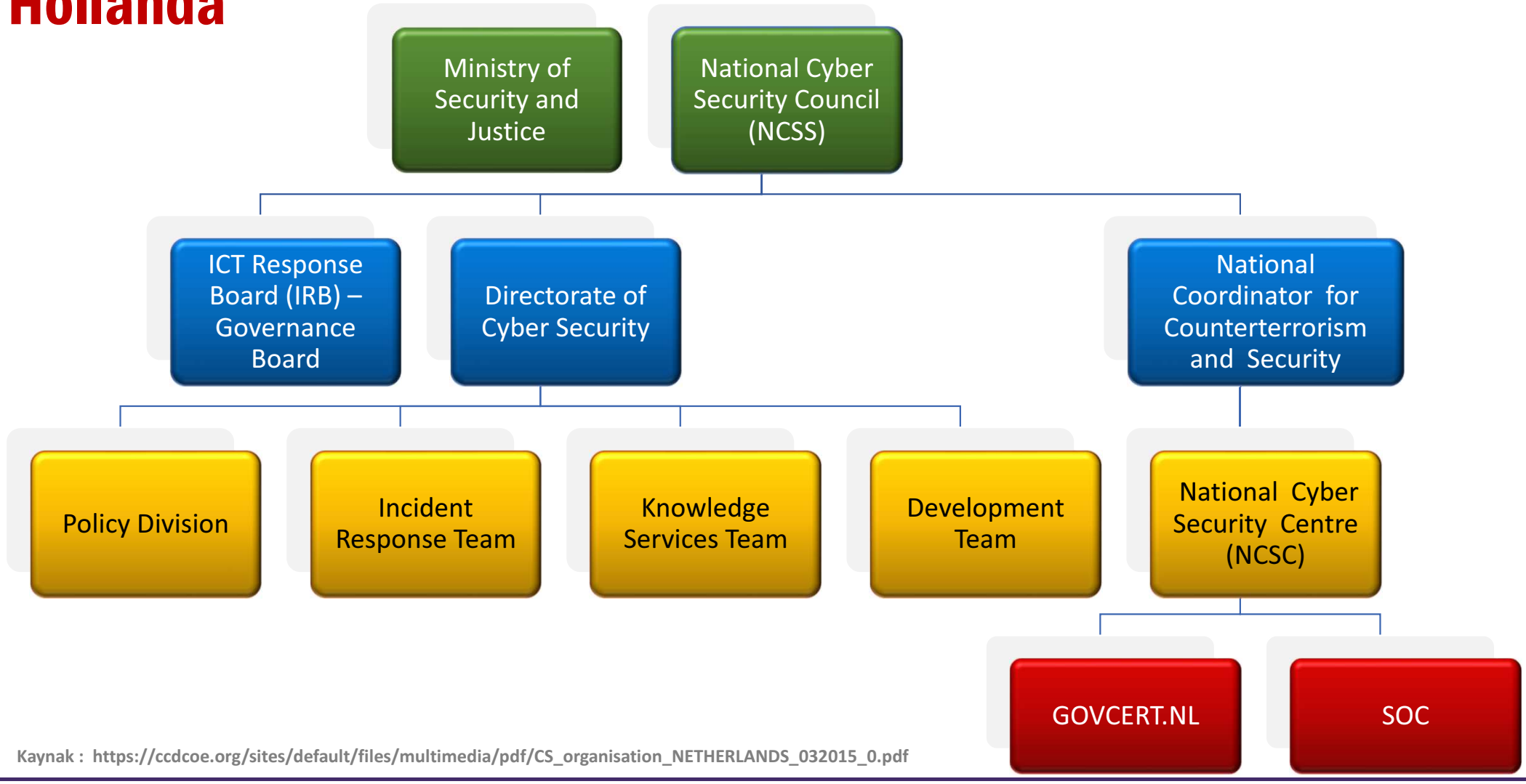
Çin



MIIT: standards, exercises, network security, information and telecoms security
MPS: cybercrime, critical infrastructure Protection, wide network of research labs
MSS: counterespionage, counterintelligence, foreign intelligence, and domestic intelligence
State Encryption Bureau: civilian and military encryption management
State Secrets Bureau: manages all classified networks
State Council Information Office (SCIO): manages the general domestic information flow
CAC: Refreshment of State Internet Information Office (SIIO)

Kaynak:
https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016_FINAL.pdf

Hollanda



Kaynak : https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_NETHERLANDS_032015_0.pdf

Kurumsal Yapılanma Tarihçesi

- **Haziran 2012** — TSK Siber Savunma Merkezi Başkanlığı kuruldu
- **Temmuz 2012** — TÜBİTAK Siber Güvenlik Enstitüsü kuruldu
- **Ekim 2012** — Siber Güvenlik Kurulu kuruldu
- **Ocak 2013** — UDHB Siber Güvenlik Dairesi kuruldu
- **Mayıs 2013** — Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) kuruldu
- **Haziran 2013** — Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı yürürlüğe girdi
- **Ekim 2013** — TSK Siber Güvenlik Komutanlığı kuruldu
- **Şubat 2014** — 5809 sayılı Elektronik Haberleşme Kanunu'na siber güvenlik maddeleri eklendi
- **Şubat 2016** — 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı onaylandı
- **Temmuz 2018** — Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Kuruldu

BİLGİGÜVENLİĞİ DERNEĞİ

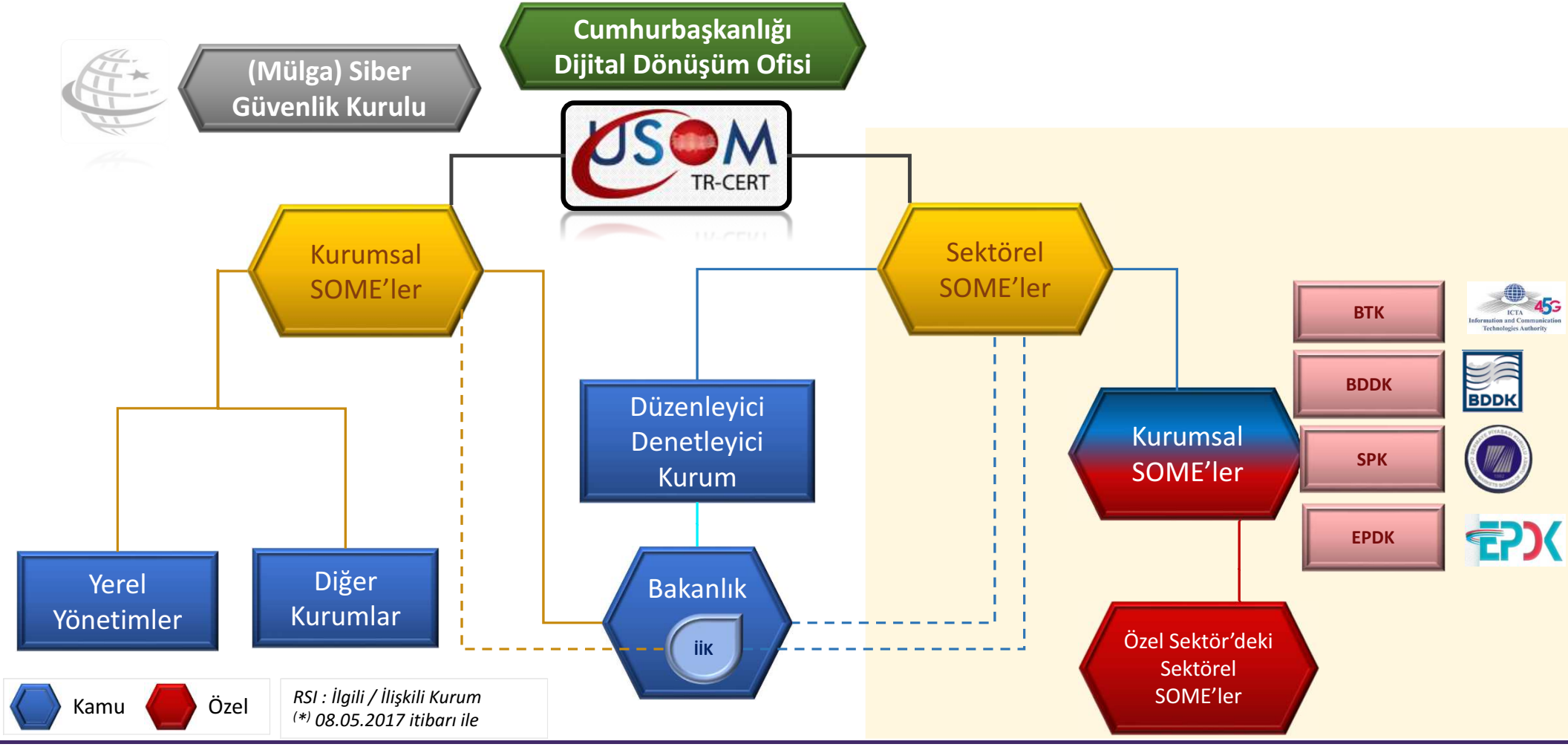
USOM ve SOME YAPILANMASI

Stratejik Üst Seviye Koordinasyon

Bütüncül teknik yönetim için:
Taktik seviyede **«Komuta Merkezi»**
Teknik seviyede **«Koordinasyon Merkezi»** dir.

Kamu Kurumları ve Kritik Altyapılar için
«Siber Birlikler»

Türkiye Siber Güvenlik Yönetişim Modeli



Diğer Yapılanmalar

Kamu Entegre Veri Merkezi
Durum: Fizibilite Analizi

Havelsan
Siber Savunma Teknoloji Merkezi (SİSATEM)
23.03.2016

STM
Siber Füzyon Merkezi
17.05. 2016

TSK Siber Savunma Komutanlığı
Siber Savunma Operasyon Merkezi
11.07. 2017

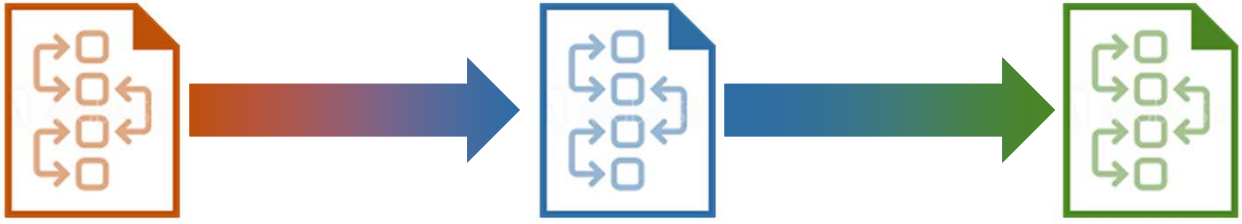
Gündem


Tanımlar ve Kapsam
1
Kritik Altyapılar ve Siber Güvenlik
2
Siber Güvenlik ve Yönetişim
3
Siber Güvenlik Stratejileri
4
Siber Güvenlik ve Mevzuat
5
Siber Güvenlik için Kaynaklar
6

Dünyada Siber Güvenlik Stratejileri

http://afyonluoglu.org/siberguvenlik/world-css/

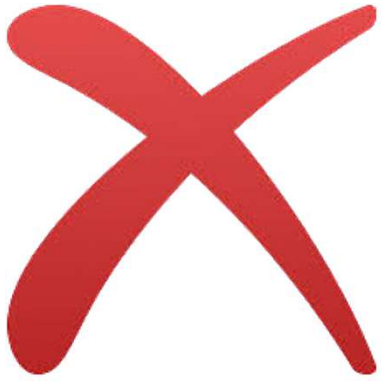
Beklenen Yapı



SİBER GÜVENLİK STRATEJİSİ

KRİTİK ALTYAPILARIN KORUNMASI STRATEJİSİ

SEKTÖREL PLANLAR

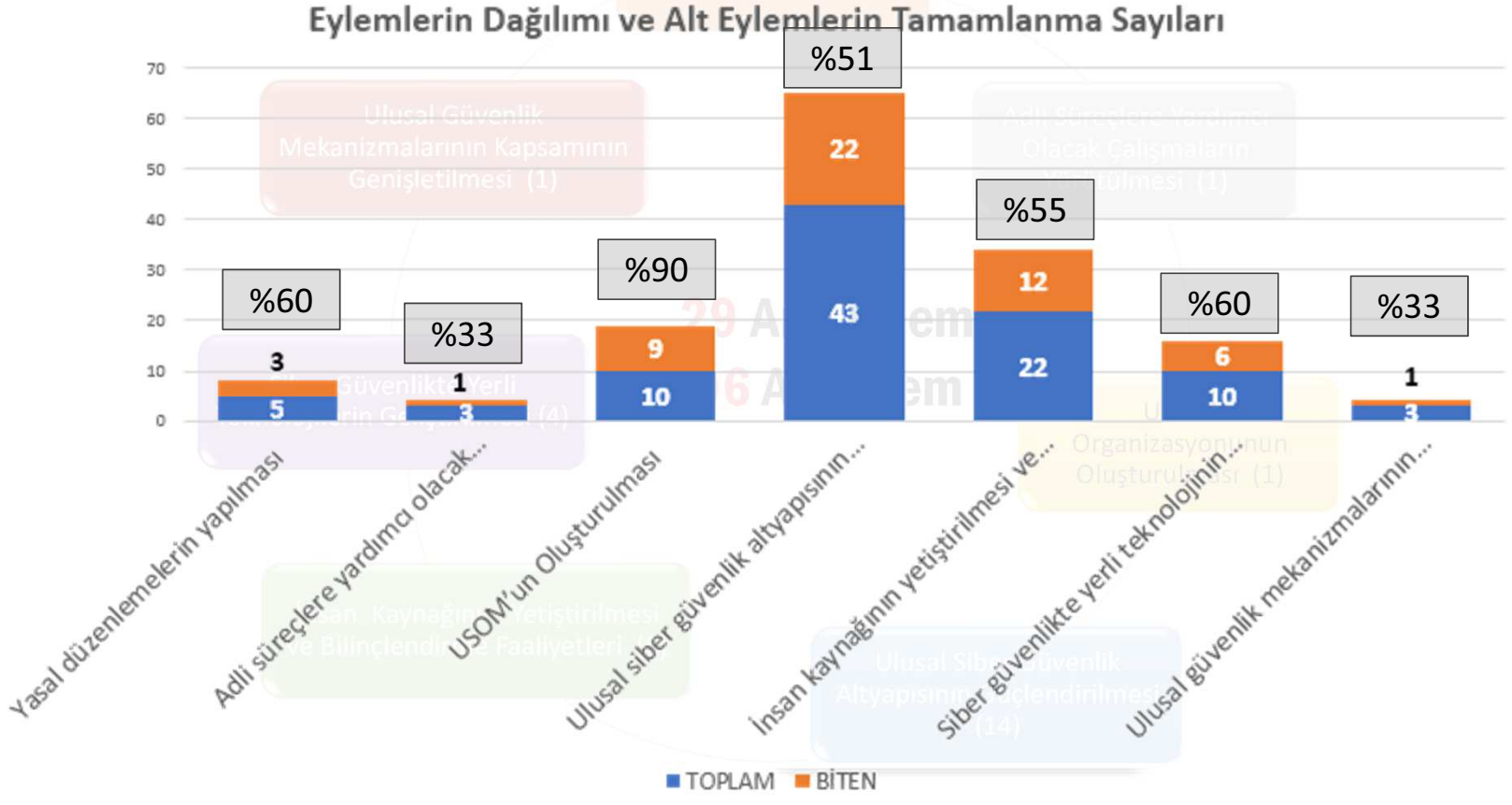


2013-2014 Siber Güvenlik Stratejisi ve Eylem Planı

2013-2014 Siber Güvenlik Stratejisi ve Eylem Planı

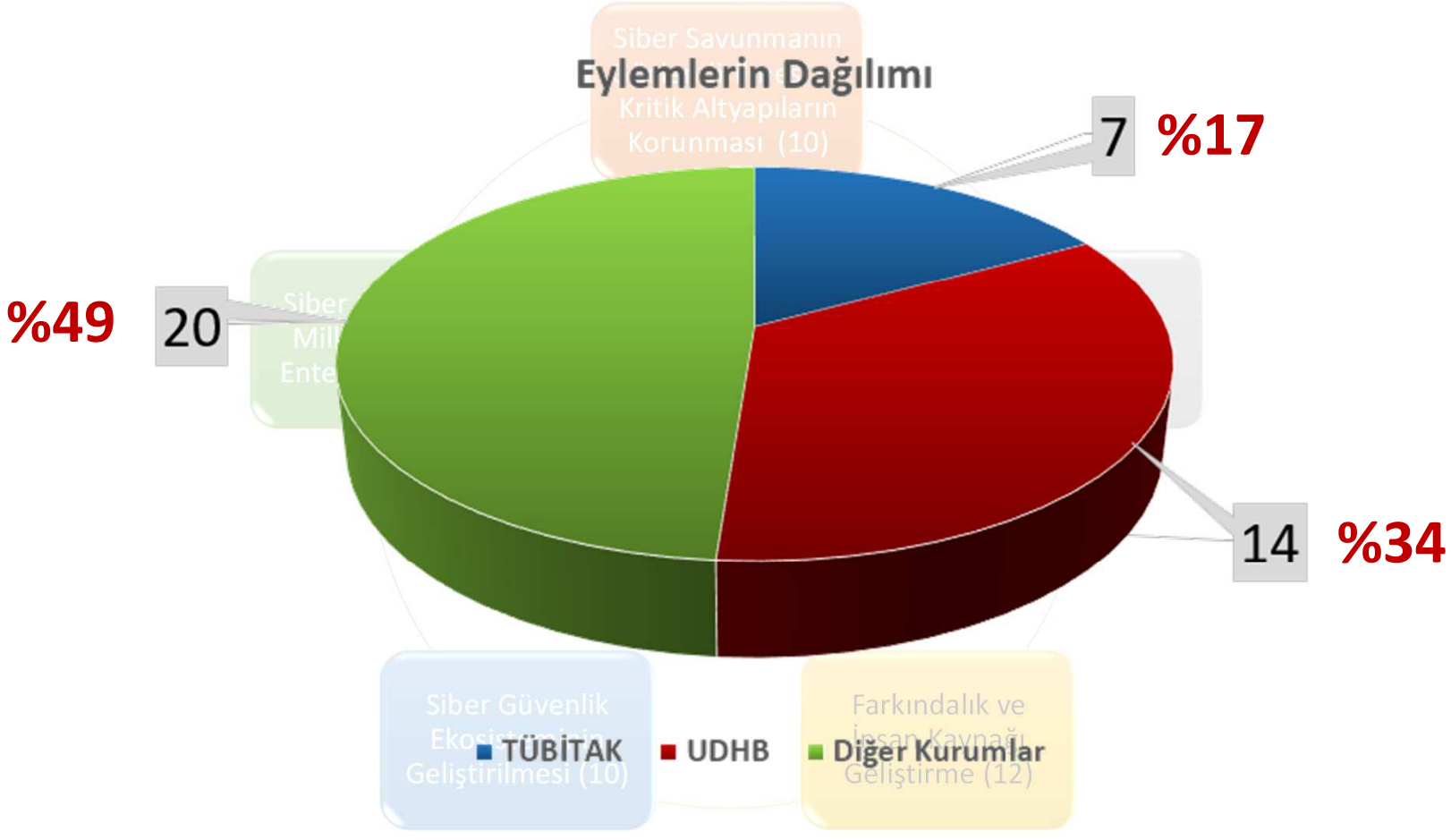
DEĞERLENDİRME (Mart 2015)

- **54 Eylem tamamlandı (% 56)**



2016-2019 Siber Güvenlik Stratejisi ve Eylem Planı

2016-2019 Siber Güvenlik Stratejisi ve Eylem Planı

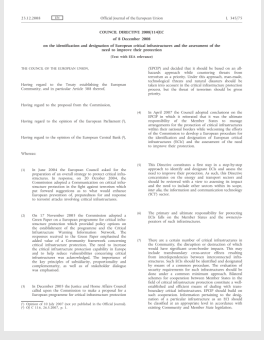


Gündem

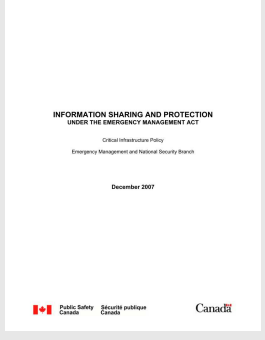

Tanımlar ve Kapsam
1
Kritik Altyapılar ve Siber Güvenlik
2
Siber Güvenlik ve Yönetişim
3
Siber Güvenlik Stratejileri
4
Siber Güvenlik ve Mevzuat
5
Siber Güvenlik için Kaynaklar
6

Kritik Altyapılara İlişkin Mevzuat (Uygulama, Paylaşım, Denetim)

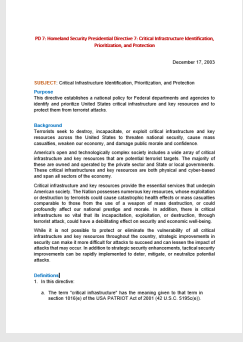
Müstakil SİBER GÜVENLİK KANUNU'na ilaveten:



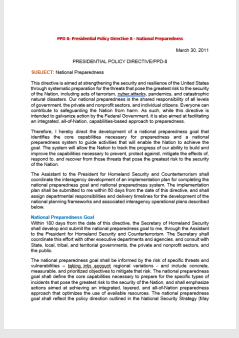
AB: 2008/114/EC
AB Kritik Altyapılar Koruma Direktifi



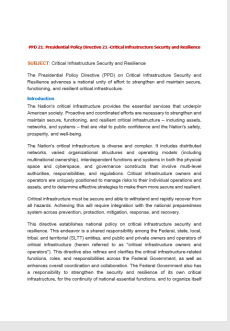
Kanada Kritik Altyapı Politika Belgesi
Acil Durum Yönetimi Çerçevesinde Bilgi Paylaşımı ve Korunması



ABD –PD 7
Kritik Altyapılar Tanım, Önceliklendirme ve Koruma Başkanlık Direktifi (2003)



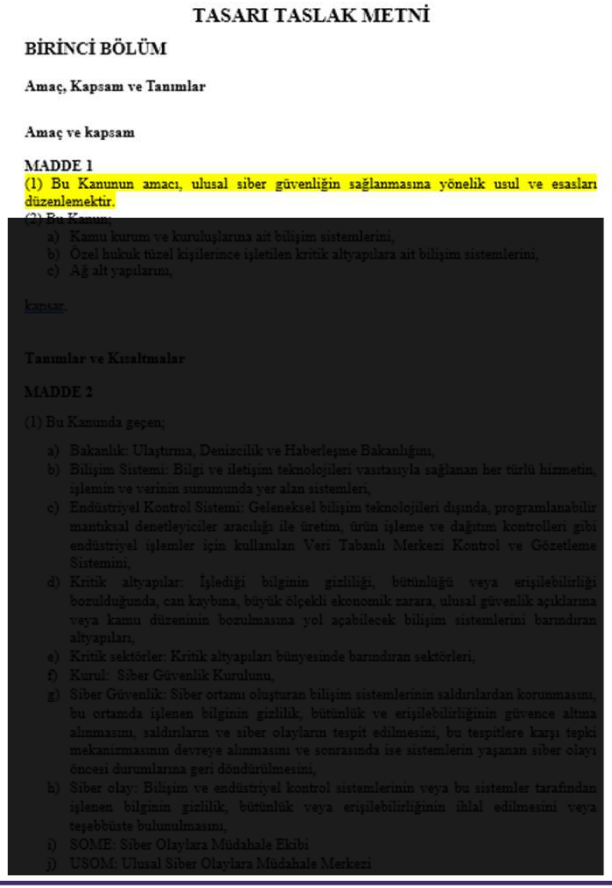
ABD –PPD 8
Ulusal Hazırlık Başkanlık Politika Direktifi (2011)



ABD –PPD 21
Kritik Altyapıların Güvenliği Başkanlık Politika Direktifi (2013)

Siber Güvenlik Kanunu

Siber Güvenlik Kanunu - Taslak
2016



TASARI TASLAK METNİ

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

Amaç ve kapsam

MADDE 1

(1) Bu Kanunun amacı, ulusal siber güvenliğin sağlanmasına yönelik usul ve esasları düzenlemektir.

(2) Bu Kanun;

a) Kamu kurum ve kuruluşlarına ait bilişim sistemlerini,

b) Özel hukuk tüzel kişilerince işletilen kritik altyapılara ait bilişim sistemlerini,

c) Ağ alt yapılarını,

kapsar.

Tanımlar ve Kısaltmalar

MADDE 2

(1) Bu Kanunda geçen;

a) Bakanlık: Ulaştırma, Denizcilik ve Haberleşme Bakanlığını,

b) Bilişim Sistemi: Bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmetin, işlemin ve verinin sunumunda yer alan sistemleri,

c) Endüstriyel Kontrol Sistemi: Geleneksel bilişim teknolojileri dışında, programlanabilir mantıksal denetleyiciler aracılığı ile üretim, ürün işleme ve dağıtım kontrolleri gibi endüstriyel işlemler için kullanılan Veri Tabanlı Merkezi Kontrol ve Gözetleme Sistemini,

d) Kritik altyapılar: İşlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapıları,

e) Kritik sektörler: Kritik altyapıları bünyesinde barındıran sektörleri,

f) Kurul: Siber Güvenlik Kurulunu,

g) Siber Güvenlik: Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber olayların tespit edilmesini, bu tespitlere karşı tepki mekanizmasının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber olayı öncesi durumlarına geri döndürülmesini,

h) Siber olay: Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya teşebbüste bulunulmasını,

ı) SOME: Siber Olaylara Müdahale Ekibi

j) USOM: Ulusal Siber Olaylara Müdahale Merkezi

5809 sayılı Elektronik Haberleşme Kanunu
6.2.2014

Elektronik Haberleşme Sektöründe Yetkili Merciler ve Görevleri
Bakanlığın görev ve yetkileri

MADDE 5 –

h) (Ek: **6/2/2014**-6518/102 md.) Ulusal siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere yönelik siber güvenliğin sağlanmasına ilişkin usul ve esasları belirlemek, eylem planlarını hazırlamak, (…) ilgili faaliyetlerin koordinasyonunu sağlamak, kritik altyapılar ile ait oldukları kurumları ve konumları belirlemek, gerekli müdahale merkezlerini kurmak, kurdurmak ve denetlemek, her türlü siber müdahale aracının ve millî çözümlerin üretilmesi ve geliştirilmesi amacı ile çalışmalar yapmak, yaptırmak ve bunları teşvik etmek ve siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütmek, siber güvenlik alanında faaliyet gösteren gerçek ve tüzel kişilerin uyması gereken usul ve esasları hazırlamak.

v) (Ek: 6/2/2014-6518/103 md.) Siber güvenlik ve internet alan adları konularında Cumhurbaşkanı, Bakanlık ve/veya Siber Güvenlik Kurulu tarafından verilen görevleri Telekomünikasyon İletişim Başkanlığı veya diğer birimleri marifetiyle yerine getirmek

Kurumun yetkisi ve idarî yaptırımlar

MADDE 60 –(11) (Ek: **15/8/2016**-KHK-671/25 md.; Aynen kabul: 9/11/2016-6757/22 md.) Kurum, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alır veya aldırır

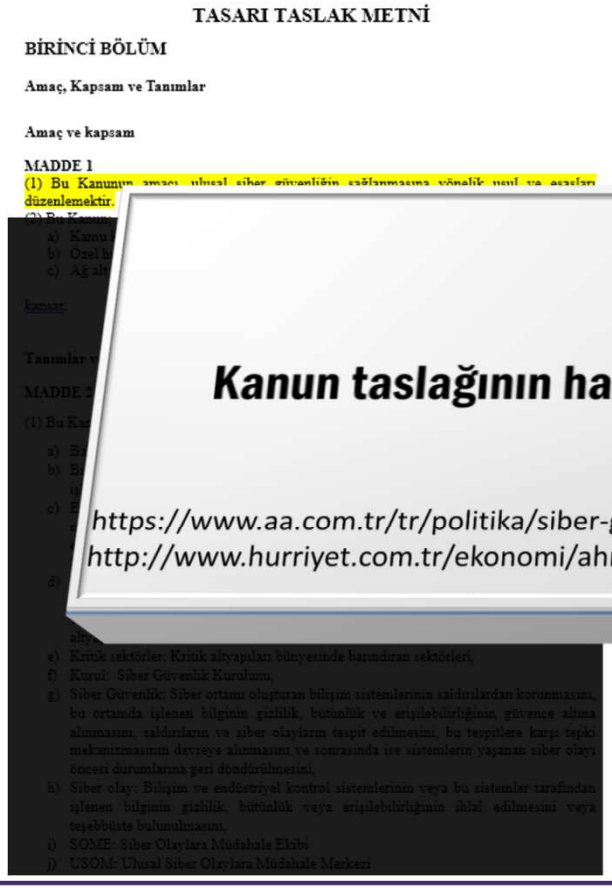
2/7/2018 tarihli ve 703 sayılı Kanun Hükmünde Kararnamenin 205 inci maddesiyle «**Siber Güvenlik Kurulu**» kapatılmıştır.

Mevzuatta Siber Güvenlik Kuruluna yapılmış olan atıflar, Cumhurbaşkanınca belirlenen kurul veya mercie yapılmış sayılır.

http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809.pdf

Siber Güvenlik Kanunu

Siber Güvenlik Kanunu - Taslak
2016



TASARI TASLAK METNİ

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

Amaç ve kapsam

MADDE 1

(1) Bu Kanunun amacı, ulusal siber güvenliğin sağlanmasına yönelik usul ve esasları düzenlemektir.

5809 sayılı Elektronik Haberleşme Kanunu
6.2.2014

Elektronik Haberleşme Sektöründe Yetkili Merciler ve Görevleri
Bakanlığın görev ve yetkileri

MADDE 5 –

h) (Ek: **6/2/2014**-6518/102 md.) Ulusal siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere yönelik siber güvenliğin sağlanmasına

rdinasyonunu

e merkezlerini

üretilmesi ve

k konusunda

yet gösteren

nı, Bakanlık

veya diğer

um, kamu

ılara karşı

caydırıcılık sağlamak için her türlü tedbiri alır veya aldırır

13 Ocak 2017

29 Kasım 2017

Kanun taslağının hazır olduğu ve yayımlanacağına ilişkin Bakan Açıklaması

https://www.aa.com.tr/tr/politika/siber-guvenlik-kanun-taslagi-calismasini-tamamladik/984785

http://www.hurriyet.com.tr/ekonomi/ahmet-arslan-siber-guvenlik-yasasi-yakin-zamanda-cikacak-40335557

2/7/2018 tarihli ve 703 sayılı Kanun Hükmünde Kararnamenin 205 inci maddesiyle «**Siber Güvenlik Kurulu**» kapatılmıştır.

Mevzuatta Siber Güvenlik Kuruluna yapılmış olan atıflar, Cumhurbaşkanınca belirlenen kurul veya mercie yapılmış sayılır.

http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809.pdf

SİBER OLAYLARA MÜDAHALE EKİPLERİNİN KURULUŞ, GÖREV VE ÇALIŞMALARINA DAİR USUL VE ESASLAR HAKKINDA TEBLİĞ

11 KASIM 2013

Kurumsal SOME'lerin görev ve sorumlulukları

Madde 5: (2) Kurumsal SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik olarak, kurumlarının bilişim sistemlerinin kurulması, işletilmesi veya geliştirilmesi ile ilgili çalışmalarda teknik ve idari tedbirler konusunda öneri sunarlar.

(4) Kurumsal SOME'ler bir siber olayla karşılaştıklarında, USOM ve birlikte çalıştığı sektörel SOME'ye bilgi vermek koşulu ile öncelikle söz konusu olayı kendi imkân ve kabiliyetleri ile bertaraf etmeye çalışırlar.

(8) [ve Made 7-(6)] Kurumsal (Sektörel) SOME'ler 7/24 erişilebilir olan iletişim bilgilerini belirleyerek birlikte çalıştığı sektörel SOME'lere ve USOM'a bildirirler.

Cumhurbaşkanlığı Hükümet Sistemi - Mevzuat

703 Numaralı Kanun Hükmünde Kararname

MADDE 205- 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununun;

c) 5 inci maddesinin birinci fıkrasının (h) bendinde yer alan "Siber Güvenlik Kurulunun sekretaryasını yapmak," ibaresi madde metninden çıkarılmıştır.

"EK MADDE 2- (1) Mevzuatta Siber Güvenlik Kuruluna yapılmış olan atıflar, Cumhurbaşkanınca belirlenen kurul veya mercie yapılmış sayılır."

1 Numaralı Cumhurbaşkanlığı Kararnamesi

DÖRDÜNCÜ KISIM
CUMHURBAŞKANLIĞI POLİTİKA KURULLARI
İKİNCİ BÖLÜM
Kurullar

Güvenlik ve Dış Politikalar Kurulu

MADDE 26- (1) Güvenlik ve Dış Politikalar Kurulunun görev ve yetkileri şunlardır:

ğ) Siber güvenlik ile ilgili politika ve strateji önerileri geliştirmek,

YEDİNCİ KISIM
CUMHURBAŞKANLIĞI OFİSLERİ
Ofislerin görevleri

MADDE 527 - (1) Dijital Dönüşüm Ofisi'nin görevleri şunlardır:

ç) Siber güvenlik ve bilgi güvenliğini artırıcı projeler geliştirmek,

Gündem


Tanımlar ve Kapsam
1
Kritik Altyapılar ve Siber Güvenlik
2
Siber Güvenlik ve Yönetişim
3
Siber Güvenlik Stratejileri
4
Siber Güvenlik ve Mevzuat
5
Siber Güvenlik için Kaynaklar
6

Siber Güvenlik Kaynakları

1312 ULUSAL ve ULUSLARARASI RAPOR

- 69 Ulusal Belge
- 133 Strateji Belgesi
- 189 Uluslararası Rapor
- 115 Akademik Çalışma
- 324 Eğitim Materyali
- 54 AB RAporu
- 119 ENISA Raporu
- 62 Kritik Altyapı Belgesi
- 88 Rapor, Rehber Standart
- 14 Ülke İdari Modeli
- 140 Kütüphane (Video vd.)

http://afyonluoglu.org/siberguvenlik/

AB ve Siber Güvenlik

http://afyonluoglu.org/siberguvenlik/enisa-raporlari/

AB ve Siber Güvenlik Eğitimleri

enisa European Union Agency for Network and Information Security

CSIRT SİBER GÜVENLİK EĞİTİMLERİ

Hazırlık Dokümanları

- Good practice guide on training methodologies
- Roadmap to provide more proactive and efficient CSIRT training

Building Artefact Handling and Analysis Environment

Purpose:

The main objective is to create safe and useful artifact analysis

Duration:

- 7 Hours

Downloads:

- Handbook
- Toolset

http://afyonluoglu.org/siberguvenlik/cybersecurity-training/

Teşekkür Ederim

Türkiye'de ve Dünyada

Siber Güvenlik

Kamu Sektöründe İnovasyon

ARGÜDEN GOVERNANCE ACADEMY

Good Governance for Quality of Life

MUSTAFA AFYONLUOĞLU

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

http://afyonluoglu.org

26 Kasım 2018