Cyber Security for National Security
«Coordination, Capacity Building and National Solutions»

Mustafa AFYONLUOĞLU
Cyber Security, e-Governance and eGovernment Chief Expert

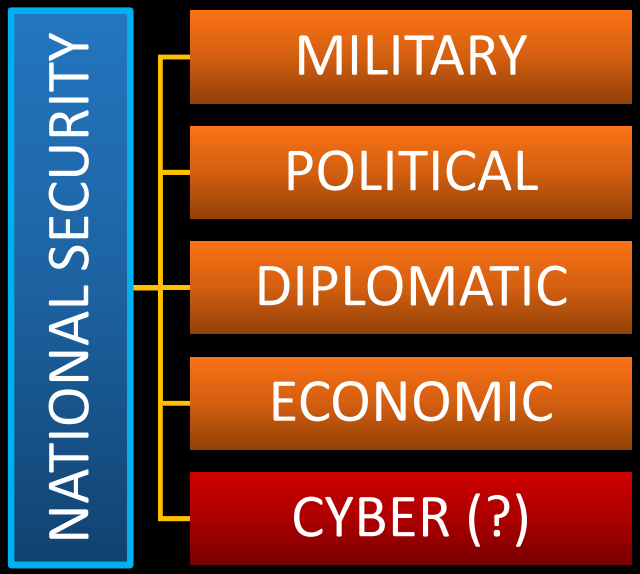
teknoloji platformları

SİBER GÜVENLİK 4.0 ve FELAKET YÖNETİMİ
TEKNOLOJİ PLATFORMU - 25 NİSAN 2017 / İSTANBUL

25.04.2017

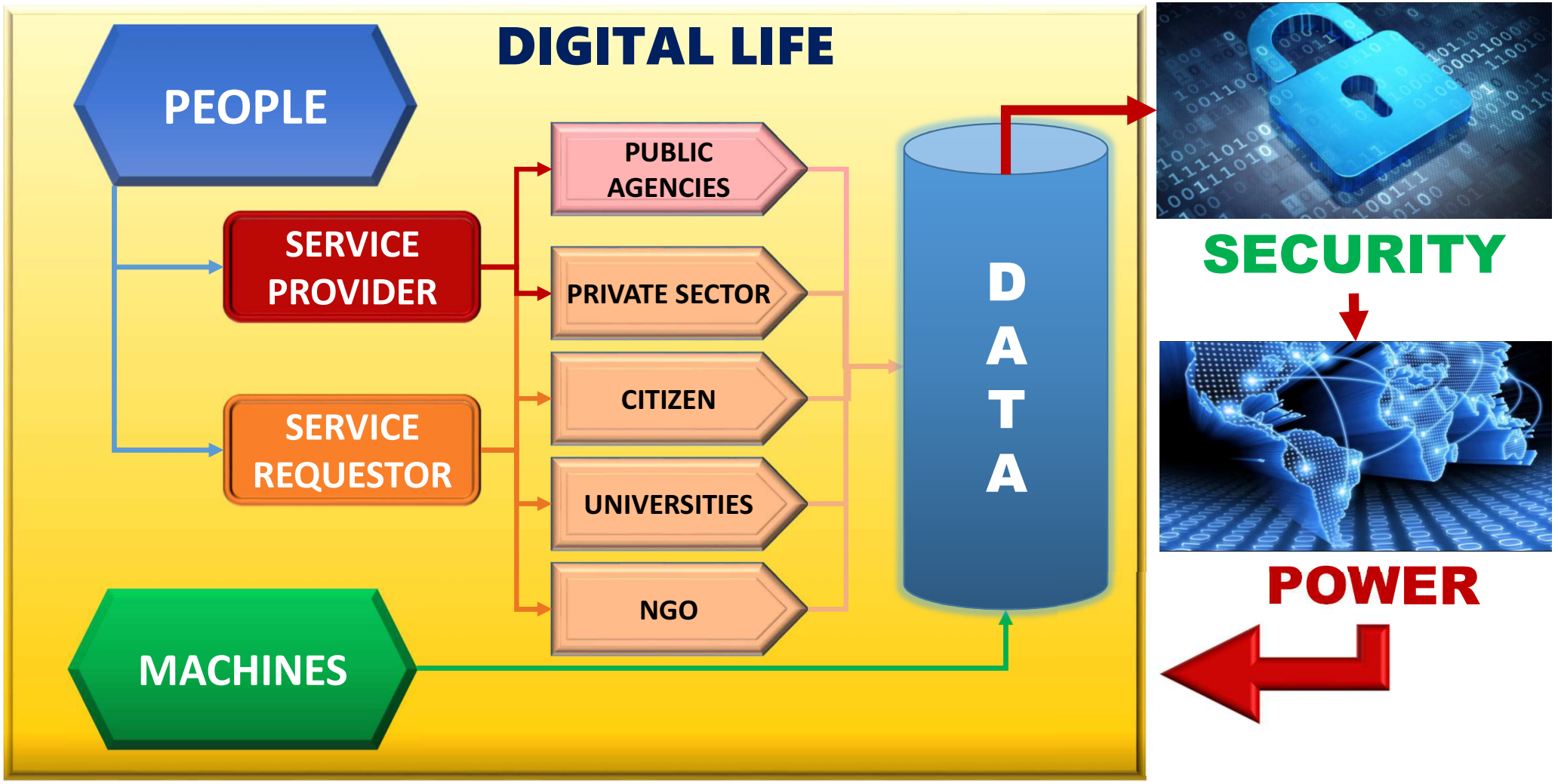
Cyber Security for National Security

National Security: Identification of threats and opportunities by monitoring the regional and global environment in order to take measures against the threats to the national state and security, and the processes to determine the politics appropriate to these issues and to implement the most appropriate policies (National Security Committee)*



* 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

Mustafa AFYONLUOGLU (afyonluoglu [at] gmail.com)



Mustafa AFYONLUOGLU (afyonluoglu [at] gmail.com)

SECURITY

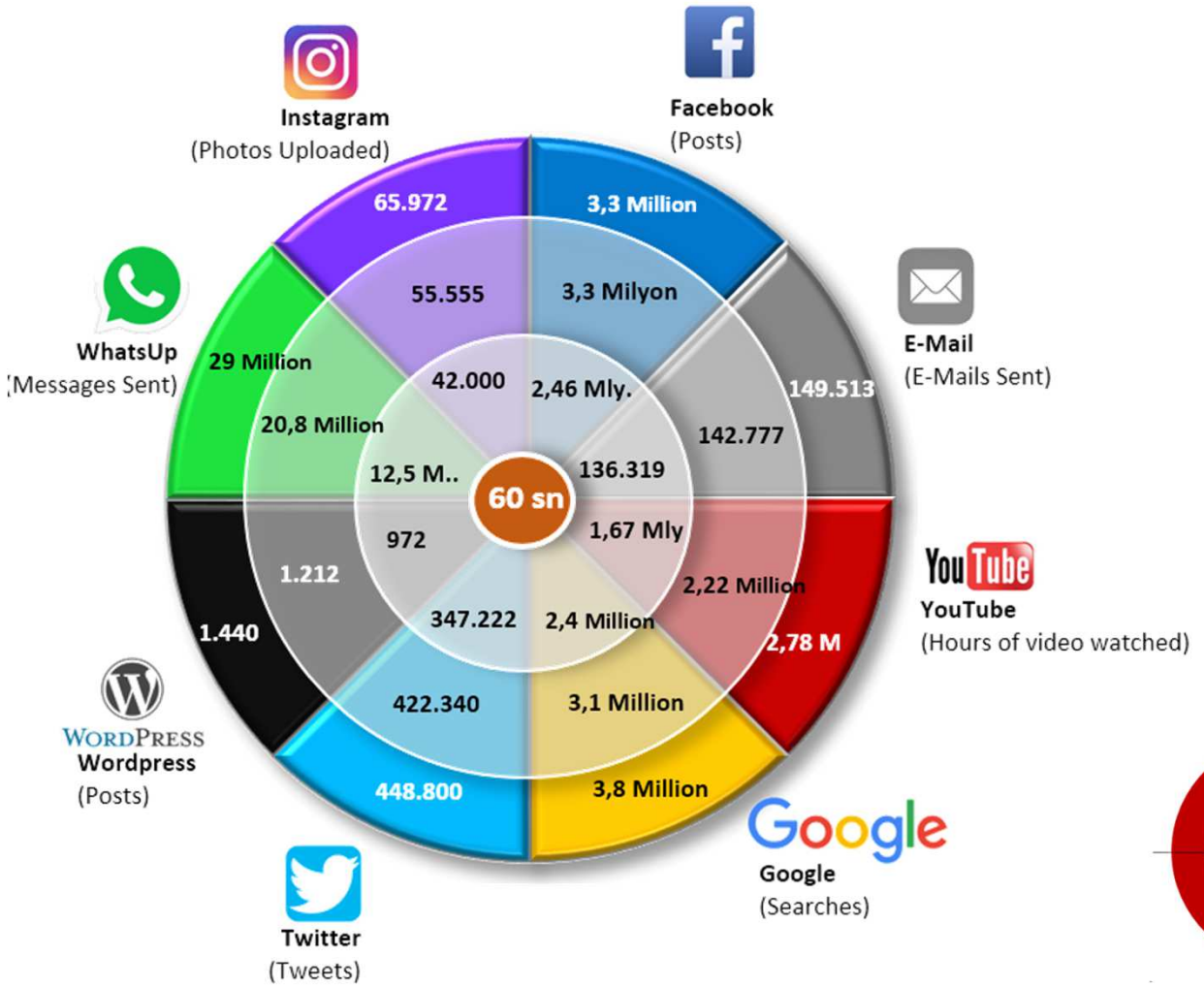
POWER

PUBLIC SECTOR & PRIVATE SECTOR
LIKE TWO WINGS OF A BIRD…
… IN HARMONY !

Mustafa AFYONLUOGLU (afyonluoglu [at] gmail.com)

What happens on the internet for 60 seconds?

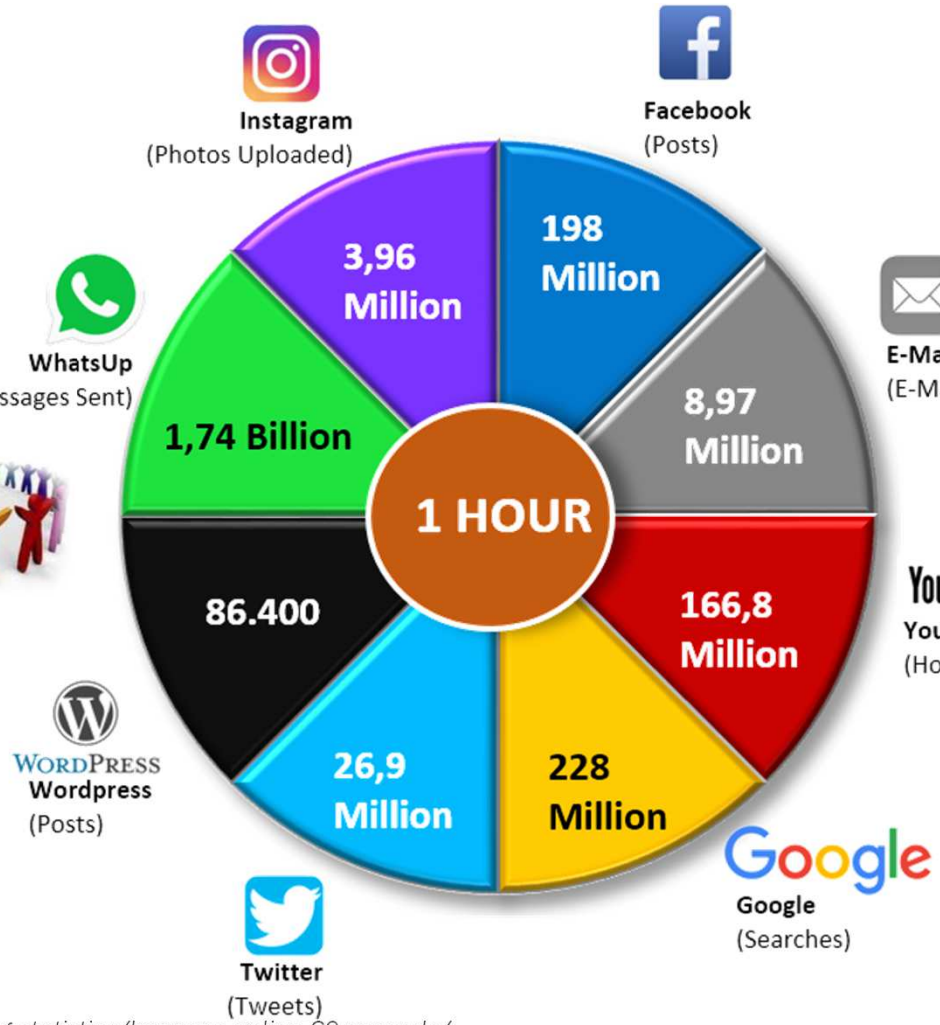
(February 2017)



http://www.smartinsights.com/internet-marketing-statistics/happens-online-60-seconds/

What happens on the internet for 1 Hour ?

(February 2017)



272

http://www.smartinsights.com/internet-marketing-statistics/happens-online-60-seconds/

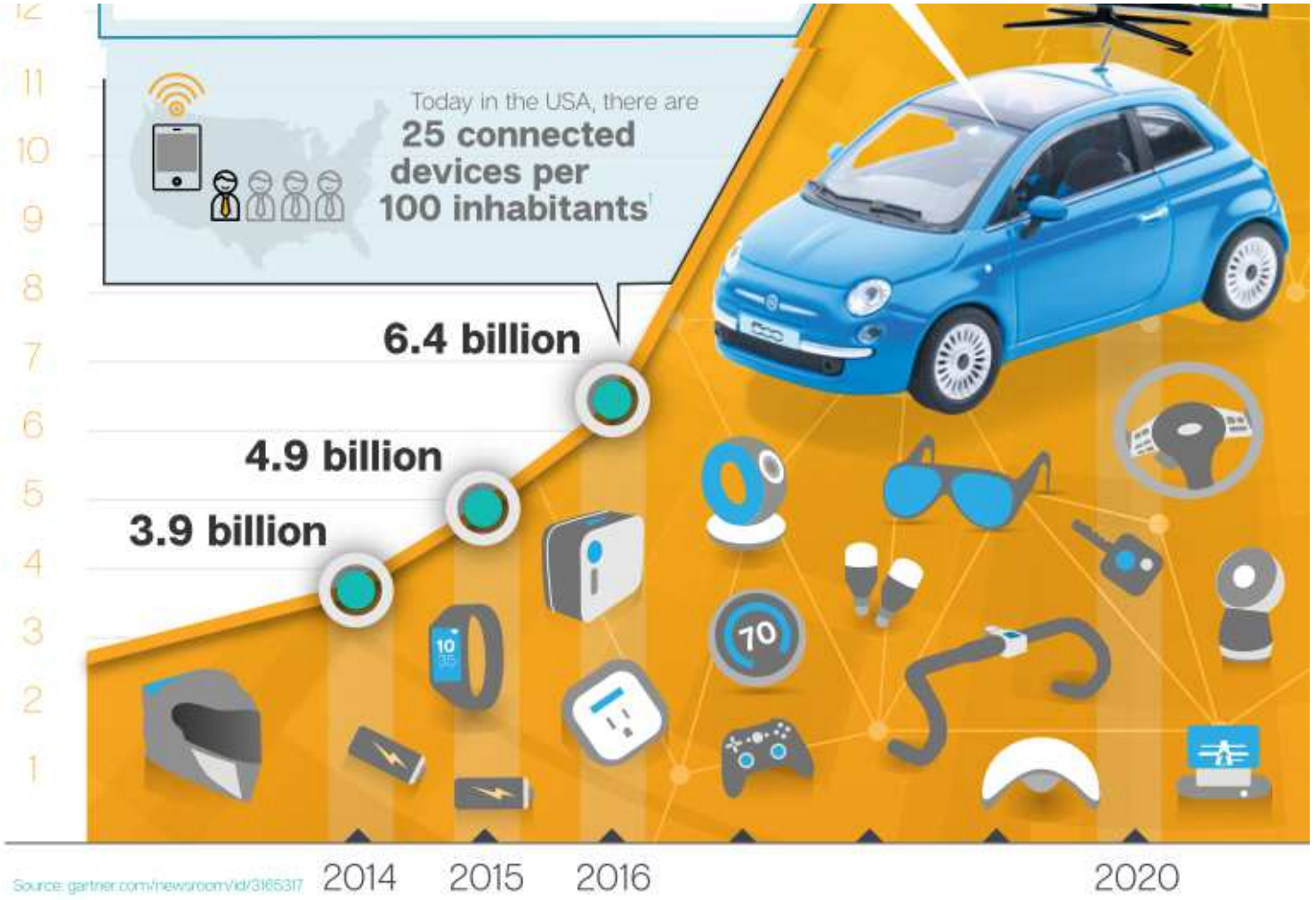
Internet Connected Devices

Internet of Things

2016 Symantec Internet Security Thread Report,, Gartner IoT Report 10 Kasım 2015

Internet Connected Devices

Internet of Things



2016 Symantec Internet Security Thread Report,, Gartner IoT Report 10 Kasım 2015

Internet Connected Devices

Internet of Things

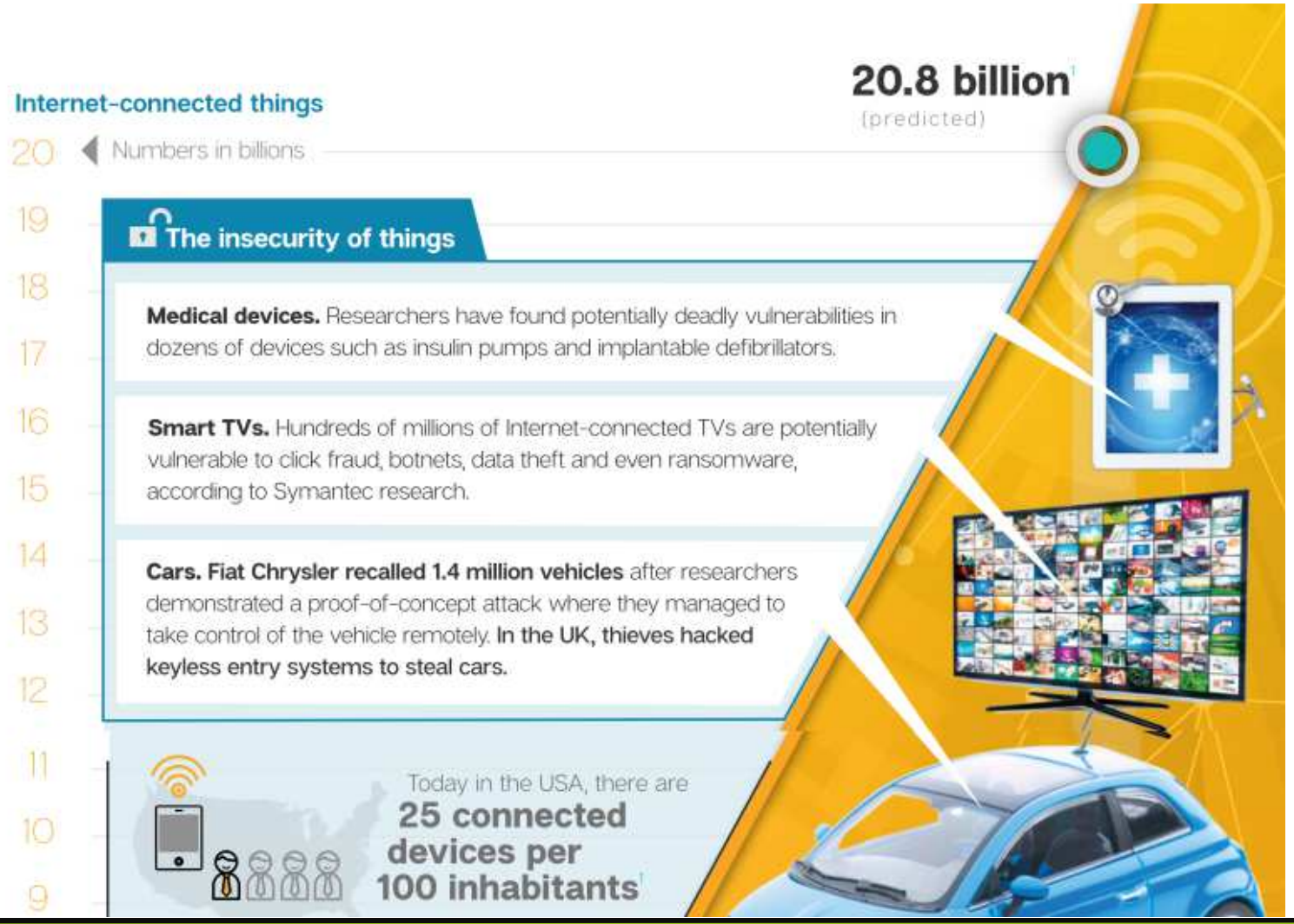
Expected Economical Size in IoT

2 Trillion Dollars

2016 Symantec Internet Security Thread Report,, Gartner IoT Report 10 Kasım 2015

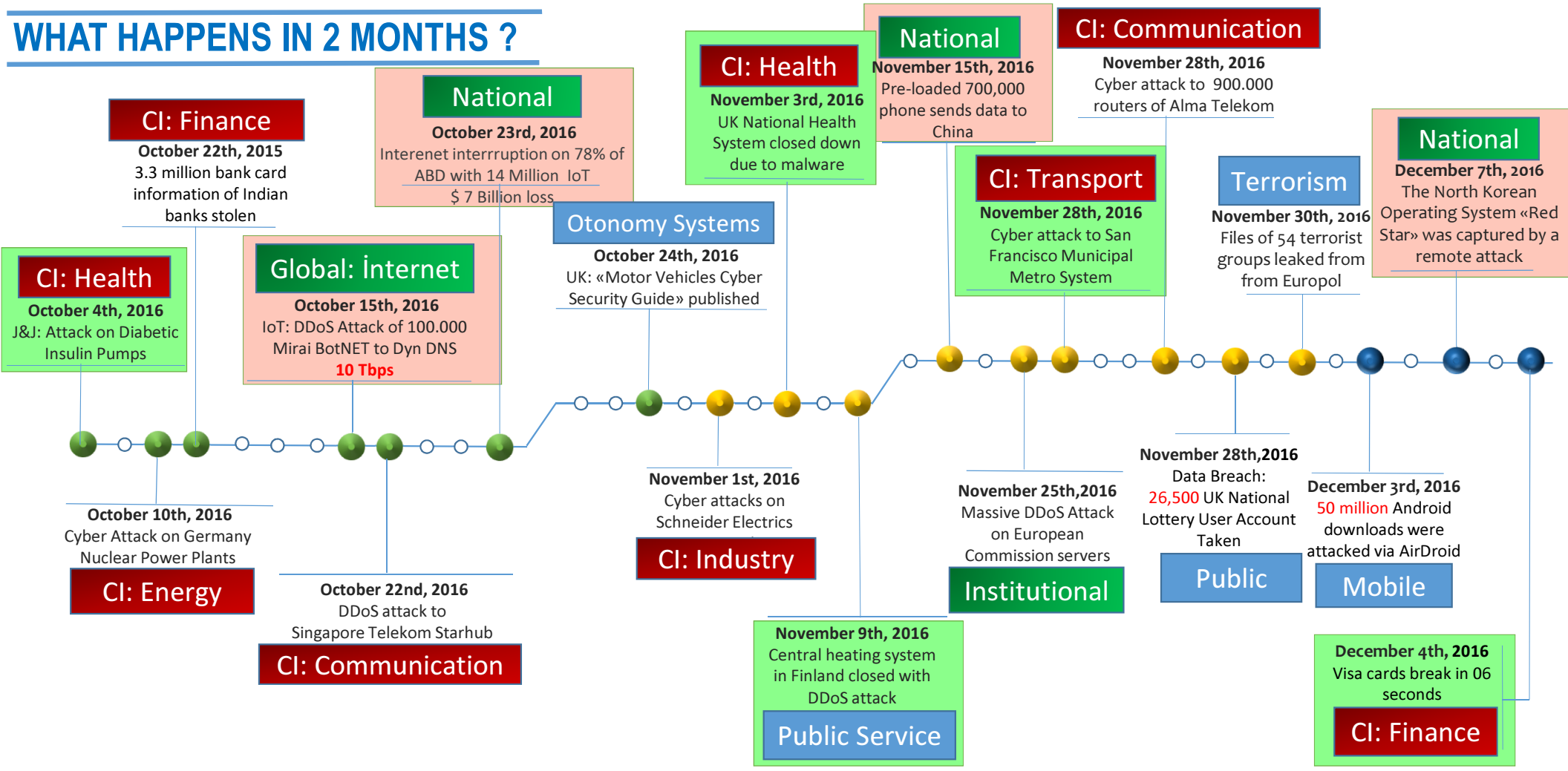
Internet Connected Devices

Internet of Things



Mustafa AFYONLUOGLU (afyonluoglu [at] gmail.com)

WHAT HAPPENS IN 2 MONTHS ?



CI: Critical Infrastructure
ICS: Industrial Control System
IoT: Internet of Things (100.000 IoT: 7.500 $ - DarkWeb)

December 14th 2015 – nic TR Domain Name System DDoS Attack

Dünya Tarihinde Yaşanmış En Yoğun Saldırı

Ulaştırma Bakanı Binali Yıldırım 'tr' uzantılı adreslere yaşanan siber saldırıya ilişkin ODTÜ'nün yeterli önlemi almadığını söyledi. ODTÜ Rektörü Acar ise 14 Aralık'ta dünya tarihinde yaşanmış en yoğun saldırıya maruz kaldıklarını belirterek güvenlik tedbirlerinin fazlasıyla alındığını vurguladı.

Tarih: 01-01-2016 23:42

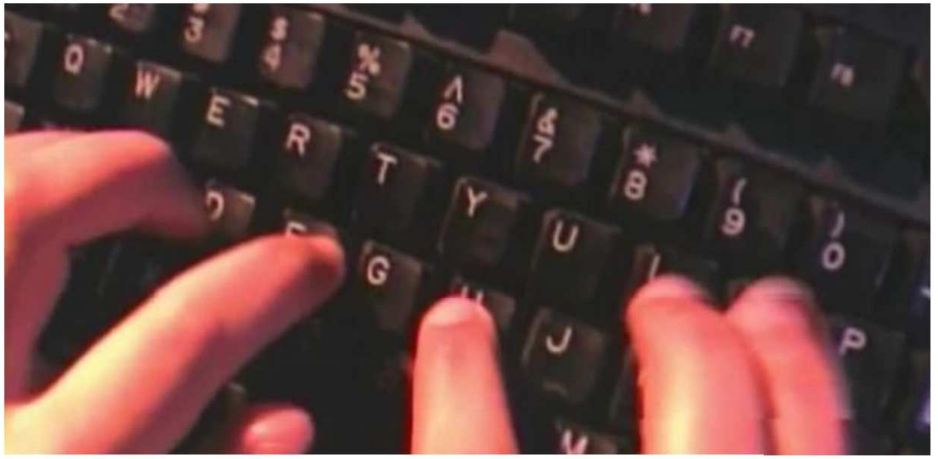
Ulaştırma, Havacılık ve Denizcilik Bakanı Binali Yıldırım, Türkiye'nin geçen hafta hedefi olduğu büyük siber saldırıyla ilgili olarak, "Siber savaş, gerçek savaştan bin beter sonuçlar doğurabiliyor, her türlü önlemi alıyoruz, daha da almamız lazım" dedi.

'ULUSAL GÜVENLİK MESELESİ'

Yıldırım, yurtdışı kaynaklı olan ve menşei tam olarak bilinemeyen saldırının 14 Aralık'tan itibaren etkili olduğunu, hemen karşı önlemlerin devreye alındığını söyledi. Bakan Yıldırım, saldırının esas olarak Ortadoğu Teknik Üniversitesi tarafından işletilmekte olan `nick.tr' adlı Türkiye'deki bütün `.tr' uzantılı web adreslerinin yönetildiği DNS sunucularını hedef aldığını belirterek, "Sunucuyu ODTÜ işletiyor ama mesele bir ulusal güvenlik meselesi, bu çeşit saldırılara karşı gerekli önlemlere sahip olunmalı" dedi.

December 24th, 2015 – Finance

Türkiye'de Bankalar Siber Saldırı Altında



Ziraat, İş Bankası, Akbank ve Garanti Bankası internet hizmeti veremedi

24 Aralık 2015

Ancak öğleden sonra bu kez bazı bankaların internet sitelerine erişim mümkün olmadı. Türkiye saatiyle 16.00'dan itibaren aktif, mevduat, şube sayısı büyüklüğünde ülkenin en büyük dört bankası olan Ziraat Bankası, İş Bankası, Garanti Bankası, Akbank'a internet üzerinden girilemediği görüldü.

Bankalardan konuyla ilgili herhangi bir açıklama gelmedi.

Mustafa AFYONLUOGLU (afyonluoglu [at] gmail.com)

April 08th, 2016 – National ID Number Data Breach

YSK Başkanı Güven: İnternete sızan kimlikler ile 2008'de paylaştığımız veriler uyuşuyor

AA

08 Nisan 2016 - 16:43| Son Güncelleme : 08 Nisan 2016 - 17:19

YSK Başkanı Sadi Güven, internette yayınlanan kimlik bilgileri ile ilgili olarak inceleme yaptıklarını belirterek, "İnternet sitelerinde yaptığımız araştırma sonucunda elde ettiğimiz bilgiler, siyasi partilere verdiğimiz veri tabanıyla uyuşmaktadır. Mühendislerimiz incelemeleri yaptılar, bizdeki kayıtlarla bire bir uyumlu olmasına rağmen bizim sistemimizden herhangi bir sızma yoktur" dedi. Güven, "Verilerin 2008 tarihinde paylaşılan dosyalarla uyumlu olduğu görülmüştür" diye konuştu.

https://onedio.com/haber/devlet-hastanelerine-siber-saldiri-binlerce-hastanin-kayitlari-sizdi--711565

May 18th, 2016 – Health Sector Data Breach

Devlet Hastanelerine Siber Saldırı: 'Binlerce Hastanın Kayıtları Sızdı'

Ana Sayfa > Haberler > Türkiye > Gündem - 18 Mayıs 2016, 17:48'de eklendi

Emre Ordu
Onedio Editörü

44 Paylaşım | Facebook'ta Paylaş | Twitter'da Paylaş | CROPY | 13b OKUNMA

Sağlık Bakanlığı'na bağlı 33 devlet hastanesine sabah saatlerinde siber saldırı düzenlendi. Binlerce hastanın kayıtlarının ele geçirildiği ve internette paylaşıldığı öne sürüldü. Youtube üzerinden eylemin duyurulduğu açıklamada da saldırının Anonymous grubu tarafından gerçekleştirildiği iddia edildi. Ancak akşam saatlerinde Anonymous grubunun Twitter hesabından yapılan açıklamada bu iddialar reddedildi...

Sağlık Bakanlığı'ndan yapılan açıklamada da saldırıdan sadece Diyarbakır'daki hastanelerin 'kısmen' etkilendiği belirtildi.

https://onedio.com/haber/devlet-hastanelerine-siber-saldiri-binlerce-hastanin-kayitlari-sizdi--711565

December 30th 2016 – Energy Sector

Albayrak: ABD merkezli siber saldırı yapıldı

06 Ocak 2017 Cuma - 11:36 | Son Güncelleme : 06 01 2017 - 12:55

Enerji ve Tabii Kaynaklar Bakanı Berat Albayrak, elektrik ve doğal gaza bu yıl zam öngörmediklerini söyleyerek, geçtiğimiz hafta yaşanan elektrik kesintileriyle ilgili ise "ABD merkezli siber saldırı yapıldı" dedi.

Paylaş Tweet G+1 2 Yorum Yaz 0

July 2016 – Institutional Data Breach

WikiLeaks, AKP'nin iç yazışmalarını yayınladı

Wikileaks 762 e-posta adresinden 294 bin 548 yazışma ve bunlarla birlikte binlerce ek dosya yayınlandı

19 Temmuz 2016 23:50

Beğen 455 Paylaş

Tweetle

Paylaşın

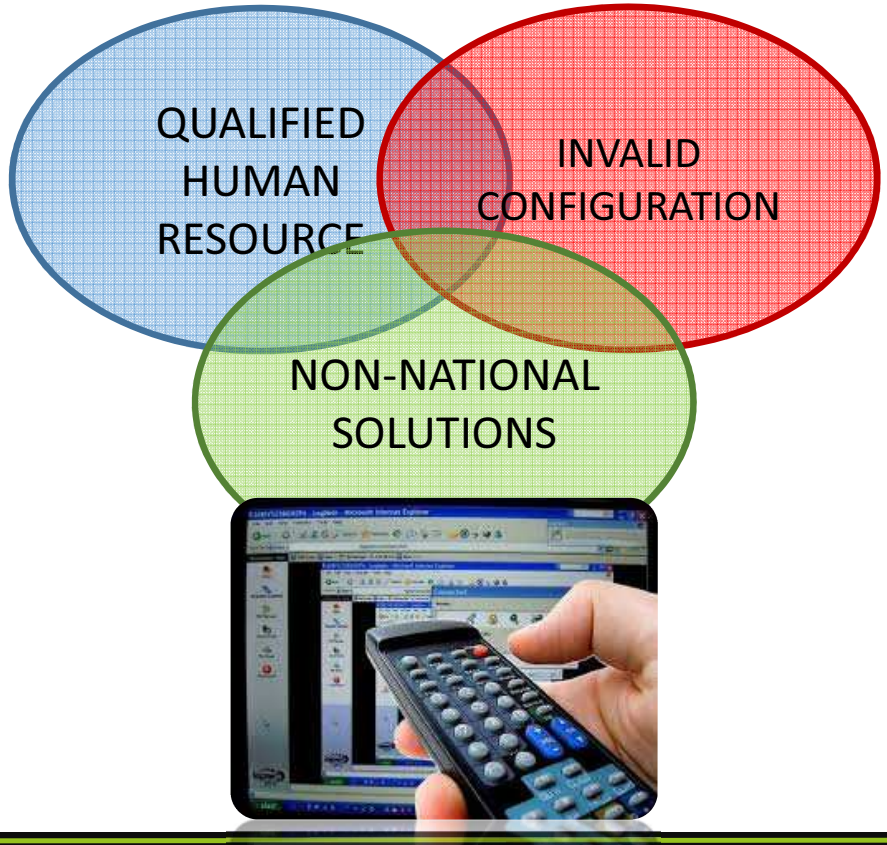
G+1 2

WikiLeaks, yayınlamayı planladığı bir seri e-postanın ilk adımı olarak, 2010 yılından başlayarak darbe girişiminden bir hafta önceye kadar süren AKP içi mail'leri paylaştı.

E-postaların akparti.org.trden geldiği belirtilirken, gönderilen e-postaların en yenisi 6 Temmuz 2016 tarihi taşıyor. En eskisi ise 2010 yılına ait.

http://www.gazetevatan.com/elektrik-hatlarina-sabotaj-var-mi-bakan-albayrak-yanitladi-1025710-gundem/

WEAK LINKS



Mustafa AFYONLUOGLU (afyonluoglu [at] gmail.com)

WEAK LINKS

Mustafa AFYONLUOGLU (afyonluoglu [at] gmail.com)

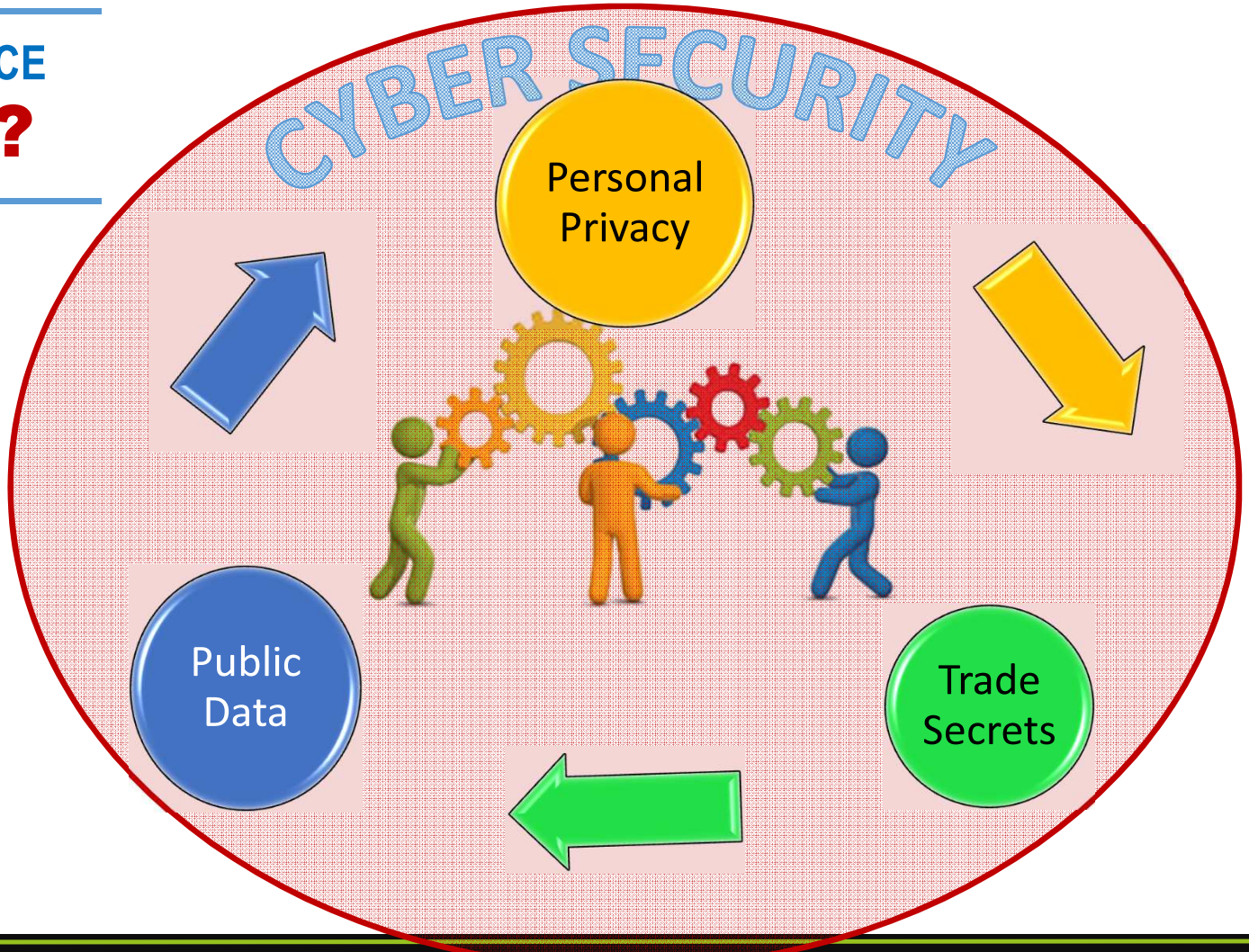
NATO OTAN

NORTH ATLANTIC TREATY ORGANIZATION

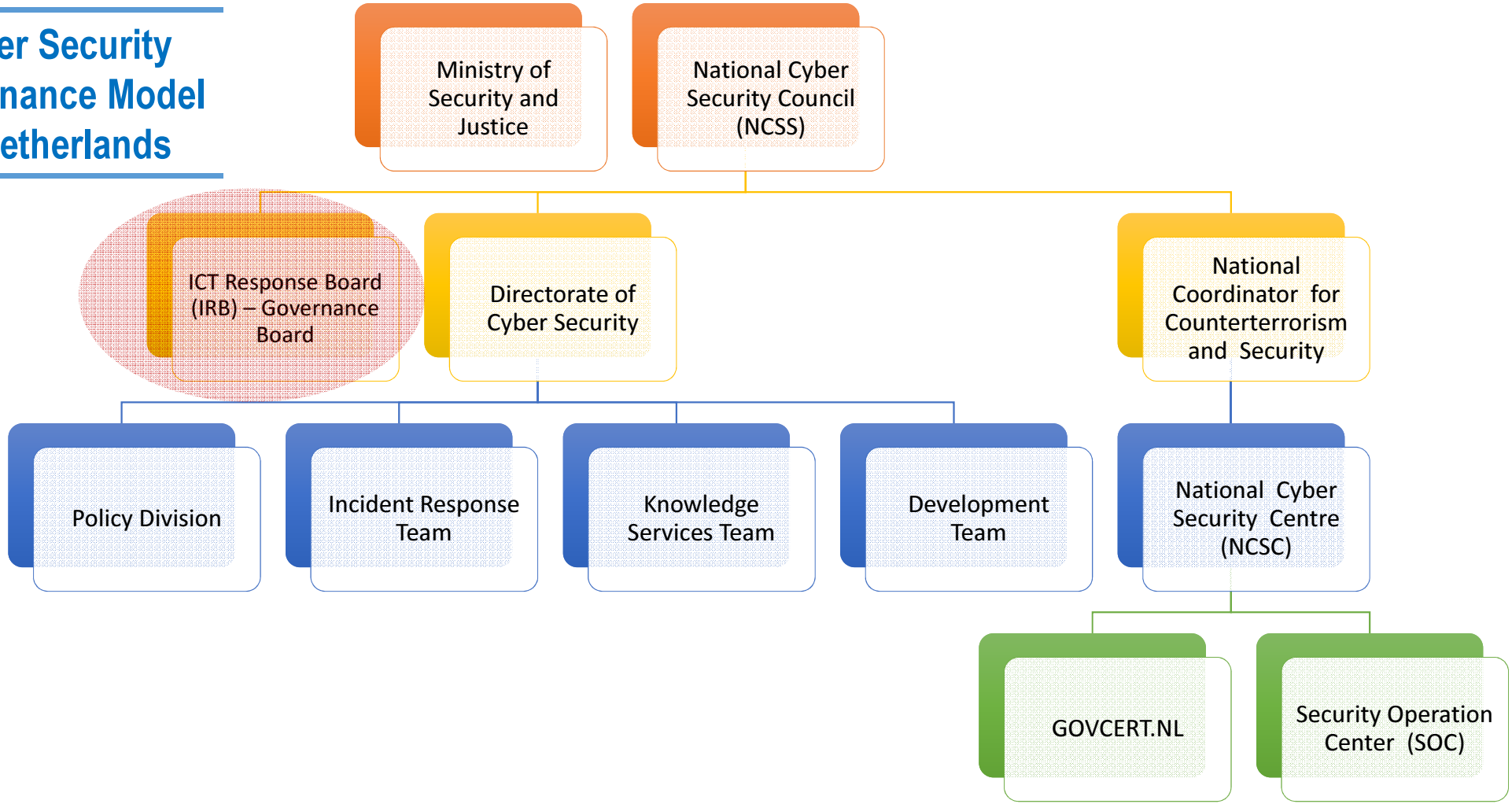
- **February 2016**: The Technical Arrangement on cooperation in cyber defense with the European Union was signed.
- **July 2016**: Cyber Space is the 5th operational area after Land, Air, Sea and Space.
- **December 2016**: Cyber defense is one of NATO's key tasks in the field of collective defense.
- International law should also be applied to the cyber field.
- NATO will develop cyber training and exercise skills.

http://www.nato.int/cps/en/natohq/topics_78170.htm

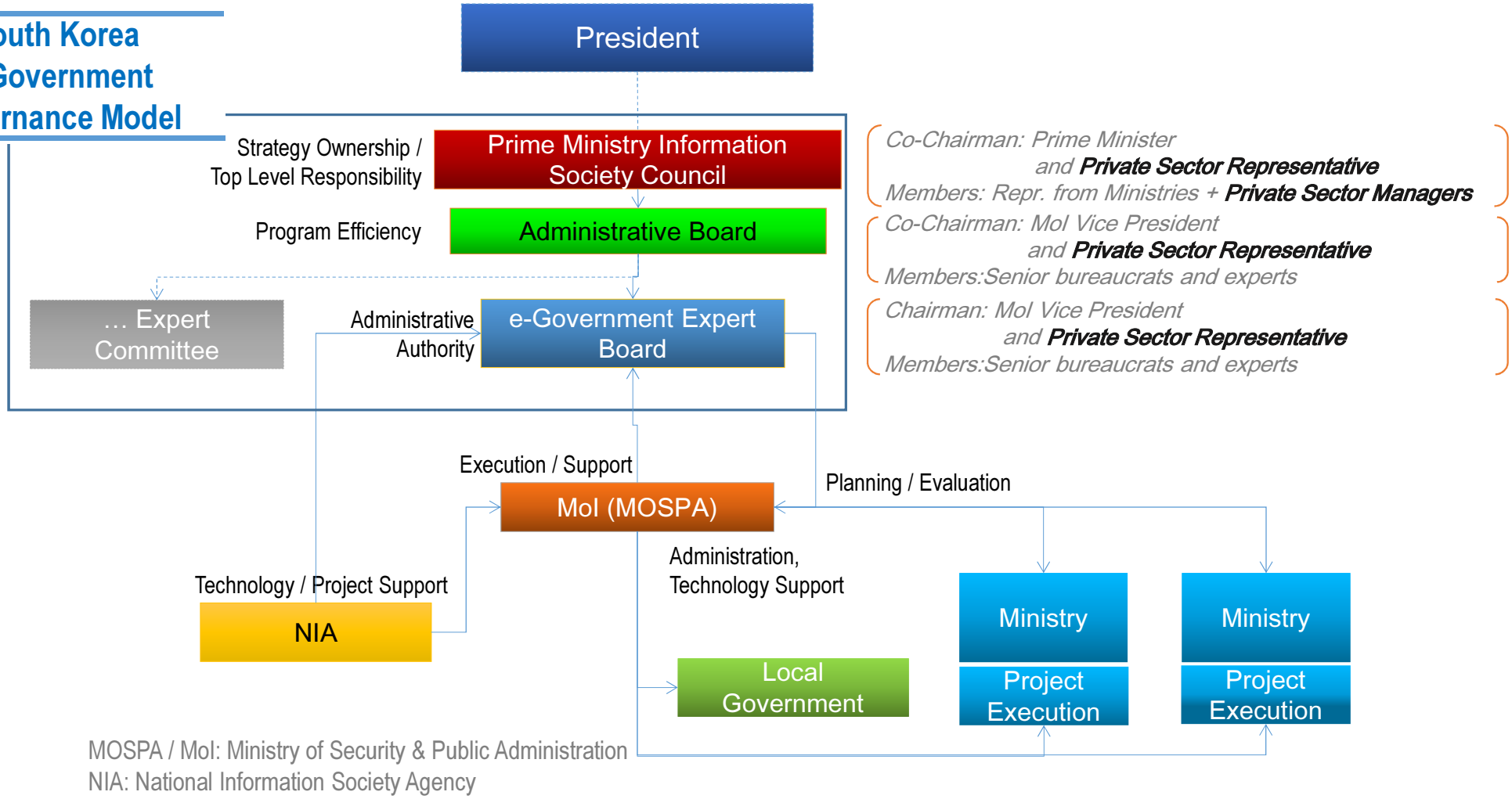
GOVERNANCE
HOW ?



Syber Security Governance Model of Netherlands

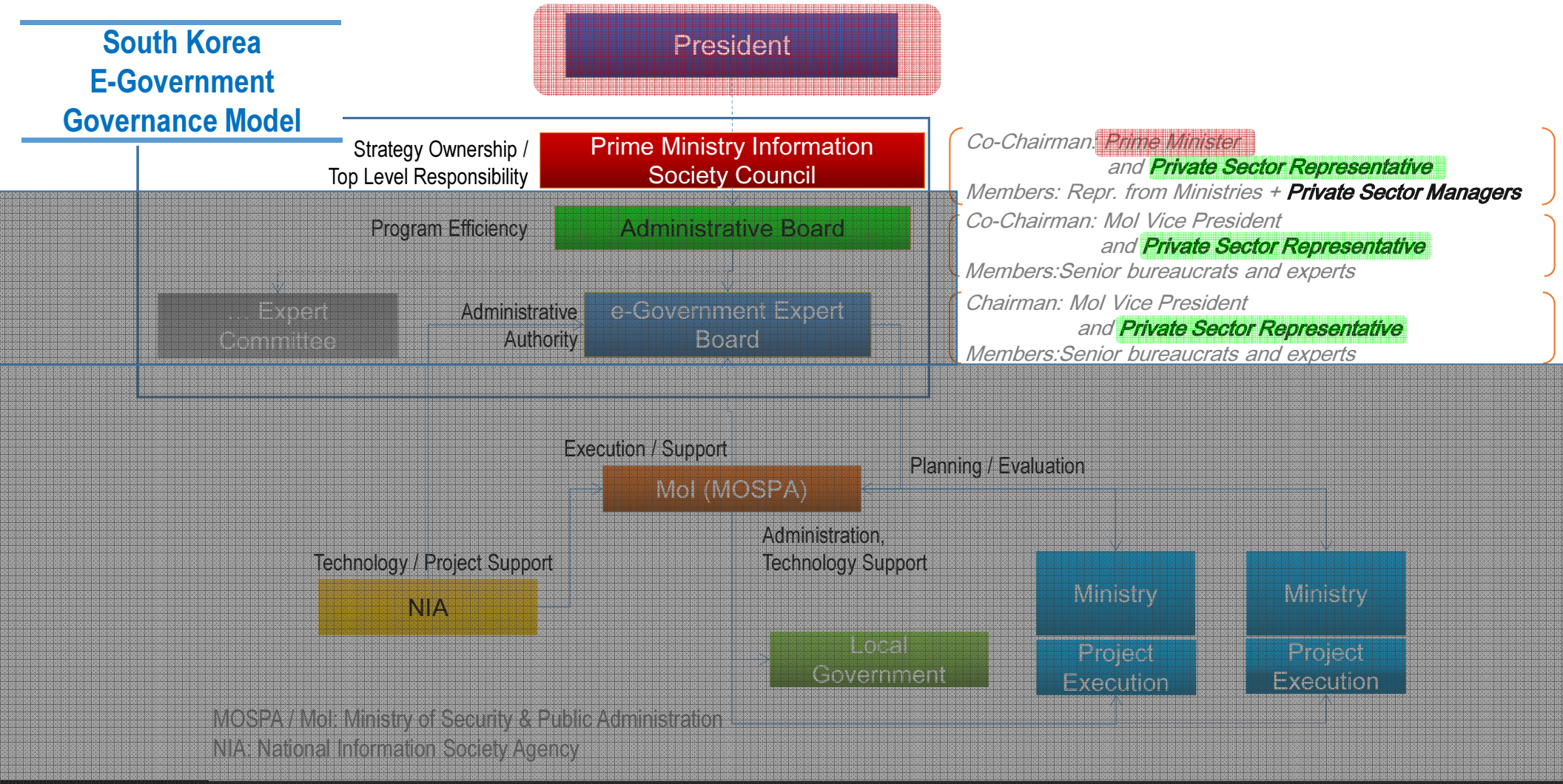


South Korea E-Government Governance Model

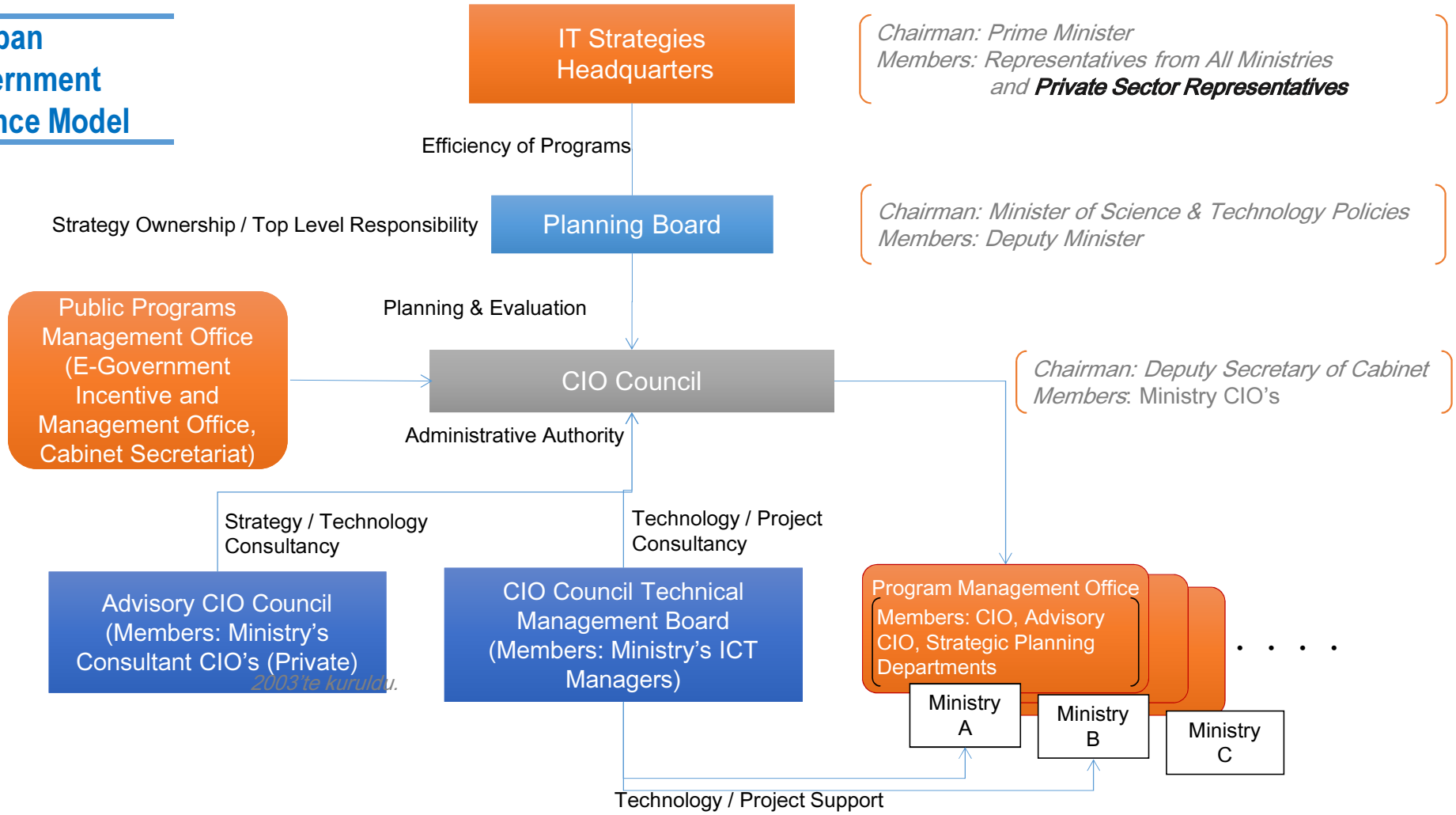


MOSPA / MoI: Ministry of Security & Public Administration
NIA: National Information Society Agency

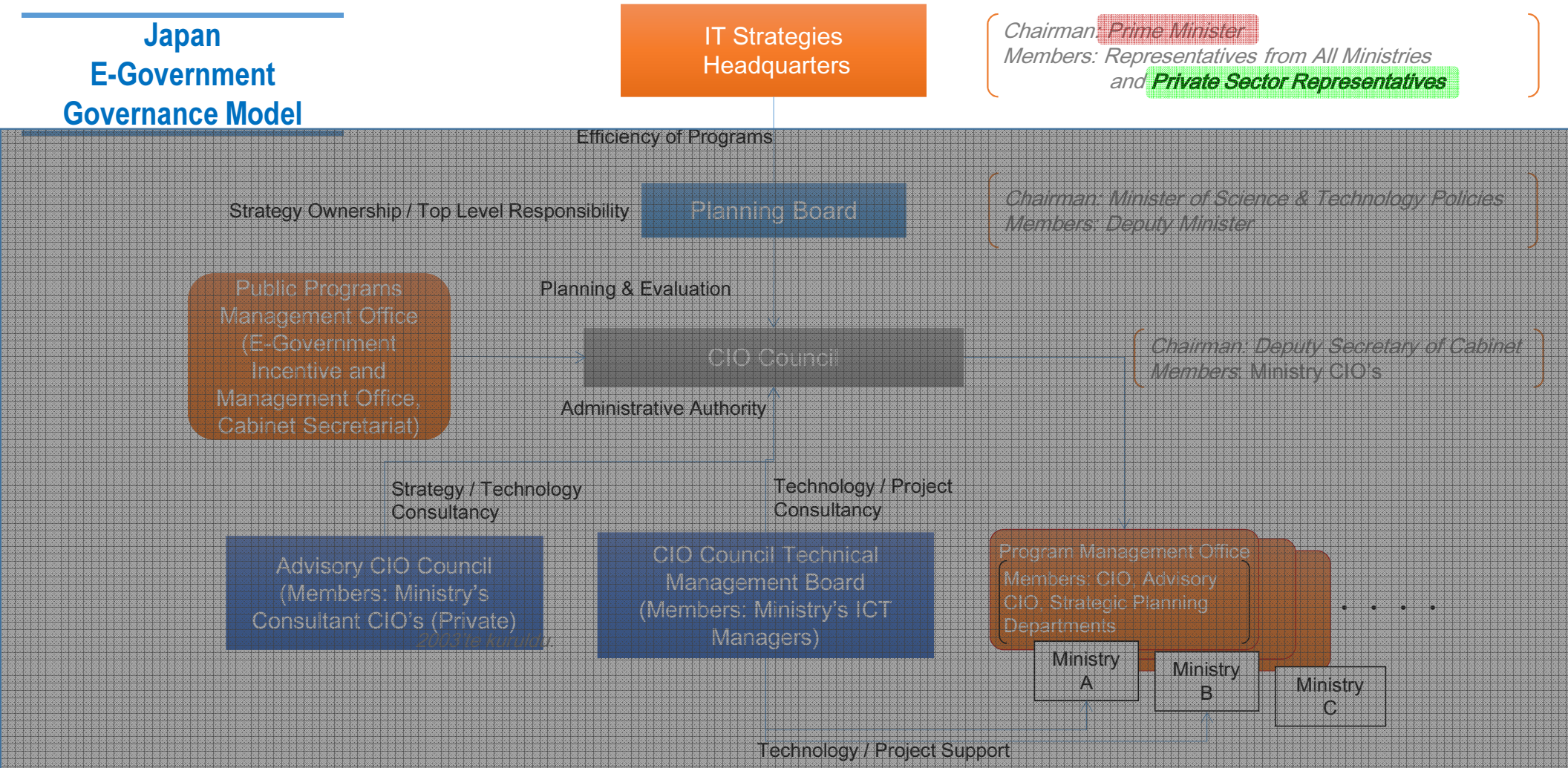
South Korea E-Government Governance Model



Japan E-Government Governance Model



Japan E-Government Governance Model



SUGGESTIONS : Coordination & Leadership

1. **Cyber Security** should be coordinated from top level in **ONE CENTERAL ADMINISTRATION**

2. In this Center, there should be **Public-Private Governance Board**

3. **National Cyber Security Policy** and **Prioritized Sectoral Areas** should be prepared

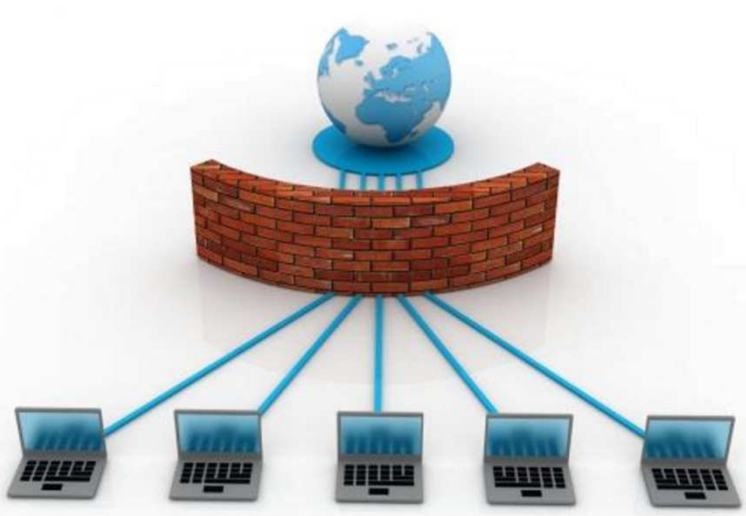
PRIVATE SECTOR

- National Solutions in «Perimeter Security» Layer:
  - National Firewall
  - National Intrusion Detection & Prevention systems
  - National Web Filtering
  - National Anti-virus Solutions

National "Cyber Thread Intelligence Bank (CTIB)"

PUBLIC

- National Operating System
- National E-Mail
- National Storage Cloud
- Secure Public Network



SUGGESTIONS : Capacity Building

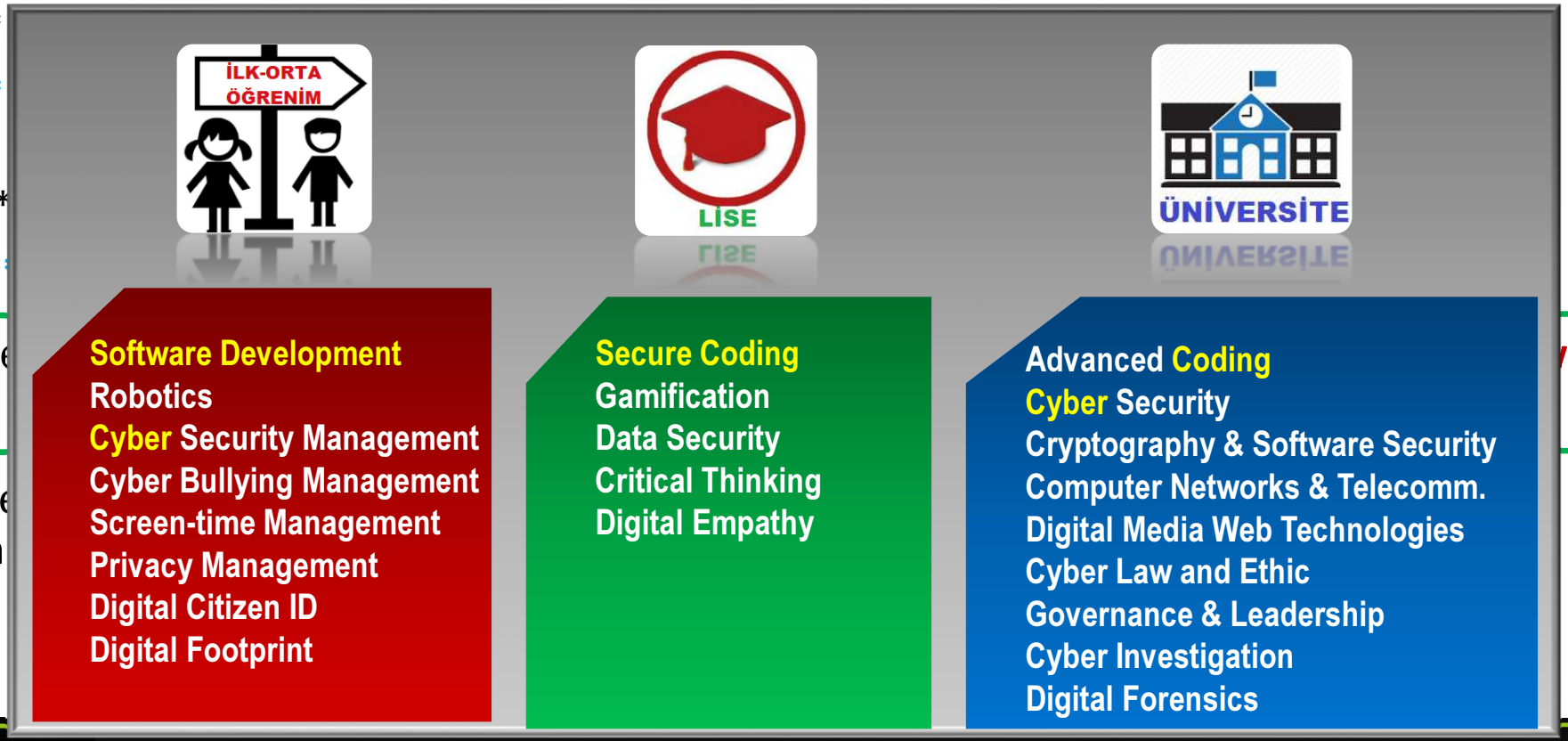
4. Government should support private sector, while developing **Sectoral Capacity**
   * Definitions of Cyber Security, Data Security and e-Government **Expertizes / Professions**
   * **Software Development** and **Cyber Security** Education Programs from Primary School to Universities
   * Preparation of **HR Capacity Developing Programs** for private sectotr
   * **Innovation** Incentives in prioritized areas

5. The government should be beside the sector in creating the **regional and global power** of the sector

6. Special incentives for the sector targeted to **grow in the region** (financial and administrative)

SUGGESTIONS : Capacity Building

4. Government should support private sector, while developing **Sectoral Capacity**



5. The
of the

6. Spe
admin

SUGGESTIONS : National Solutions

7. Use of **NATIONAL PRODUCTS** without exception as a **National Policy** in the public sector

«WE WILL USE FIRST !»

Dissemination Policy in Public Sector:

- «**Company Rating**» in public procurement with accreditation and certification
- Promotion Model: **R&D** → For successful results «**Production Support**» → Pilot Applications → Support & Development Infrastructure → Positioning in Public
- Current products in the first layer, **National Products** in the second layer
- After transition and maturity, national products in all layers
- At least two **National Solution Policy** in each segment
- **Regional Dissemination**

Cyber Security for National Security
«Coordination, Capacity Building and National Solutions»

Mustafa AFYONLUOĞLU
Cyber Security & e-Governance Chief Expert
afyonluoglu [at] gmail.com
Linkedin: http://linkedin.com/in/afyonluoglu
Twitter: http://twitter.com/#!/afyonluoglu
Web: afyonluoglu.com

teknoloji platformları
SİBER GÜVENLİK 4.0 ve FELAKET YÖNETİMİ
TEKNOLOJİ PLATFORMU - 25 NİSAN 2017 / İSTANBUL

25.04.2017