Siber Savunma (Saldırı) Organizasyonu

Nebi Şenol YILMAZ
Danışman / Yönetici Ortak
senol.yilmaz@secrove.com

Secrove Information Security Consulting

Hakkımda

- Nebi Şenol YILMAZ, CISA, CEH, ISO 27001 LA
- Secrove Information Security Consulting
  - Bilgi Güvenliği Danışmanlığı
  - Bilgi Sistemleri Denetimi
  - Penetrasyon Testleri
  - Zafiyet Araştırması
  - Exploit Geliştirme
  - Bilgi Güvenliği Ar-Ge (Tubitak Destekli)

Ajanda

- Ulusal Siber Güvenlik / Siber Savunma
- Siber Güvenlik Kurulu
- Siber Savaşlar ve Ülkeler
- Siber Savaşa Hazır mıyız?
- Siber Savunma (Saldırı) Organizasyonu
- Özet

Ulusal Siber Güvenlik / Siber Savunma

- Ulusal Güvenlik,
  - Harici güçleri savaştan caydırmak, ülkeyi ve varlıklarını korumak için gerekli tedbirler bütünü.

Ulusal Siber Güvenlik / Siber Savunma

- “Siber Pencere”den baktığımızda,
  - Ülkenin ve varlıklarının “siber ortamda” korunması için alınan tedbirler bütünü.

Ulusal Siber Güvenlik / Siber Savunma

- Ulusal Siber Güvenlik'te milat:

Bakanlar Kurulu Kararı: 2012/3842

"Ulusal siber güvenlik çalışmalarının yürütülmesi, yönetilmesi ve koordinasyonuna ilişkin karar"

Rega-28447
20 Ekim 2012

Siber Güvenlik Kurulu

20 Aralık 2012

- UDH Müsteşarı
- Milli Savunma Müsteşarı
- Genelkurmay MEBS Başkanı
- Kamu Düzeni ve Güvenliği Müsteşarı
- TÜBİTAK Başkanı
- UDH Bakanı
- Mali Suçları Araştırma Kurulu Başkanı
- BTK Başkanı
- TİB Başkanı
- MİT Müsteşarı
- İçişleri Müsteşarı
- Dışişleri Müsteşarı

Siber Güvenlik Kurulu

Strateji Belgesi doğrultusunda öngörülen,

- Ulusal Siber Güvenlik Eylem Planı
  - Siber güvenlik farkındalık çalışmaları
  - Ulusal Siber Olaylara Müdahale Merkezi
  - Siber güvenlik Ar-Ge politikası oluşturulması
  - İnsan kaynağı yetiştirilmesi
  - Yasal mevzuatın düzenlenmesi

Siber Savaşlar ve Ülkeler

Ülke Stratejileri

Siber Savaşlar ve Ülkeler

Ülke Stratejileri – 1
Almanya:

- Protection of critical information infrastructures
- National Cyber Response Centre
- National Cyber Security Council

- Tools to respond to cyber attacks

- Strengthening IT security in the public administration
- Secure IT systems in Germany

Siber Savaşlar ve Ülkeler

Ülke Stratejileri – 1
Almanya:

- Tools to respond to cyber attacks:

If the state wants to be fully prepared for cyber attacks, a coordinated and comprehensive set of tools to respond to cyber attacks must be created in cooperation with the competent state authorities. We will continue to assess the threat situation regularly and take appropriate protection measures. If necessary, we have to examine whether additional statutory powers must be created at federal or Länder level. Above all, the aims, mechanisms and institutions mentioned above must be internalized through a permanent exercise process with the relevant federal and Länder authorities as well as businesses.

Siber Savaşlar ve Ülkeler

Ülke Stratejileri – 2
İngiltere:

- Tackling cyber crime and making the UK one of the most secure places in the world to do business
- Making the UK more resilient to cyber attack and better able to protect our interests in cyberspace
- Helping to shape an open, vibrant and stable cyberspace which the UK public can use safely and that supports open societies

- Building the UK's cross-cutting knowledge, skills and capability to underpin all cyber security objectives

Siber Savaşlar ve Ülkeler

Ülke Stratejileri – 2
İngiltere:

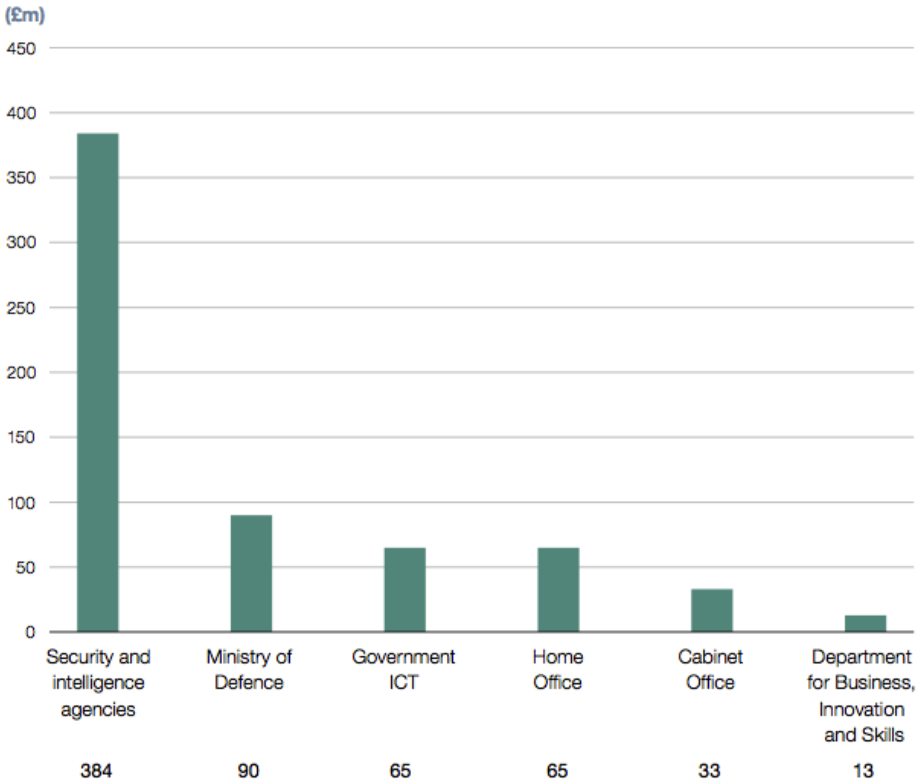
- Building the UK's cross-cutting knowledge, skills and capability to underpin all cyber security objectives

The intelligence agencies and Ministry of Defence have a strong role in improving our understanding of – and reducing – the vulnerabilities and threats that the UK faces in cyberspace. With the rise of cyber crime what was a concern primarily for the defence and intelligence elements of government is now something that concerns us all.

Siber Savaşlar ve Ülkeler

Ülke Stratejileri – 2
İngiltere:

£650 million			
2011-12	**2012-13**	**2013-14**	**2014-15**
£105m	£155m	£180m	£210m



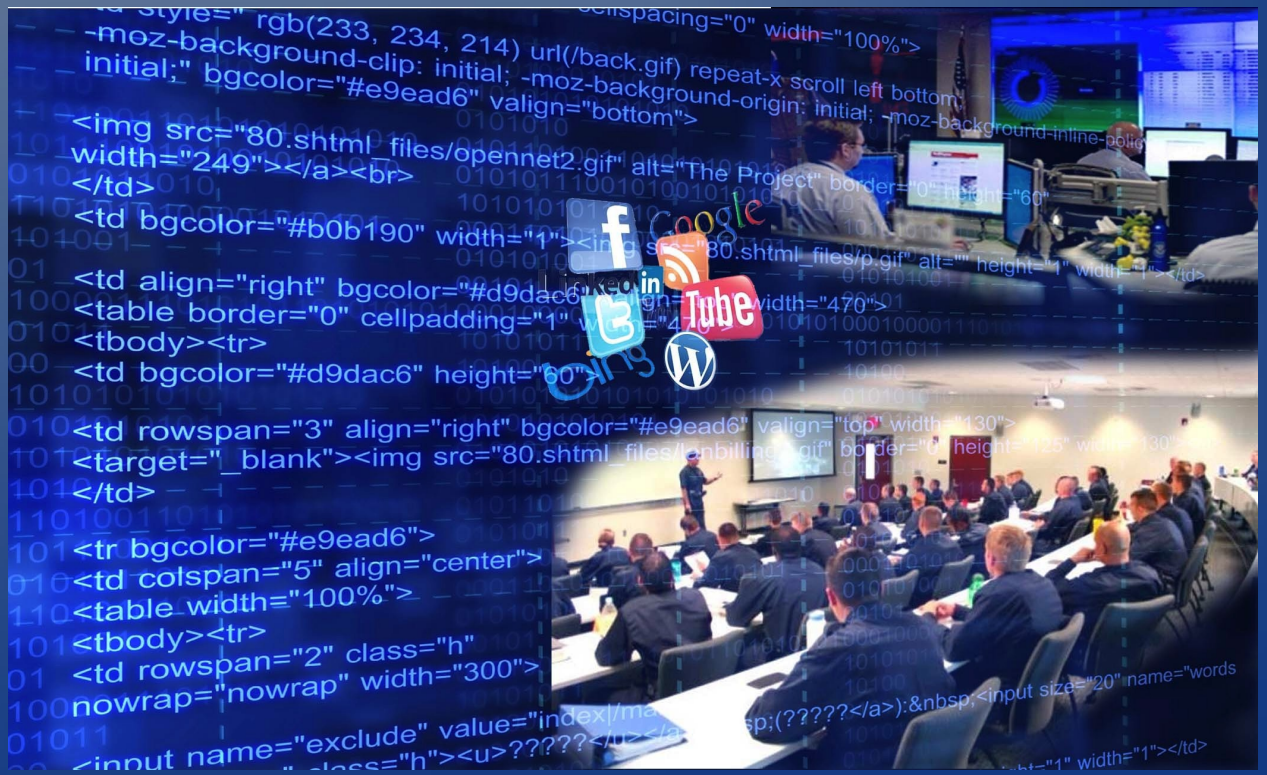
£ million	384	90	65	65	33	13
Percentage	59%	14%	10%	10%	5%	2%

Siber Savaşlar ve Ülkeler

Ülke Stratejileri – 3
ABD:

- Deploy an intrusion detection system of sensors across the Federal enterprise
- Pursue deployment of intrusion prevention systems across the Federal enterprise
- Coordinate and redirect research and development (R&D) efforts

- Develop and implement a government-wide cyber counterintelligence (CI) plan



Siber Savaşlar ve Ülkeler

Ülke Stratejileri – 3
ABD:

- Develop and implement a government-wide cyber counterintelligence (CI) plan:

A government-wide cyber counterintelligence plan is necessary to coordinate activities across all Federal Agencies to detect, deter, and mitigate the foreign-sponsored cyber intelligence threat to U.S. and private sector information systems. To accomplish these goals, the plan establishes and expands cyber CI education and awareness programs and workforce development to integrate CI into all cyber operations and analysis, increase employee awareness of the cyber CI threat, and increase counterintelligence collaboration across the government. The Cyber CI Plan is aligned with the National Counterintelligence Strategy of the United States of America (2007) and supports the other programmatic elements of the CNCI.

Siber Savaşlar ve Ülkeler

Ülke Stratejileri – 3
ABD:

- Develop and implement a government-wide cyber counterintelligence (CI) plan:

Cyber Intelligence Sharing and Protection Act

Siber Savaşlar ve Ülkeler

Ülke Stratejileri – 3
ABD:

- Develop and implement a government-wide cyber counterintelligence (CI) plan:

Siber Savaşlar ve Ülkeler

Bilinenler

- 2003 – Titan Rain

Çin – ABD

Çin'in “Hacker Asker”leri

Casusluk amacıyla, ABD savunma sanayi şirketlerine sızıldı.

Siber Savaşlar ve Ülkeler

Bilinenler

- Nisan 2007

  Rusya – Estonya

  Estonya devlet siteleri hedef alındı (DDoS ağırlıklı).

  NATO
  Siber Savunma Mükemmeliyet Merkezi kuruldu.

Siber Savaşlar ve Ülkeler

Bilinenler

- Haziran 2010 – Stuxnet

ABD & İrail – İran
Operation “Olympic Games”
(G.W. Bush, 2005-2006)
İran nükleer programına yönelik, worm saldırısı.

Scada sistemlerin zafiyetleri kullanıldı.

Casusluk ve sabotaj.

Siber Savaşlar ve Ülkeler

Bilinenler

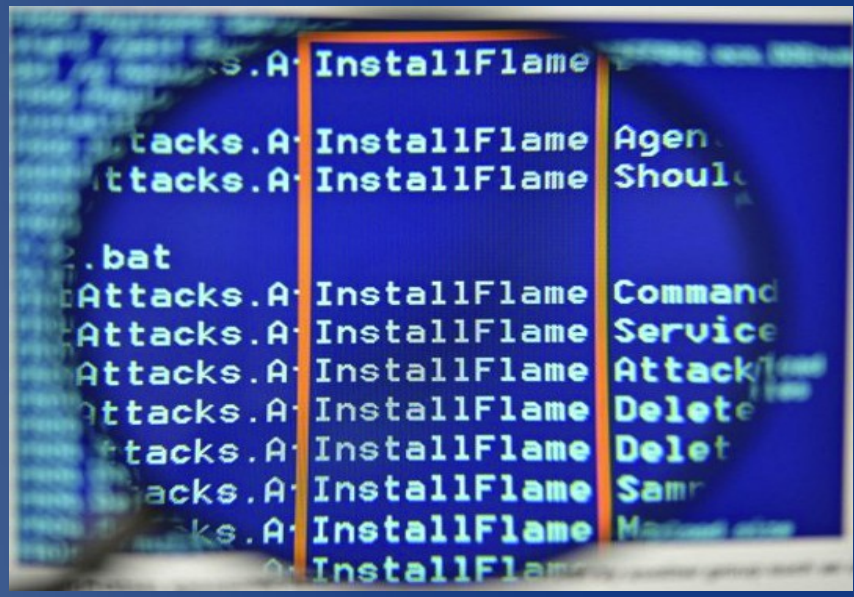
- Eylül 2011 – Duqu

ABD – İran
Stuxnet'e benzer yönleri mevcut

İran nükleer programına yönelik

Casusluk amaçlı görünüyor.

Siber Savaşlar ve Ülkeler



Bilinenler

- Mayıs 2012 – Flame

ABD & İsrail – İran, Ortadoğu
Operation “Olympic Games”
(G.W. Bush, 2005-2006) (Parallel to Stuxnet)

Sabotaj'dan çok ortadoğuda casusluk amaçlı kullanılıyor.

Siber Savaşlar ve Ülkeler

Bilinenler

- Mart 2013 – Güney Kore

  Güney Kore bankaları ve Medya kanalları “hack”lendi.

  Kuzey Kore - Güney Kore

  Karşılıklı olarak “Hacker Ordusu” yetiştiriyor.

Siber Savaşlar ve Ülkeler

Bu da bir istihbarat anlaşması mı?

Canonical, the makers of Ubuntu have announced that they will be officially affiliated with the Chinese government to bring a new Ubuntu based OS to the Chinese population.

Siber Savaşlar ve Ülkeler

ve aslında liste uzayıp gidiyor...

Siber Savaşa Hazır mıyız?

- Siber Güvenlik çalışmaları başlatıldı.
- Kamuda ciddi olarak bilinçlenme adımları atılıyor.
- Siber Savunma Merkezi kuruldu.
- USOM kuruluyor.

...

- Siber istihbarat
- “Offensive Security” için neler yapılıyor?

Siber Savunma (Saldırı) Organizasyonu

Savunma (Defensive)

Eğitim (Training)

Atak (Offensive)

Siber Savunma (Saldırı) Organizasyonu

Ofansif olarak,

- Casusluk (Espionage)
- Sabotaj (Sabotage)
- Siber İstihbarat (Cyber Intelligence)

çalışmalarının yürütülmesi gerekmektedir.

ABD başta olmak üzere, Çin, İngiltere, Güney Kore ve Kuzey Kore yıllardır ciddi çalışmalar yaptı.

Siber Savunma (Saldırı) Organizasyonu

- Siber savunmaya(*) yönelik ürün ihracatının desteklenmesi
- Exploit geliştirme çalışmalarının desteklenmesi
- Malware/Worm anlizi ve geliştirme çalışmalarının desteklenmesi
- Tehdit potansiyeli olan ülkelere/organizasyonlara karşı keşif mekanizmalarının oluşturulması
- Aktif saldırı durumunda karşı atak mekanizmalarını planlanması

gerekmektedir.

Özet

Siber savunmada belirleyici kriterler:

- Ne kadar hazırlıklısınız?
- Ne kadar yeteneklisiniz?
- Düşman hakkında ne kadar bilgiye sahipsiniz?

“Foreknowledge is main part of winning strategy...”

Sun Tzu

Teşekkürler !

http://www.secrove.com/

senol.yilmaz@secrove.com

@nsyilmaz

nsyilmaz