



KRİTİK BİLGİ ALTYAPILARI VE SİBER GÜVENLİK

Bilge KARABACAK

Siber Güvenlik Konferansı

22 Aralık 2011

- Kritik Altyapılar / Kritik Bilgi Altyapıları
 - SCADA Sistemleri
- Kritik Altyapılara Yönelik Siber Tehditler
- Karşı Önlemler

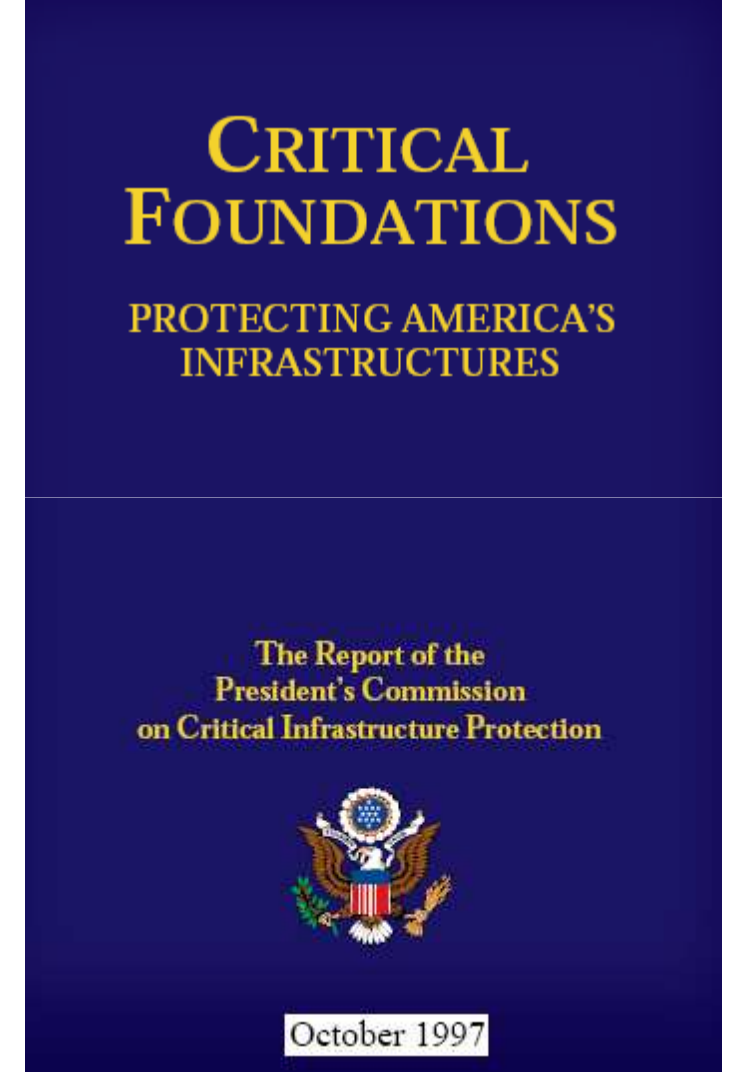
Kritik Altyapılar – Tarihçe & Tanım

Ekonominin ve devletin düzeni için gerekli olan fiziksel ve **siber** sistemler.

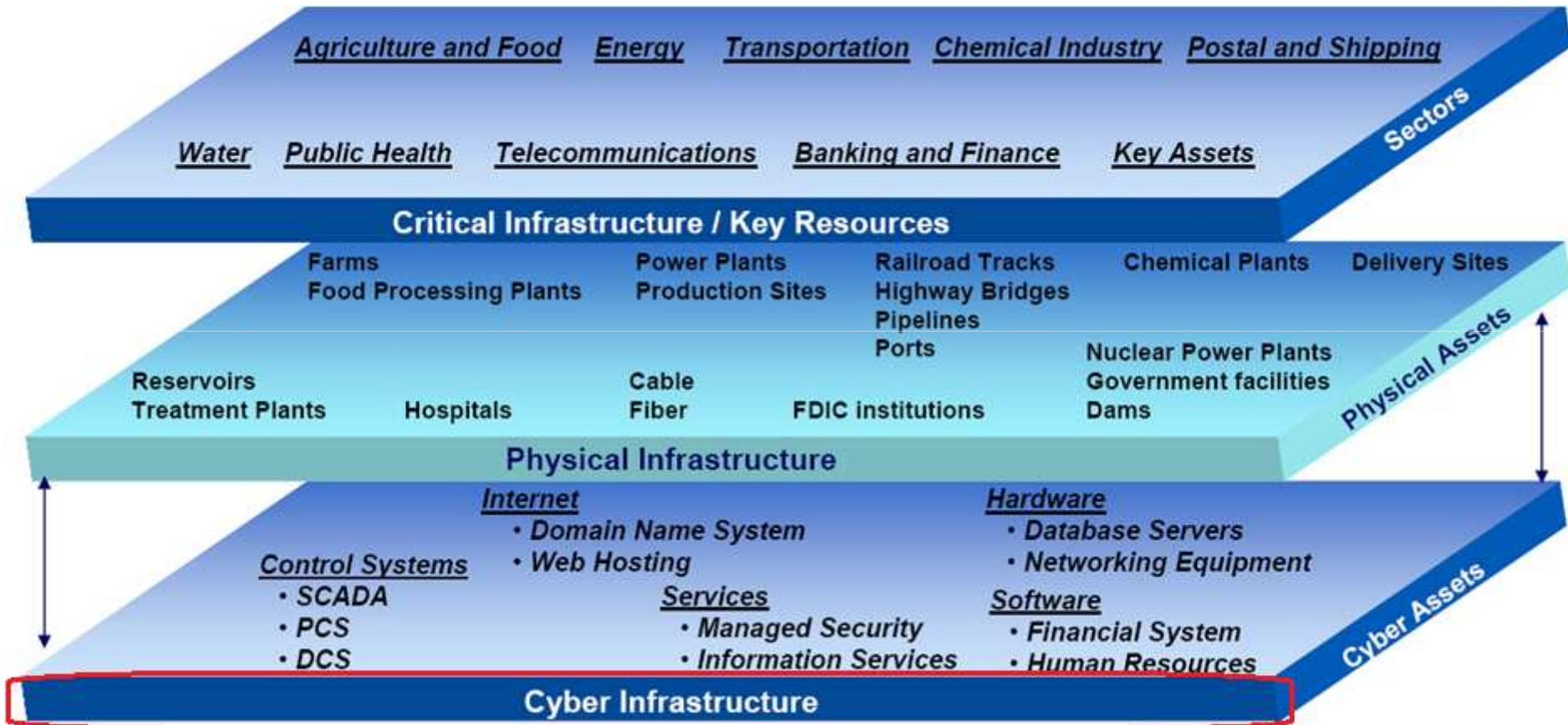
Kamu ve özel sektör tarafından işletilen:

- iletişim,
- enerji,
- finans,
- ulaşım,
- su sistemleri,
- acil durum servisleri.

Geçmişte kritik altyapılar fiziksel ve mantıksal olarak ayrıldı. **Bilgi teknolojilerindeki** gelişmeler, kritik altyapıların **otomasyonunu**, birbirilerine olan **bağımlılıklarını** ve **ilişkilerini** gün geçtikçe artırmakta.



Siber Altyapı ve Kritik Altyapılar



BT'yi kullanan kritik altyapılar:

- Ulaşım
- Bankacılık ve finans
- Sağlık ve acil durum servisleri
- Kritik kamu servisleri

Tamamen BT'den oluşan kritik altyapılar:

- Telekomünikasyon

SCADA ile kontrol edilen ve izlenen kritik altyapılar:

- Kritik üretim tesisleri
- Enerji ve su

BT'yi kullanan kritik altyapılar

Tamamen BT'den oluşan kritik altyapılar

SCADA ile kontrol edilen ve izlenen kritik altyapılar

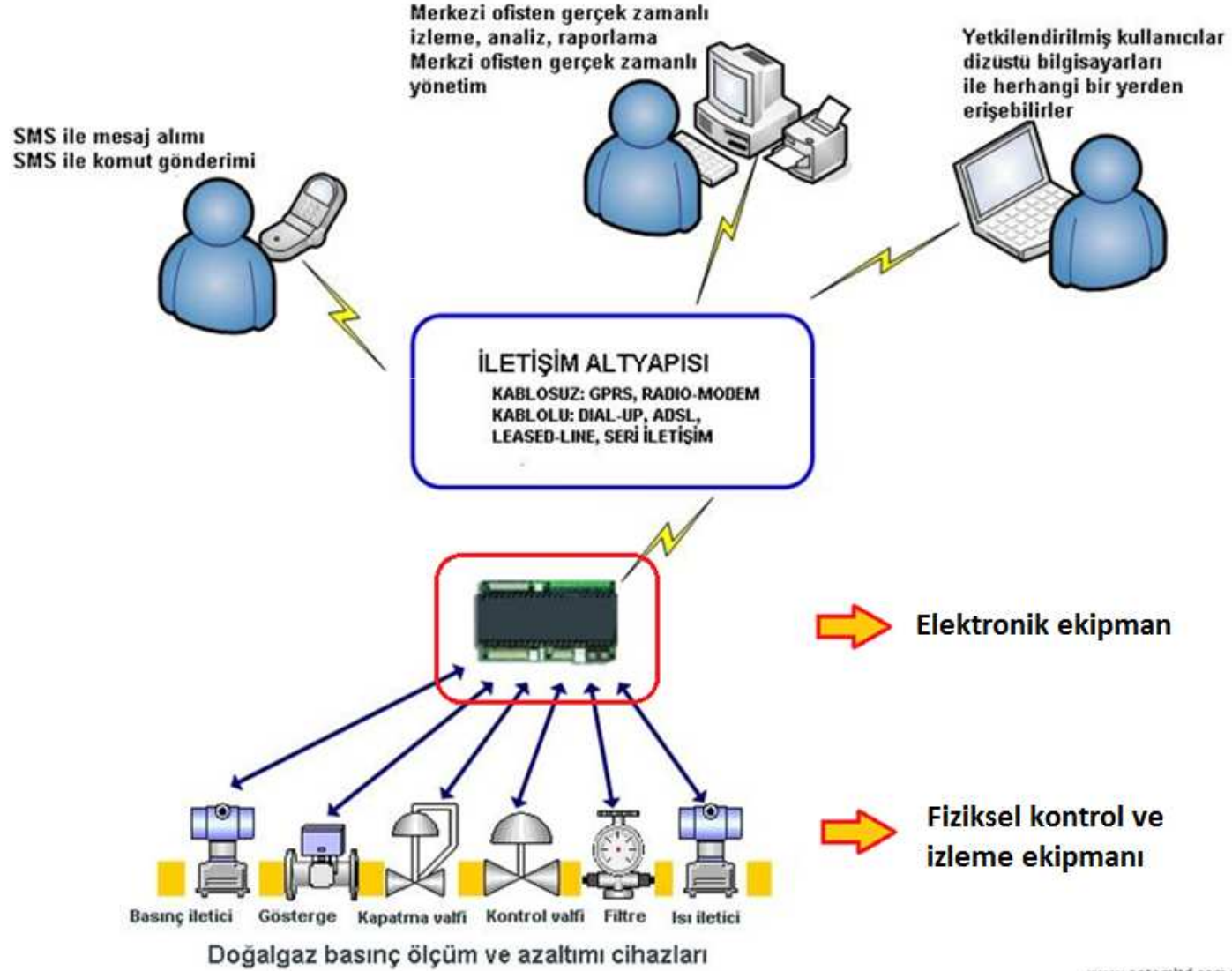
Kritik bilgi altyapılarını, fonksiyonelliğini yitirmesi durumunda sağlık hizmetlerine, toplumsal emniyet ve güvenliğe, vatandaşların ekonomik refahına veya hükümetin/ekonomünün verimli çalışmasına ciddi yönde tesir eden bilgi ağları ve sistemleridir.

Endüstriyel sistemlerin izlenmesi ve kontrolü:

- Barajlar
- Sulama sistemleri
- Elektrik üretim ve dağıtım sistemleri
- Petrol rafinerileri
- Gaz iletim sistemleri
- Fabrikalar

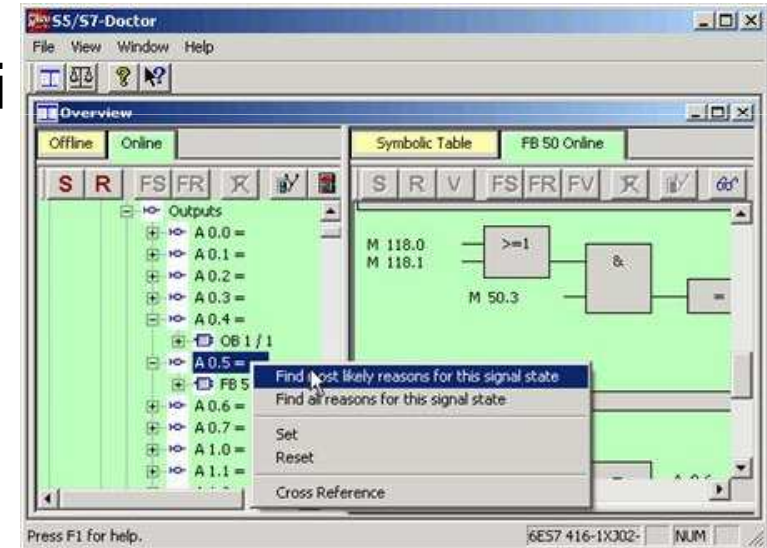


DOĞALGAZ DAĞITIM ŞEBEKESİ İZLEME VE KONTROL SİSTEMİ

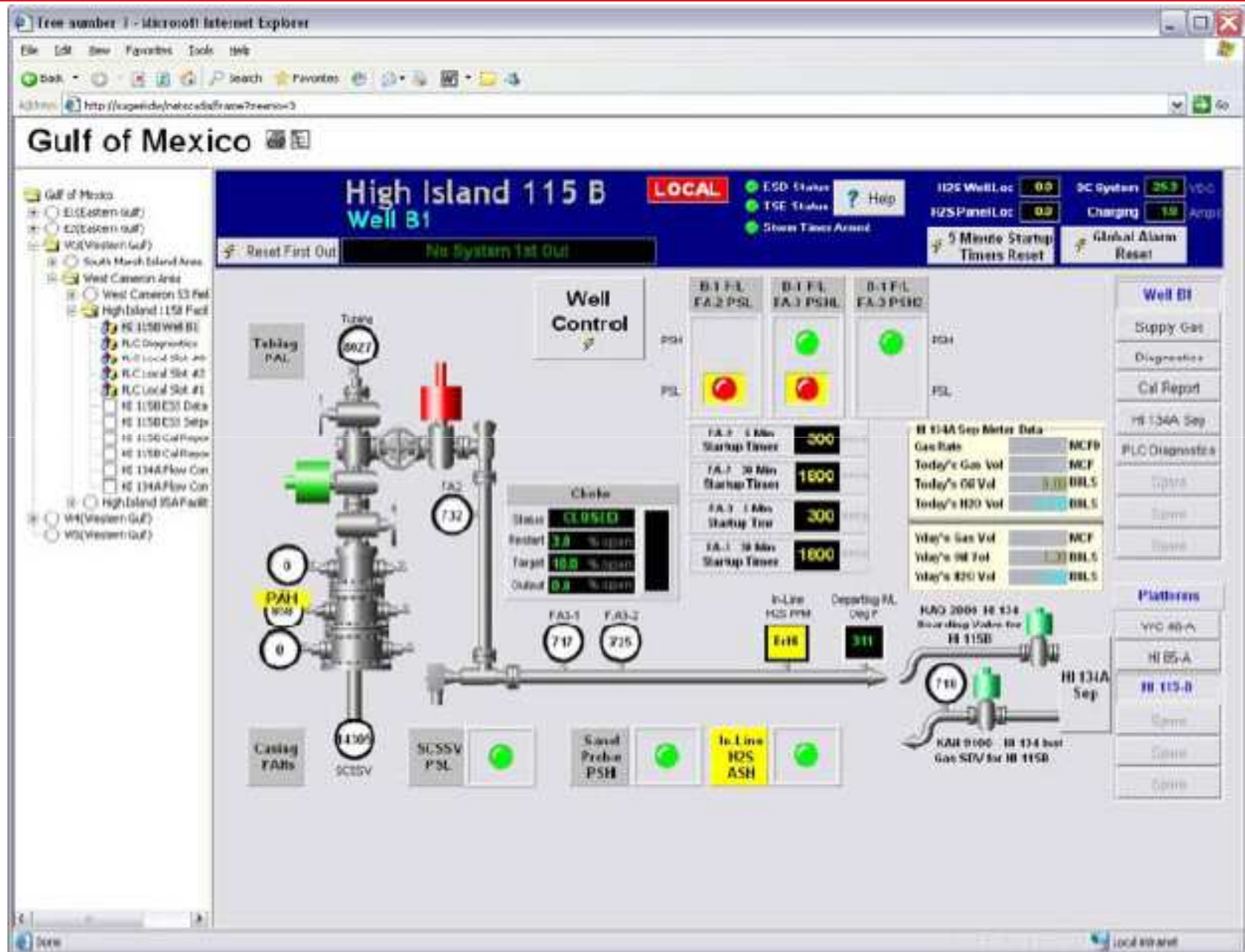


SCADA: Dünü ve Bugünü

- 1970 - 1990
 - Özelleşmiş
 - İzole
- Bugün
 - Standart donanım
 - Standart işletim sistemi
 - Standart protokol
 - Dokümante
 - Bağlantılı
 - Kablosuz
 - Internet
 - Ethernet, TCP/IP, Windows, RPC, SMB, 802.11b, HTTP/HTTPS, Unix/Linux/Solaris, SQL



SCADA – Meksika Körfezi Web Tarayıcı Yönetim Arayüzü



Gulf of Mexico

High Island 115 B Well B1 LOCAL

Reset First Out **No System 1st Out**

Well Control

Close

Status	CLOSED
Restart	3.8 %/hour
Target	18.8 %/hour
Output	0.8 %/hour

FA-1 1 Min Startup Times	300
FA-2 30 Min Startup Times	1000
FA-3 1 Min Startup Times	300
FA-1 30 Min Startup Times	1000

HI 134A Sep Meter Data

Gas Rate	MCFB
Today's Gas Vol	MCF
Today's G0 Vol	0.00 BBL5
Today's H2O Vol	BBL5
Yday's Gas Vol	MCF
Yday's G0 Vol	0.00 BBL5
Yday's H2O Vol	BBL5

Platform

YOC 40-A

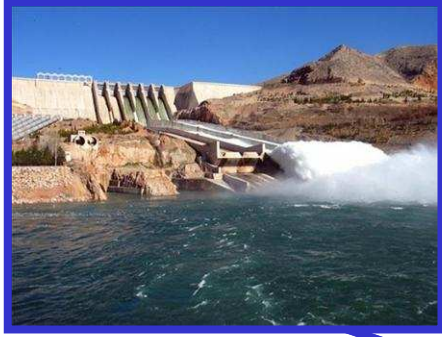
HI 115-A

HI 115-B

HI 134A Sep

KAR 0100 - HI 134 best Gas STD for HI 115B

Siber Uzay



INTERNET = Siber Uzay
Fiziksel olarak dağıtık ...
Mantıksal olarak tek ...



Dijital savaş çağı



Bir ülkenin başta su ve elektrik şebekesi olmak üzere kritik altyapı sistemini bilgisayar ağları üzerinden vuran sanal saldırıların ciddiyeti artıyor. Hükümetler büyük mali kayba yol açan saldırılara karşı önlem arıyor.

Bir ülkenin başta su ve elektrik şebekesi olmak üzere kritik altyapı sistemini bilgisayar ağları üzerinden vuran sanal saldırıların ciddiyeti artıyor. Hükümetler büyük mali kayba yol açan saldırılara karşı önlem arıyor.

Siber savaş, sanal saldırı ve dijital muharebe... Bunlar, İnternet'in hızlı

gelişimiyle birlikte son yıllarda giderek daha fazla işittiğimiz kavramlar. Tanımlamak gerekirse; ekonomik, politik veya askeri amaçlar için bir ülkeye yönelik bilgi ve iletişim sistemleri üzerinden gerçekleştirilen organize saldırıların tamamına siber savaş adı veriliyor. Bu saldırılarda bir ülke açısından son derece kritik altyapı tesisleri hedef alındığından hükümetler de bu konuya artık daha fazla ağırlık veriyor.

Güvenlik uzmanı Kevin Coleman, sanal saldırı yöntemlerini tatbik etmeyen ülkenin kalmadığını belirtiyor. Coleman'a göre İnternet ağına bağlı olmayan az sayıdaki ülke dışında hemen bütün dünyada bu yöneme başvuruluyor.

"Sanal dünyada her an milyonlarca saldırı düzenleniyor. Bir ay içinde Çin'den dakikada 128 adet sanal saldırı girişimi kaydedildi. Bu saldırılar, askeri birimlerin dışında, kamu ve özel sektöre ait kuruluşları hedef alıyordu. Mali ve ekonomik alanın dışındaki saldırıları da hesaba katarsanız karşınıza muazzam büyüklükte bir sorun çıkıyor."



İlk siber savaşın galibi 'Kızıl Ordu'

Geçtiğimiz ay sessiz sedasız ve yöntem olarak benzersiz bir savaş yaşandı. Rusya, Estonya'ya organize bir saldırı düzenledi ve ülkenin ticaret ve kamu düzenini dize getirmeyi başardı

[04/06/2007](#) (6756 defa okundu)

1918 yılında Alman ordularına yenilen Rusya'dan bağımsızlığını ilan eden Estonya, aynı Almanya'nın Rusya ile yaptığı gizli bir anlaşmanın ardından 1940 yılında Rus askerlerinin işgaliyle başlayan süreçte Sovyet Sosyalist Cumhuriyetler Birliği'nin bir üyesi olmak zorunda kalmıştı. 1989'da şarkılarla başlayan kıpırdanmanın ardından 1991 yılında sonunda Estonya yeniden bağımsızlığını kazandı. Ancak bu yeni süreçte Rusya'nın Estonya üstündeki hâkimiyet arzusunun söndüğü de söylenemez. Bunun son örneklerinden biri de geçtiğimiz günlerde internette yaşandı.

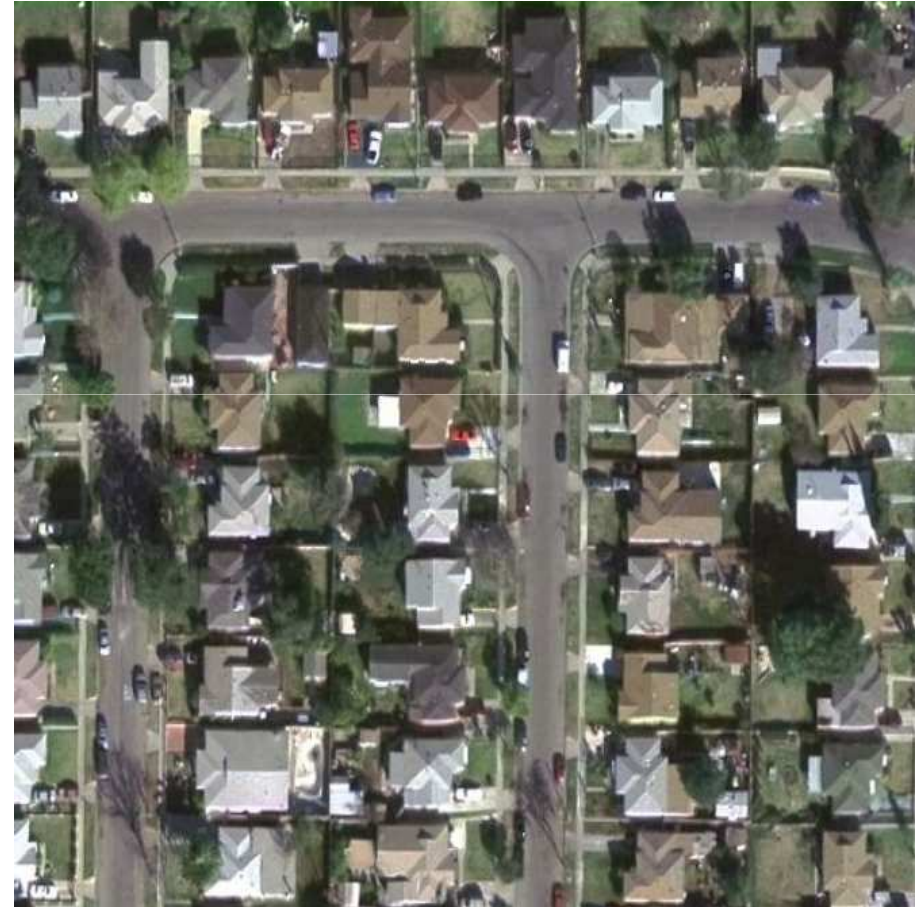


Tanklar eşliğinde yeri göğü inleterek bir ülkeyi dize getirmek hâlâ mümkün. Ama artık başka yollar da var.

Nükleer Silah Tesisi



Siber Silah Tesisi



Asimetrik Siber Tehdit – Elde Edilebilirlik



Uçak maliyeti:

100.000.000 dolar



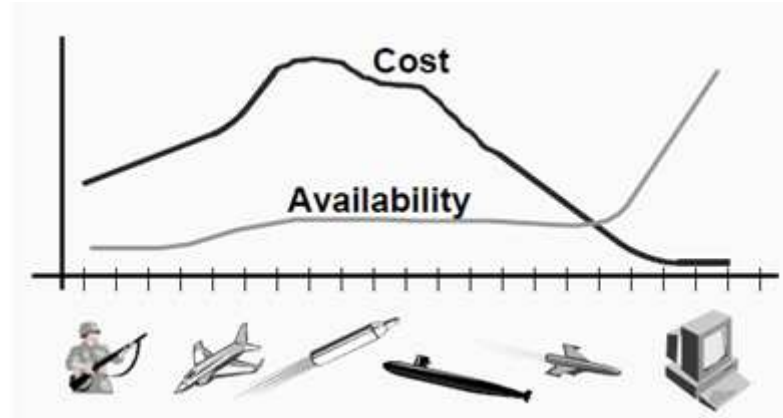
Kruz füzesi maliyeti:

1.000.000 dolar



Siber silah maliyeti:

10 – 50,000 dolar



 SecurityFocus™ 19 August 2003

Slammer worm crashed Ohio nuke plant network

The Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant in January and disabled a safety monitoring system for nearly five hours, despite a belief by plant personnel that the network was protected by a firewall, SecurityFocus has learned.

The breach did not pose a safety hazard. The troubled plant had been offline since February, 2002, when workers discovered a 6-by-5-inch hole in the plant's reactor head. Moreover, the monitoring system, called a Safety Parameter Display System, had a redundant analog backup that was unaffected by the worm. But at least one expert says the case illustrates a growing cybersecurity problem in the nuclear power industry, where interconnection between plant and corporate networks is becoming more common, and is permitted by federal safety regulations.



Aussie hacker gets two year sentence

A Queensland court has sentenced a local computer hacker to two years jail. A Maroochydore District Court jury convicted Vitek Boden of hacking into the computer-controlled sewerage system of the local council and deliberately releasing raw sewerage into local creeks and parks.

He was sentenced for 12 months for wilfully causing serious environmental harm, and also received a two year sentence for several computer hacking and theft charges.

The sentences will be served concurrently.

31 October 2001

Los Angeles Times

13 August 2001

Power Grid Vulnerable to Hackers

For two weeks last spring, hackers wormed their way inside a computer system that plays a key role in moving electrical power where it is needed around the state. The computers belong to the California Independent Service Operator, an agency that oversees much of the state's electricity transmission grid—including the massive complex of power plants and transmission lines.

Cal-ISO patched the flaw that allowed hackers to roam through portions of its network before power supplies were affected. But the episode sent shock waves throughout the energy industry.

Stuxnet worm 'targeted high-value Iranian assets'

By Jonathan Fildes

Technology reporter, BBC News



23 September 2010 Last updated at 10:46 GMT

One of the most sophisticated pieces of malware ever detected was probably targeting "high value" infrastructure in Iran, experts have told the BBC.

Stuxnet's complexity suggests it could only have been written by a "nation state", some researchers have claimed.

It is believed to be the first-known worm designed to target real-world infrastructure such as power stations, water plants and industrial units.

It was first detected in June and has been intensely studied ever since.



Some have speculated the intended target was Iran's nuclear power plant

Stuxnet Worm Still Out of Control at Iran's Nuclear Sites, Experts Say

By Ed Barnes
Published December 09, 2010 | FoxNews.com



Iran International Photo Agency, via AFP

Aug 21: The first fuel is loaded into the reactor building at the Russian-built Bushehr nuclear power plant in Iran.

EXCLUSIVE: Iran's nuclear program is still in chaos despite its leaders' adamant claim that they have contained the computer worm that attacked their facilities, cybersecurity experts in the United States and Europe say.

The American and European experts say their security websites, which deal with the computer worm known as Stuxnet, continue to be swamped with traffic from Tehran and other places in the

Islamic Republic, an indication that the worm continues to infect the computers at Iran's two nuclear sites.

The Stuxnet worm, named after initials found in its code, is the most sophisticated cyberweapon ever created. Examination of the worm shows it was a cybermissile designed to penetrate advanced security systems. It was equipped with a warhead that targeted and took over the controls of the centrifuge systems at Iran's uranium processing center in Natanz, and it had a second warhead that targeted the massive turbine at the nuclear reactor in Bashehr.

Stuxnet was designed to take over the control systems and evade detection, and it apparently was very successful. Last week President Mahmoud Ahmadinejad, after months of denials, admitted that the worm had penetrated Iran's nuclear sites, but he said it was detected and controlled.

Şimdiye Kadar Geliştirilmiş En Karmaşık Siber Silah !

- Sadece belli SCADA sistemlerini hedef alan bir solucandır. (Siemens SCADA sistemi)
- Windows işletim sisteminin dört adet bilinmeyen açıklığını kullanmıştır.
- Kötücül yazılımların programlanmasında yaygın olarak kullanılmayan bir programlama dili kullanılmıştır.
- Güney Kore'deki iki adet firmaya ait sayısal sertifikaların gizli anahtarları ile imzalanmıştır.
- Siemens'in ilgili yazılımı yok ise kendisini etkisiz hale getirmektedir.

Keşif Uçağı: DUQU

- Stuxnet ile ciddi benzerlikler taşıyor.
- Keşif tarihi: 1 Eylül 2011
- Bulaşma şekli: e-posta ortalama
- Stuxnet: zarar verir / Duqu: istihbarat toplar
- Zero-day açıklık kullanıyor. (Üretici açıklaması: 3 Kasım 2011)
- Sürücü dosyası dijital sertifika ile imzalı.
- Kendisini kopyalamıyor. (C&C sunucusu bulaştırır).
- İletişim kuramazsa 1 ay sonra kendisini siler.
- Anormal ağ trafiğı yaratmıyor.
- En çok İran'daki kuruluşlar etkilenmiş.

The CHRISTIAN SCIENCE
MONITOR

Exclusive: Iran hijacked US drone, says Iranian engineer (Video)

In an exclusive interview, an engineer working to unlock the secrets of the captured RQ-170 Sentinel says they exploited a known vulnerability and tricked the US drone into landing in Iran.

By Scott Peterson, Staff writer, Payam Faramarzi*, Correspondent / December 15, 2011



- Iran guided the CIA's "lost" stealth drone to an intact landing inside hostile territory by exploiting a navigational weakness long-known to the US military, according to an Iranian engineer now working on the captured drone's systems inside Iran.

HABER TURK

Atatürk Havalimanı'nda virüs kabusu

Bilet ve bagaj işlemleri aksadı!



TÜBİTAK'ın uyardığı "downadup" adındaki "networm" virüsü Atatürk Havalimanı Dış Hatlar Terminali'ndeki sistemleri de etkiledi. Bilet ve bagaj işlemlerinin yapıldığı SITA-CUTE sistemleri bozulunca işlemler elle yapıldı.

Birçok yolcunun bagajları havalimanında kaldı. TAV, virüs nedeniyle sistem problemi yaşandığını doğruladı.

TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) bünyesinde faaliyet gösteren Türkiye Bilgisayar Olayları Müdahale Ekibi (TR-BOME), bilgi sistemlerinde hızla yayılan yeni bir solucanı "acil" koduyla bildirdi.





Batman Barajı şifrelendi

28.5.2003

Alman firması, parasını alamadığı gerekçesiyle bilgisayarları kilitledi

Bilgisayarların şifrelenerek kilitlemesi nedeniyle Batman Barajı'nda enerji üretimi yapılamadığını söyleyen DSI yetkilileri, bu nedenle Batman'ın bazı ilçeleri ile Şırnak ve Cizre'ye kesintili olarak elektrik verebildiklerini belirttiler. Barajın yeniden elektrik üretimine başlaması için şifreyi çözmek üzere Türkiye Elektromekanik Sanayi uzmanları da yoğun çalışmalarını sürdürüyor. Uzmanlar bir yandan şifreyi çözmeye, bir yandan da Alman firması yetkililerine ulaşmaya çalışıyor. Batman Barajı Hidroelektrik Santralі'nin yapımını üstlenen Alman Noel Şirketi, 1 milyon dolar alacağını tahsil edemediği gerekçesiyle şirketin bilgisayarlarını şifre ile kilitleyip, kenti terketti. Şifreleme nedeniyle santralın üç ünitesinde de enerji üretimi durdu.



260 milyar dolarlık borsa bir kepçe darbesiyle çöktü

Yol çalışmasında bir kepçe veri kablolarını kopardı. Borsa idaresi hasardan işlem saati yaklaşırken haberdar oldu. Taşeron tamircileri grevdeki sendika durdurdu

29 Kasım 2007





Gönen HES gerek mimari gerekse ergonomik kullanım yönünden Türkiye' deki santralle içinde en modern olarak inşa edilmiş Bölgemizin ilk Hidroelektrik Santralidir. Yap - İşlet - Devret Modeli ile kurulup üretime geçen ilk Hidroelektrik Santrali olan Gönen HES manuel olarak kumanda edilebildiği gibi PLC sistemi ile yarı otomatik olarak veya SCADA sistemi ile kontrol odasından tam otomatik olarak veya uzaktan (başka bir şehirden) kumanda edilerek, bilgisayarla insansız çalıştırılabilen ilk santral olma özelliğini de taşımaktadır.

- En gelişmiş güvenlik sistemleri:
 - Sayısal imzalar
 - Kriptografik önlemler
 - Biometrik güvenlik
 - Güvenlik duvarları
 - Saldırı engelleme sistemleri
 - Erişim kontrol sistemleri
 - İnternet erişimine kapalı ağ !!!
- En zayıf halka: İnsan
 - USB bellekler !!!



by Elinor Mills

USB thumb drives are convenient, popular and often free—and they're spreading viruses like sailors on shore leave.*

The US-CERT (Computer Emergency Response Team) issued a warning on Thursday that malicious code is increasingly propagating via USB flash drive devices.


Meanwhile, the U.S. Department of Defense has temporarily banned the use of thumb drives, CDs, and other removable storage devices because of the spread of the Agent.bzt virus, a variant of the SillyFDC worm, according to Wired.

We've seen this before with portable external storage devices. Floppy disks were the culprit in the early 1990s, followed by CDs. The fact that USB thumb drives are being used by so many people makes them an attractive target for virus writers.

"The bad guys are intentionally developing new flavors of malware designed to propagate through USB devices," said Gunter Ollmann, chief security strategist for IBM's ISS security division. "They are today's floppy drives."

WIRED

Under Worm Assault, Military Bans Disks, USB Drives

By Noah Shachtman  November 19, 2008 | 3:12 pm | Categories: [Info War](#)

The Defense Department's geeks are spooked by a rapidly spreading worm crawling across their networks. So they've suspended the use of so-called thumb drives, CDs, flash media cards, and all other removable data storage devices from their nets, to try to keep the worm from multiplying any further.

The ban comes from the commander of U.S. Strategic Command, according to an internal Army e-mail. It applies to both the secret [SIPR](#) and unclassified [NIPR](#) nets. The suspension, which

includes everything from external hard drives to "floppy disks," is supposed to take effect "immediately." Similar notices went out to the other military services.



- En kritik karşı önlem:

1. Kullanıcı bilinçlendirmesi

(Kullanıcı = bilgisayar operatörü, sistem yöneticisi, kurum yöneticisi = **herkes**)



En Temel ve Öncelikli Dört Adım:

1. Üst seviye yürütmeden (Örn: Başbakanlık) destek ve katılım
2. Destekleyen mevzuatın hazırlanması ve yürürlüğe girmesi
3. Kritik altyapıların korunması ile ilgili politika belgesi hazırlanması
4. Çalışmalar için yeterli seviyede bütçe ayrılması



Kurumsal Yapılanma ve İşbirliği:

- Kritik altyapılarla ilgili çalışmalarını koordine eden merkezin kurulması
- Hükümet birimleri ve kritik altyapı işletmecileri (özel, kamu) arasında ilişkilerin kurulması
- Özel sektör ile işbirliği ve koordinasyon
- Diğer ülkeler ve uluslararası organizasyonlarla işbirliği



Teknik Karşı Önlemler

- Güncel kalma
 - Açıklıkların yamalarının yapılması
 - Son teknoloji karşı önlemlerin tedariki ve kurulması
- Güvenlik ve teknoloji tasarımı
 - Güvenliğin bir tasarım konusu olması, sonradan ek yapılmaması
 - COTS ürünlerin kullanımının kısıtlanması
 - Sertifikalı yazılım ve donanım kullanımı
 - Erişim kontrol sistemlerinin kullanımı
- USB belleklerin kullanımının kısıtlanması !



Karşı Önlemler - 5

- Periyodik güvenlik testleri ve denetimleri
- Aktif siber güvenlik takımları
 - Siber istihbarat ve önleyici faaliyetler
 - Aktif bilgisayar olaylarına müdahale takımı
- Araştırma ve geliştirme faaliyetlerini desteklenmesi



Gelecek ...

- SCADA'ya yönelik siber ataklar devam edecek:
 - Stuxnet sadece bir başlangıçtı (bildiğimiz kadarıyla)
 - Duqu
- Hükümetler tarafından desteklenen siber ataklar
- Kiralık siber uzmanlar
- Gönüllü siber gruplar (örn: *Anonymous* hacker grubu)





TÜBİTAK-BİLGEM-UEKAE Bilişim Sistemleri Güvenliği Bölümü

bilge@uekae.tubitak.gov.tr

0 312 427 73 66

www.bilgem.tubitak.gov.tr

www.bilgiguvenligi.gov.tr

www.bilgimikoruyorum.org.tr