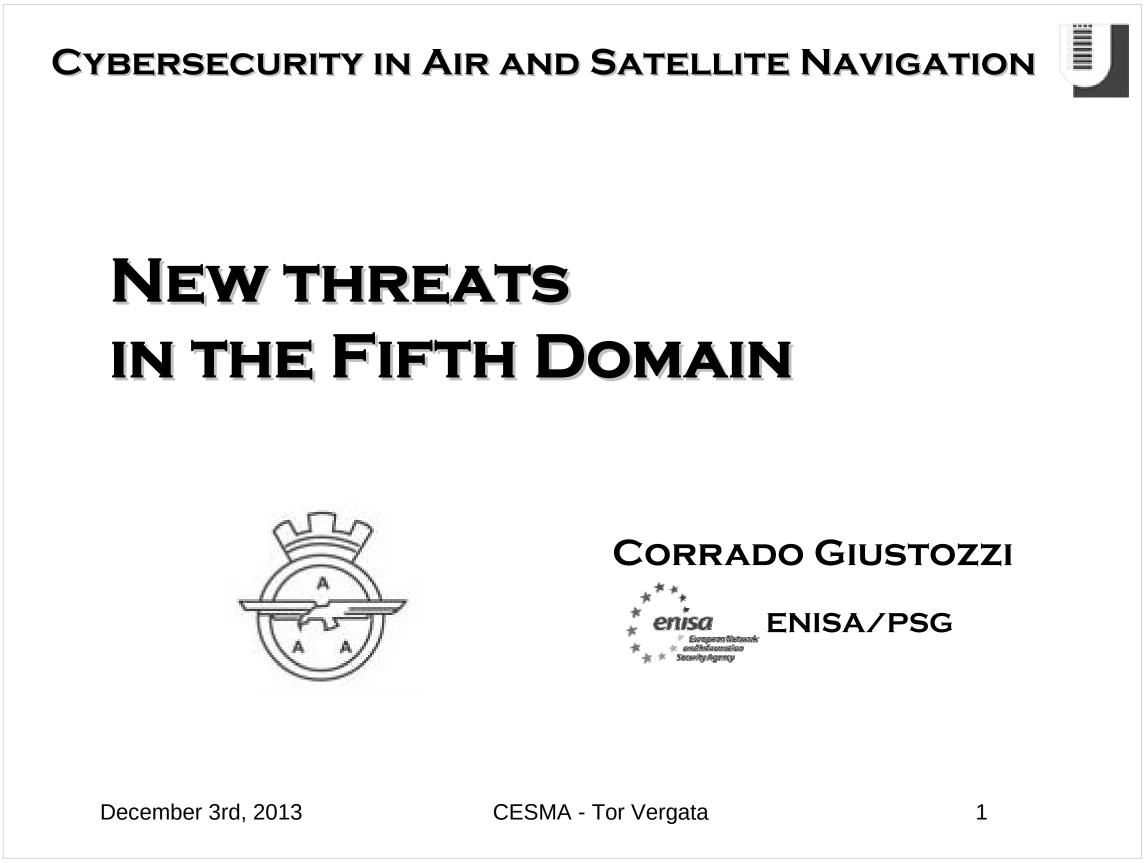


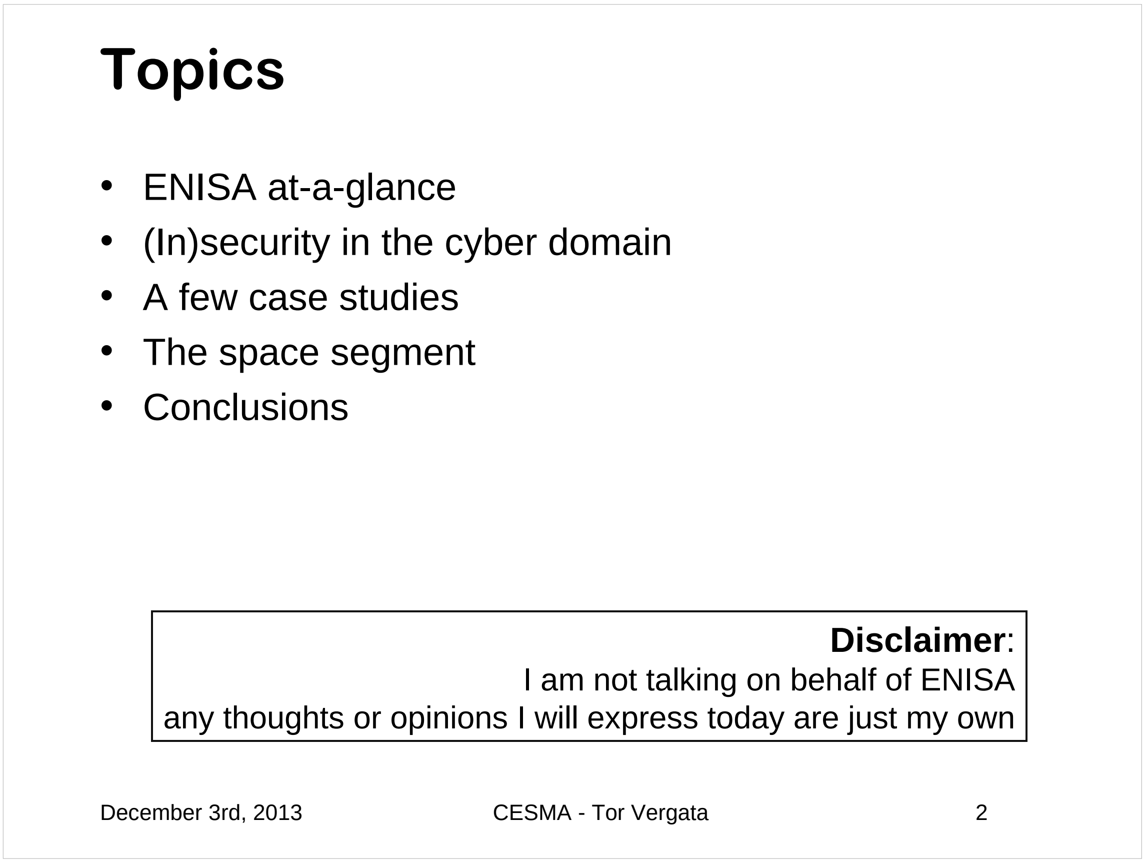
CYBERSECURITY IN AIR AND SATELLITE NAVIGATION

# NEW THREATS IN THE FIFTH DOMAIN

CORRADO GIUSTOZZI

ENISA/PSG

December 3rd, 2013 CESMA - Tor Vergata 1

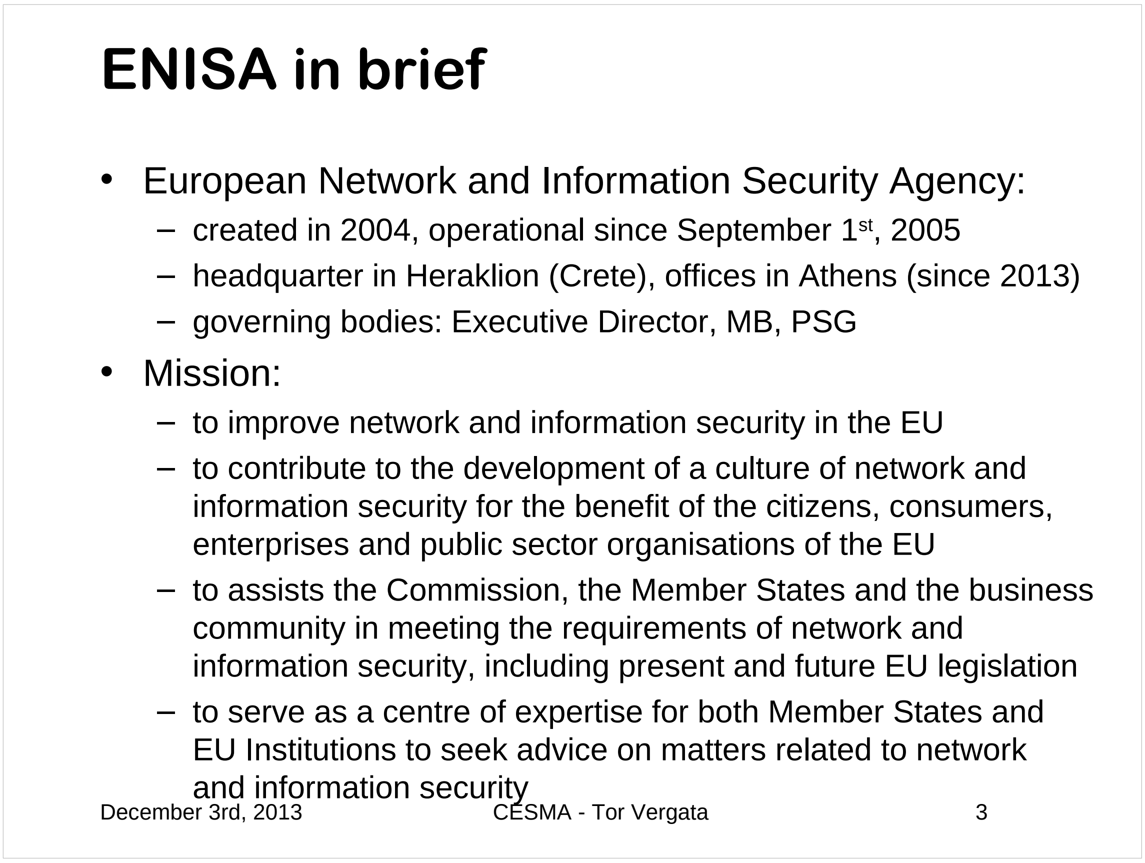


## Topics

- ENISA at-a-glance
- (In)security in the cyber domain
- A few case studies
- The space segment
- Conclusions

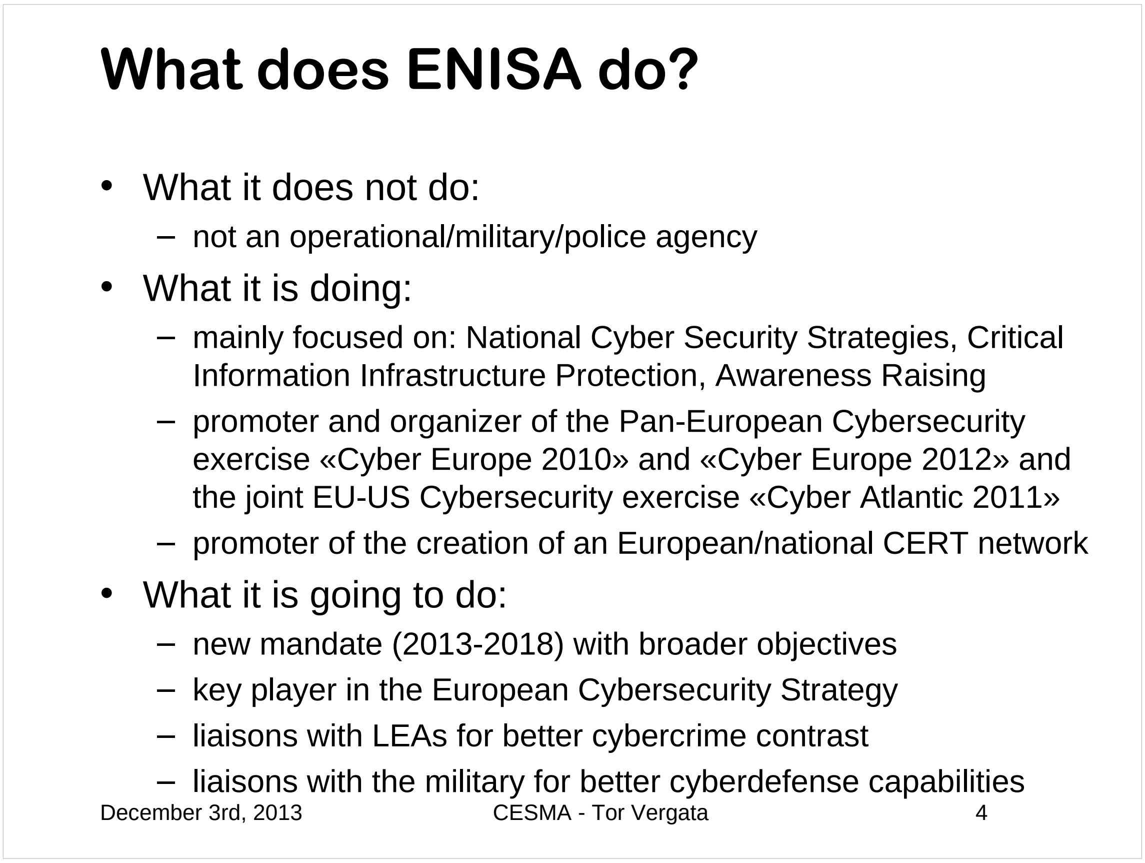
**Disclaimer**:
I am not talking on behalf of ENISA
any thoughts or opinions I will express today are just my own

December 3rd, 2013 CESMA - Tor Vergata 2



# ENISA in brief

- European Network and Information Security Agency:
  - created in 2004, operational since September 1st, 2005
  - headquarter in Heraklion (Crete), offices in Athens (since 2013)
  - governing bodies: Executive Director, MB, PSG
- Mission:
  - to improve network and information security in the EU
  - to contribute to the development of a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations of the EU
  - to assists the Commission, the Member States and the business community in meeting the requirements of network and information security, including present and future EU legislation
  - to serve as a centre of expertise for both Member States and EU Institutions to seek advice on matters related to network and information security



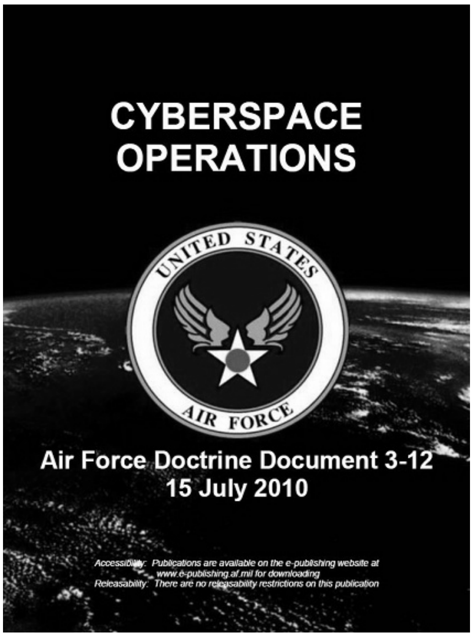
# What does ENISA do?

- What it does not do:
  - not an operational/military/police agency
- What it is doing:
  - mainly focused on: National Cyber Security Strategies, Critical Information Infrastructure Protection, Awareness Raising
  - promoter and organizer of the Pan-European Cybersecurity exercise «Cyber Europe 2010» and «Cyber Europe 2012» and the joint EU-US Cybersecurity exercise «Cyber Atlantic 2011»
  - promoter of the creation of an European/national CERT network
- What it is going to do:
  - new mandate (2013-2018) with broader objectives
  - key player in the European Cybersecurity Strategy
  - liaisons with LEAs for better cybercrime contrast
  - liaisons with the military for better cyberdefense capabilities

# THE FIFTH DOMAIN: A WORLD ON ITS OWN?

*VIRTUAL THREATS*
*IN THE REAL WORLD*

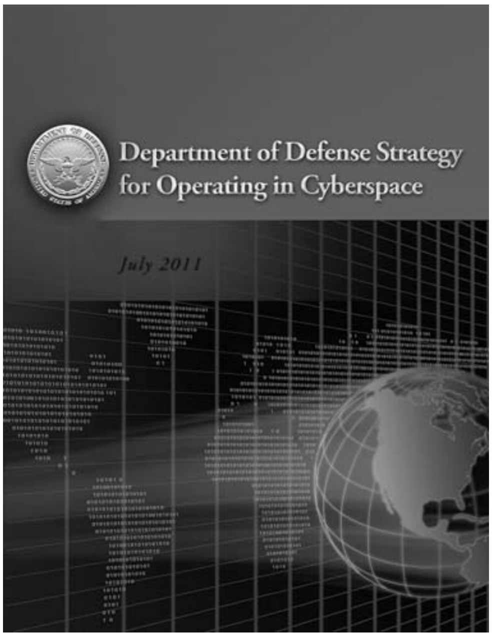
## The Fifth Domain is here…



CYBERSPACE OPERATIONS

Air Force Doctrine Document 3-12
15 July 2010

*Accessibility: Publications are available on the e-publishing website at www.e-publishing.af.mil for downloading*
*Releasability: There are no releasability restrictions on this publication*



Department of Defense Strategy for Operating in Cyberspace

July 2011

# …but is not an island

- Cyberspace is not a world apart, but the connected set of all the systems and networks on the planet
- The other four Domains are linked and tightly interconnected through cyberspace, therefore the Fifth Domain is critical to each of them:
  - Command, Control and Communications all flow through it
  - threats in the Fifth Domain can affect targets in other domains
- Cyber threats are global and pervasive, not limited to the Cyberspace itself in that they may affect real-world infrastructures
- The benefit-cost ratio of a terroristic cyber attack is getting higher and higher because of the inherent weaknessess affecting many critical infrastructures

# Do we really need security?…

- In the good ol’ days we didn’t need security
  - …or, did we?
- The first Internet was designed with no security in mind
  - everyone was supposed to act in good faith
- The same happened with many later technologies, which didn’t take into account threats from fraudsters, criminals, terrorists, …
- Assumption was: “we don’t need security because…”:
  - …we are not doing anything secret/valuable
  - …we don’t have enemies/adversaries
  - …physical security is enough (no or difficult remote access)
  - …the system is so complex/obscure that no one can possibly tamper with it (lack of money/knowledge/technology)

# An easy game

- As in the real world, cyber adversaries do their job by exploiting relevant weaknesses in the infrastructures
- Technical weaknesses:
  - insecurity by design (weak/no authentication, no cryptography…)
  - protocols are often flawed and/or bugged
  - systems are bugged and/or not enough protected
- Complexity weaknesses:
  - systems/networks complexity is overwhelming
  - there are simply too many people/devices on the Net
  - traffic volume is becoming unmanageable
- Human/behavioural weaknesses:
  - no awareness and/or security culture by the end users
  - fundamental assumption is good faith on everyone else’s part

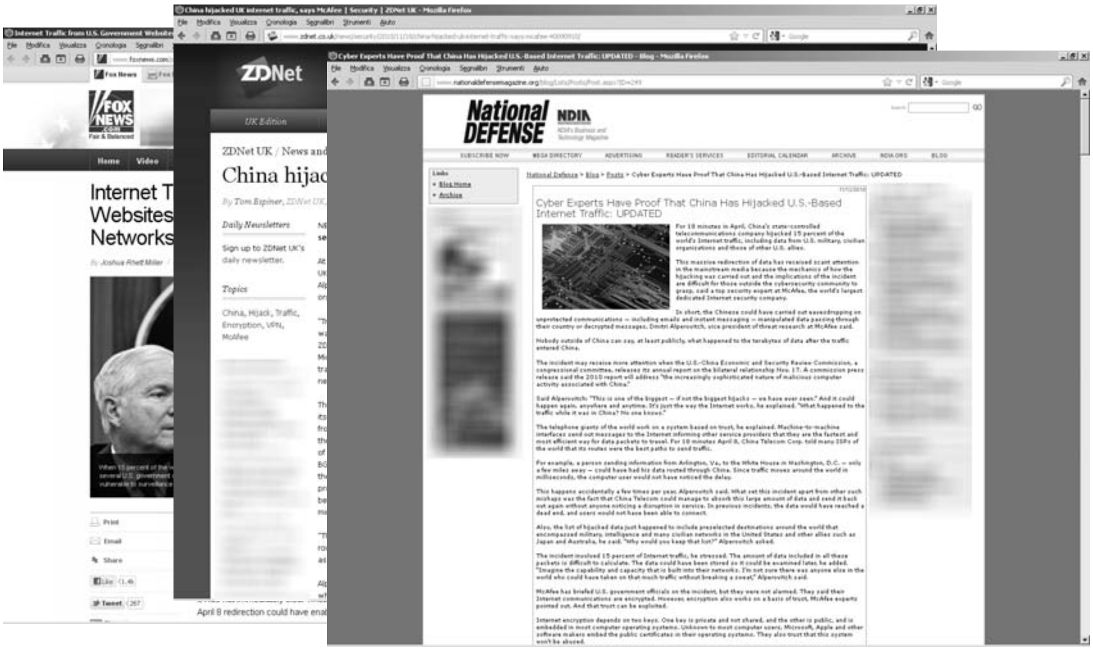
# Four case studies

*Noteworthy facts*
*and incidents*

# Case #1: cellular networks

- 1G (TACS) network was “naively” designed:
  - assuming that all users would be in good faith
  - not taking into account the risk of fraudsters
- Two major design flaws:
  - voice was transmitted in the clear
    - allowing for intentional or unintentional eavesdropping
  - controls (handshake/handover) were transmitted in the clear
    - allowing for easy “terminal cloning”
- This lack of protections led to huge losses:
  - big black market for “cloned” terminals
  - phone bills charged to wrong users, payed by the operator
- 2G (GSM) network introduced security measures:
  - control and voice channel protected by encryption

# Case #2: Internet traffic routing (1/2)


Internet Traffic from U.S. Government Websites
File Modifica Visualizza Cronologia Segnalibri
Fox News
FOX NEWS .com Fair & Balanced
Home Video
Internet T
Websites
Networks
By Joshua Rhett Miller
Print
Email
Share
Like
Tweet
China hijacked UK internet traffic, says McAfee | Security | ZDNet UK - Mozilla Firefox
File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto
zdnet.co.uk
ZDNet
UK Edition
ZDNet UK / News and
China hijac
By Tom Espiner, ZDNet UK
Daily Newsletters
Sign up to ZDNet UK's daily newsletter.
Topics
China, Hijack, Traffic, Encryption, VPN, McAfee
April 8 redirection could have enal
Cyber Experts Have Proof That China Has Hijacked U.S.-Based Internet Traffic: UPDATED - Blog - Mozilla Firefox
File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto
nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=249
Google
National DEFENSE
NDIA
NDIA's Business and Technology Magazine
Search GO
SUBSCRIBE NOW
MEGA DIRECTORY
ADVERTISING
READER'S SERVICES
EDITORIAL CALENDAR
ARCHIVE
NDIA.ORG
BLOG
Links
Blog Home
Archive
National Defense > Blog > Posts > Cyber Experts Have Proof That China Has Hijacked U.S.-Based Internet Traffic: UPDATED

Cyber Experts Have Proof That China Has Hijacked U.S.-Based Internet Traffic: UPDATED

For 18 minutes in April, China's state-controlled telecommunications company hijacked 15 percent of the world's Internet traffic, including data from U.S. military, civilian organizations and those of other U.S. allies.

This massive redirection of data has received scant attention in the mainstream media because the mechanics of how the hijacking was carried out and the implications of the incident are difficult for those outside the cybersecurity community to grasp, said a top security expert at McAfee, the world's largest dedicated Internet security company.

In short, the Chinese could have carried out eavesdropping on unprotected communications — including emails and instant messaging — manipulated data passing through their country or decrypted messages, Dmitri Alperovitch, vice president of threat research at McAfee said.

Nobody outside of China can say, at least publicly, what happened to the terabytes of data after the traffic entered China.

The incident may receive more attention when the U.S.-China Economic and Security Review Commission, a congressional committee, releases its annual report on the bilateral relationship Nov. 17. A commission press release said the 2010 report will address "the increasingly sophisticated nature of malicious computer activity associated with China."

Said Alperovitch: "This is one of the biggest — if not the biggest hijacks — we have ever seen." And it could happen again, anywhere and anytime. It's just the way the Internet works, he explained. "What happened to the traffic while it was in China? No one knows."

The telephone giants of the world work on a system based on trust, he explained. Machine-to-machine interfaces send out messages to the Internet informing other service providers that they are the fastest and most efficient way for data packets to travel. For 18 minutes April 8, China Telecom Corp. told many ISPs of the world that its routes were the best paths to send traffic.

For example, a person sending information from Arlington, Va., to the White House in Washington, D.C. — only a few miles away — could have had his data routed through China. Since traffic moves around the world in milliseconds, the computer user would not have noticed the delay.

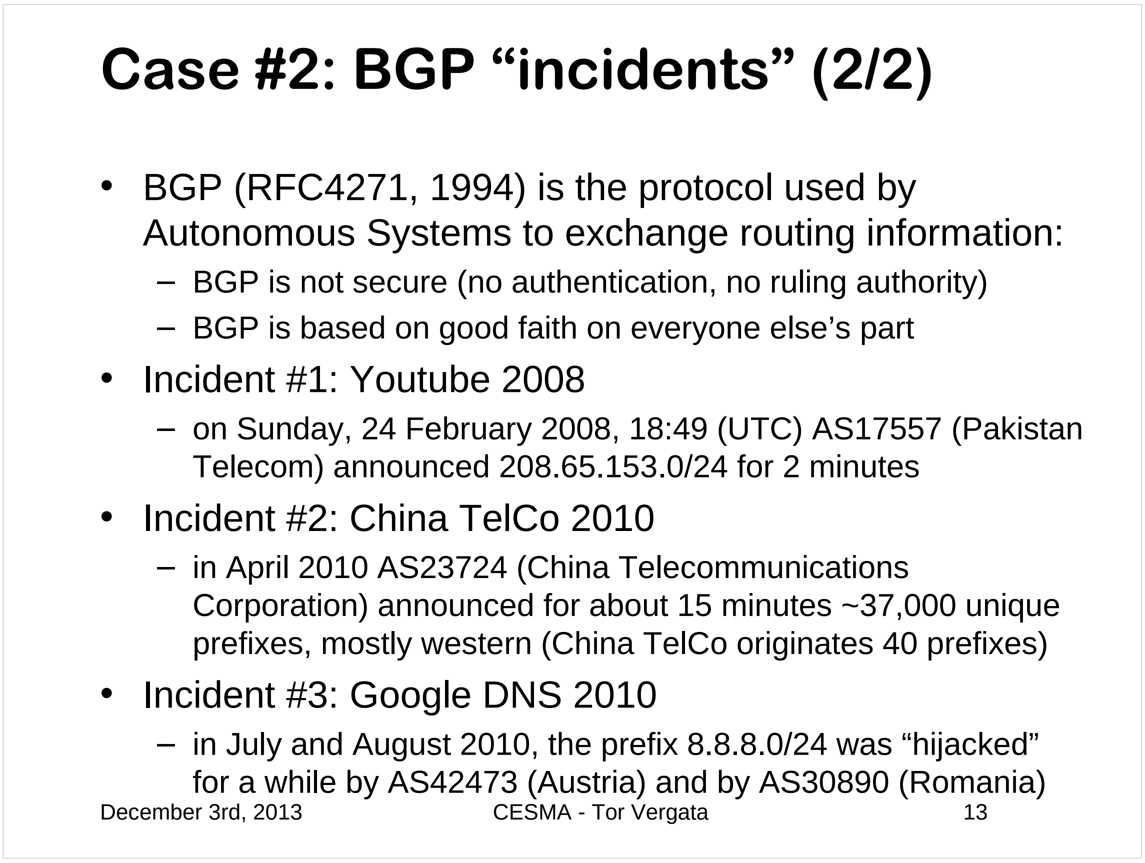
This happens accidentally a few times per year, Alperovitch said. What set this incident apart from other such mishaps was the fact that China Telecom could manage to absorb this large amount of data and send it back out again without anyone noticing a disruption in service. In previous incidents, the data would have reached a dead end, and users would not have been able to connect.

Also, the list of hijacked data just happened to include preselected destinations around the world that encompassed military, intelligence and many civilian networks in the United States and other allies such as Japan and Australia, he said. "Why would you keep that list?" Alperovitch asked.

The incident involved 15 percent of Internet traffic, he stressed. The amount of data included in all these packets is difficult to calculate. The data could have been stored so it could be examined later, he added. "Imagine the capability and capacity that is built into their networks. I'm not sure there was anyone else in the world who could have taken on that much traffic without breaking a sweat," Alperovitch said.

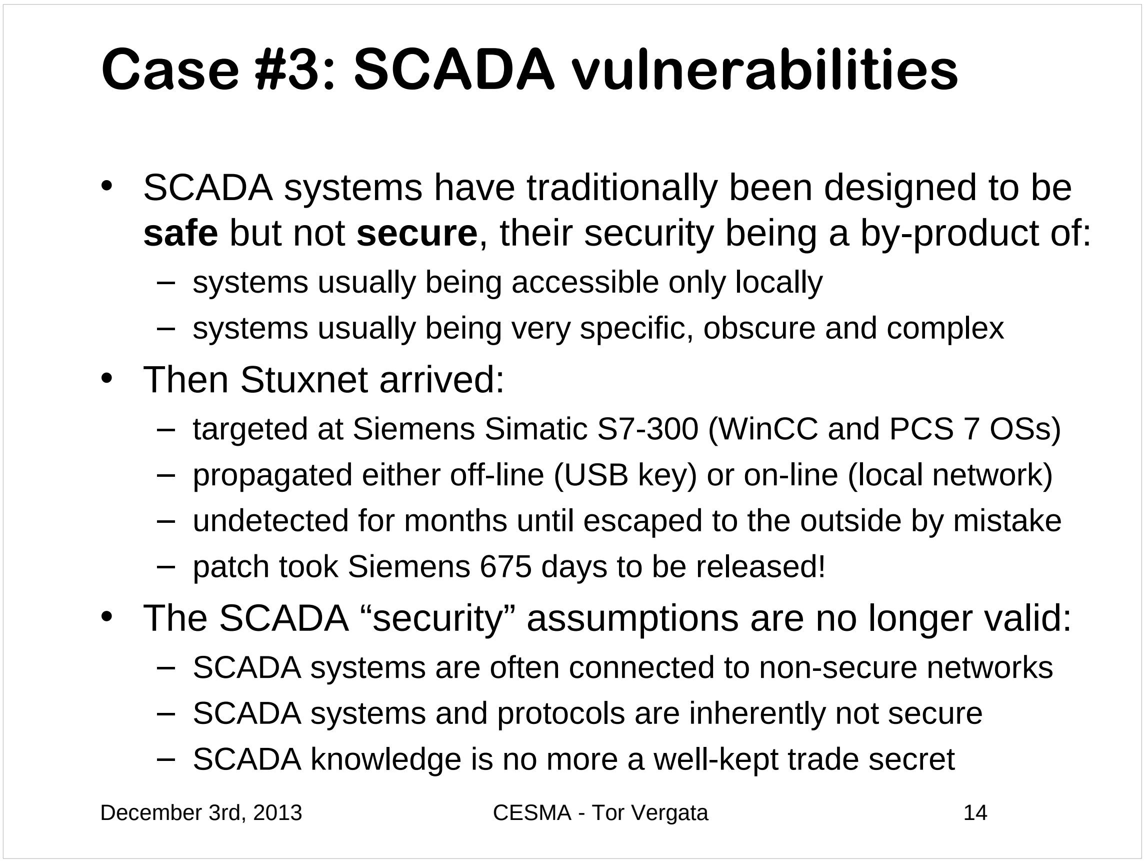
McAfee has briefed U.S. government officials on the incident, but they were not alarmed. They said their Internet communications are encrypted. However, encryption also works on a basis of trust, McAfee experts pointed out. And that trust can be exploited.

Internet encryption depends on two keys. One key is private and not shared, and the other is public, and is embedded in most computer operating systems. Unknown to most computer users, Microsoft, Apple and other software makers embed the public certificates in their operating systems. They also trust that this system won't be abused.



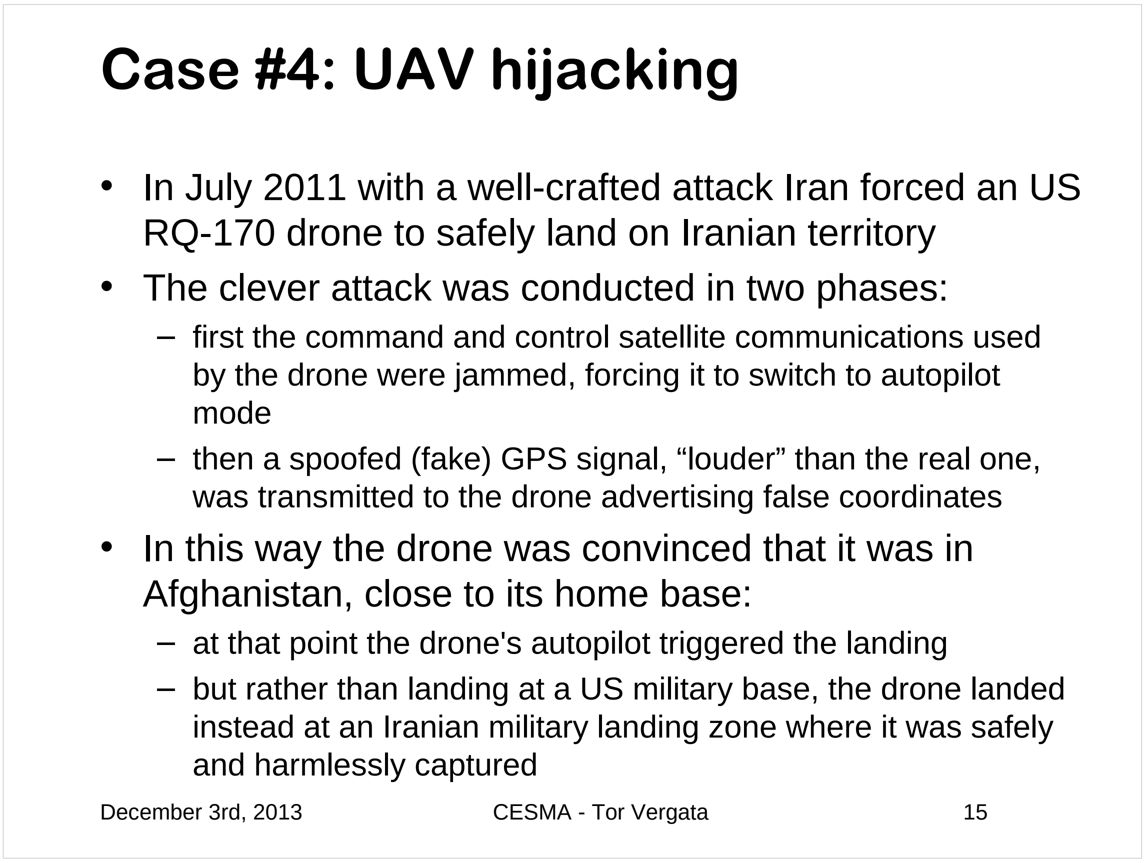
# Case #2: BGP “incidents” (2/2)

- BGP (RFC4271, 1994) is the protocol used by Autonomous Systems to exchange routing information:
  - BGP is not secure (no authentication, no ruling authority)
  - BGP is based on good faith on everyone else’s part
- Incident #1: Youtube 2008
  - on Sunday, 24 February 2008, 18:49 (UTC) AS17557 (Pakistan Telecom) announced 208.65.153.0/24 for 2 minutes
- Incident #2: China TelCo 2010
  - in April 2010 AS23724 (China Telecommunications Corporation) announced for about 15 minutes ~37,000 unique prefixes, mostly western (China TelCo originates 40 prefixes)
- Incident #3: Google DNS 2010
  - in July and August 2010, the prefix 8.8.8.0/24 was “hijacked” for a while by AS42473 (Austria) and by AS30890 (Romania)



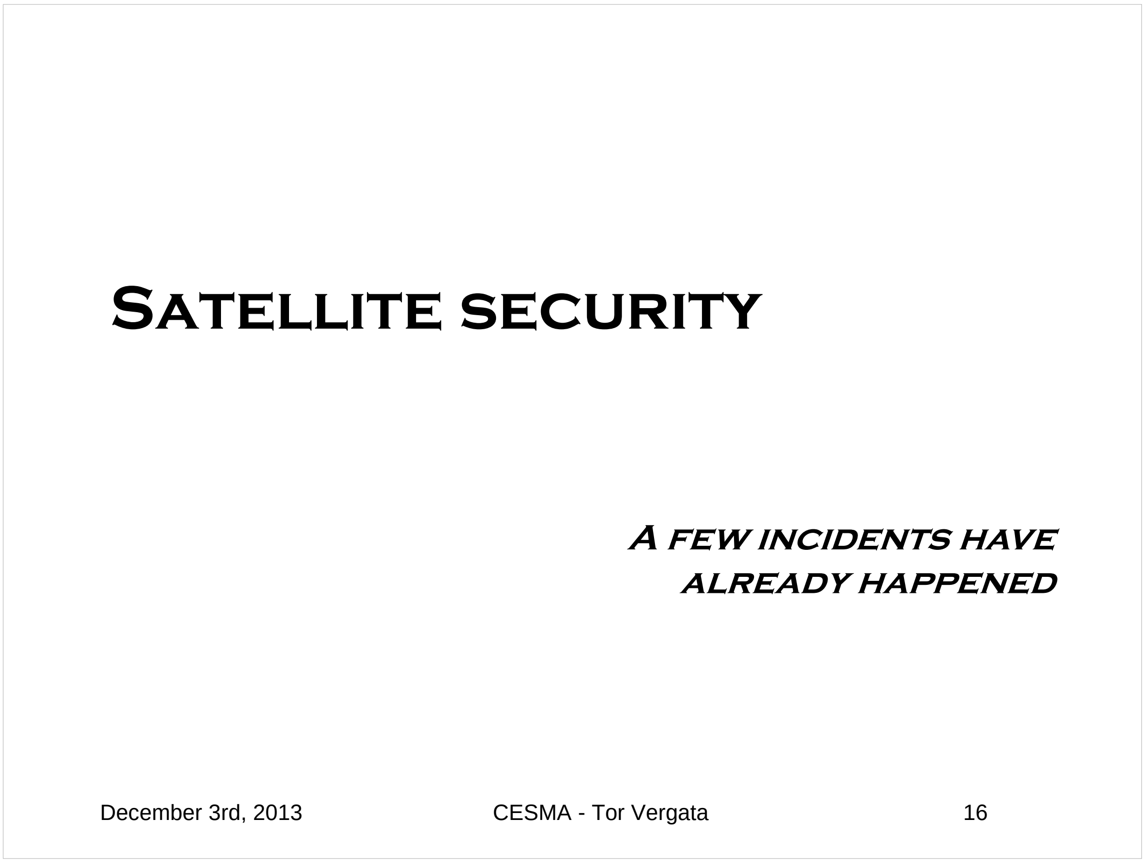
# Case #3: SCADA vulnerabilities

- SCADA systems have traditionally been designed to be **safe** but not **secure**, their security being a by-product of:
  - systems usually being accessible only locally
  - systems usually being very specific, obscure and complex
- Then Stuxnet arrived:
  - targeted at Siemens Simatic S7-300 (WinCC and PCS 7 OSs)
  - propagated either off-line (USB key) or on-line (local network)
  - undetected for months until escaped to the outside by mistake
  - patch took Siemens 675 days to be released!
- The SCADA “security” assumptions are no longer valid:
  - SCADA systems are often connected to non-secure networks
  - SCADA systems and protocols are inherently not secure
  - SCADA knowledge is no more a well-kept trade secret



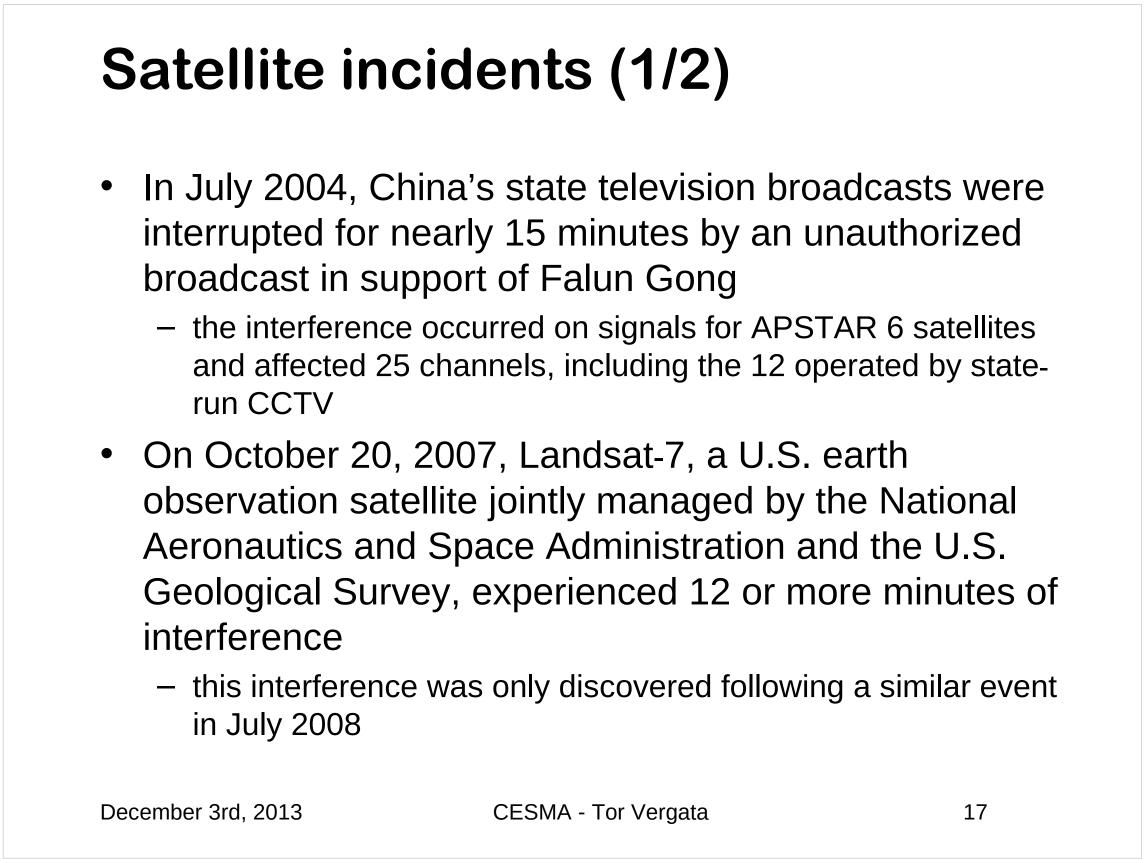
# Case #4: UAV hijacking

- In July 2011 with a well-crafted attack Iran forced an US RQ-170 drone to safely land on Iranian territory
- The clever attack was conducted in two phases:
  - first the command and control satellite communications used by the drone were jammed, forcing it to switch to autopilot mode
  - then a spoofed (fake) GPS signal, “louder” than the real one, was transmitted to the drone advertising false coordinates
- In this way the drone was convinced that it was in Afghanistan, close to its home base:
  - at that point the drone's autopilot triggered the landing
  - but rather than landing at a US military base, the drone landed instead at an Iranian military landing zone where it was safely and harmlessly captured



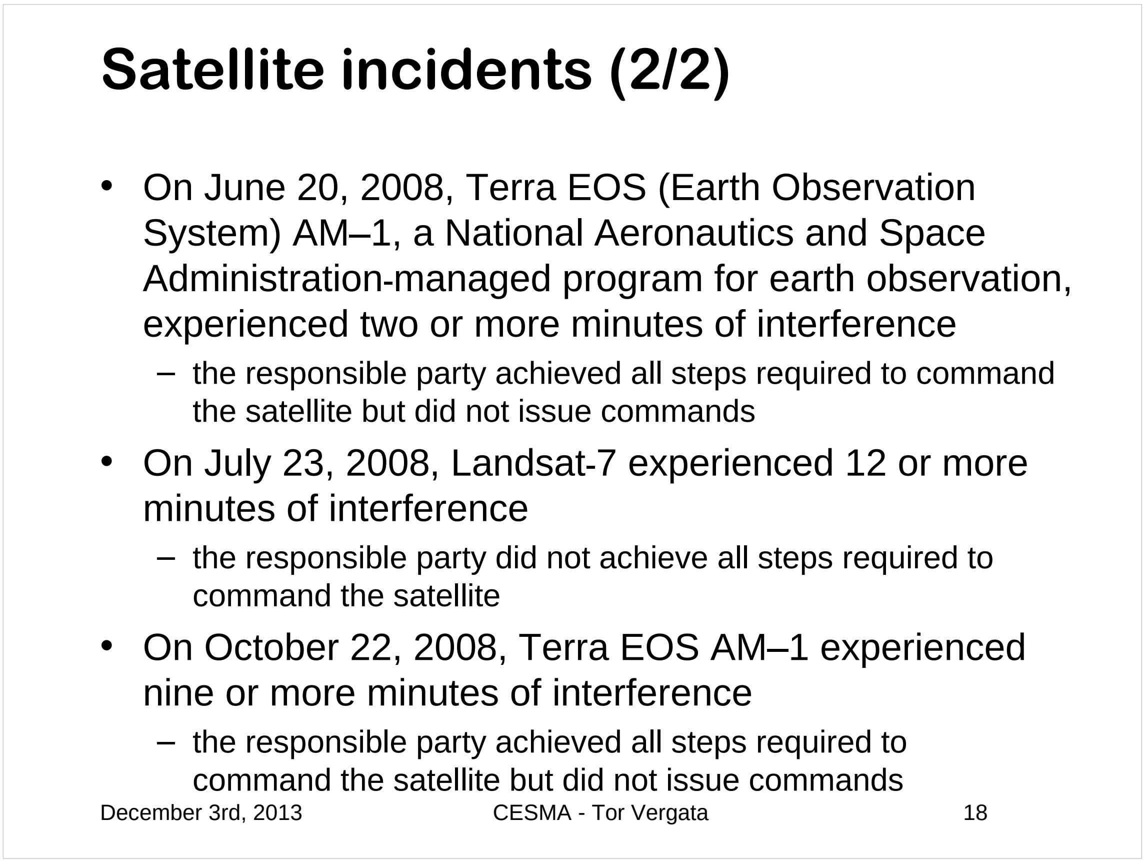
# Satellite security

A few incidents have already happened



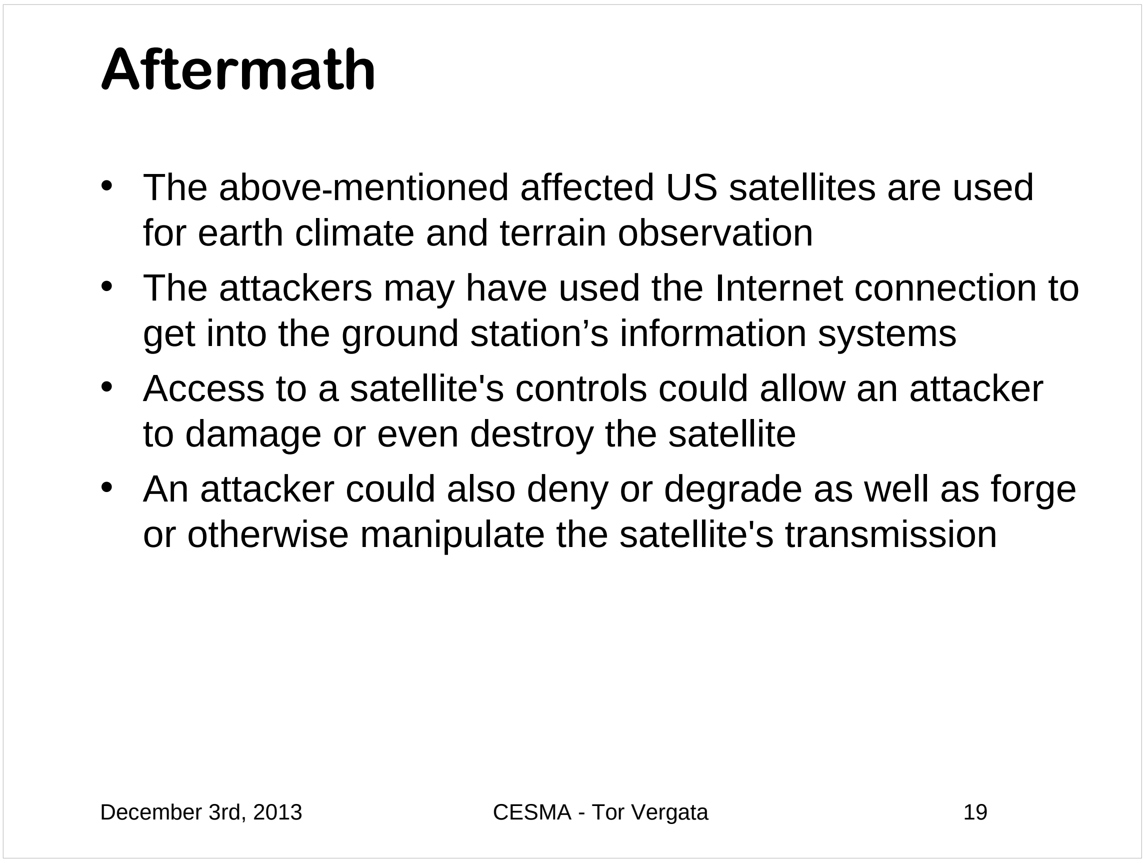
# Satellite incidents (1/2)

- In July 2004, China’s state television broadcasts were interrupted for nearly 15 minutes by an unauthorized broadcast in support of Falun Gong
  - the interference occurred on signals for APSTAR 6 satellites and affected 25 channels, including the 12 operated by state-run CCTV
- On October 20, 2007, Landsat-7, a U.S. earth observation satellite jointly managed by the National Aeronautics and Space Administration and the U.S. Geological Survey, experienced 12 or more minutes of interference
  - this interference was only discovered following a similar event in July 2008



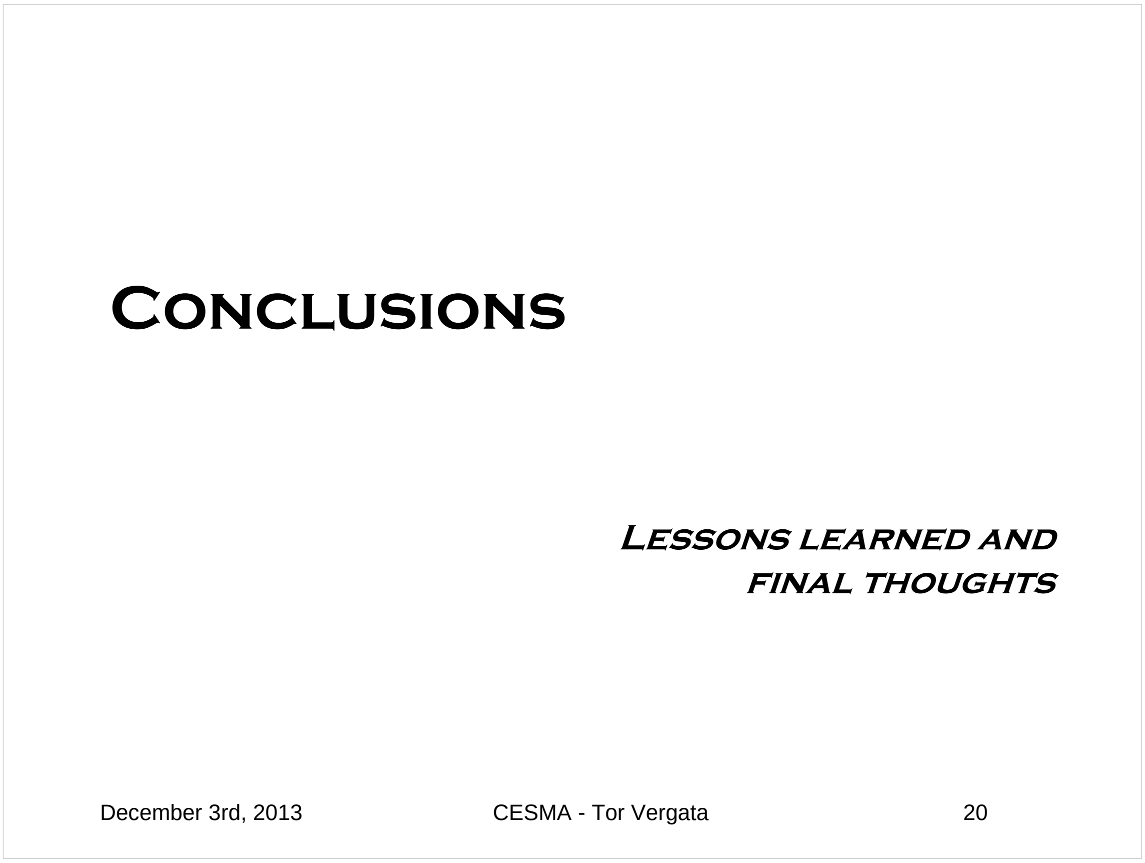
# Satellite incidents (2/2)

- On June 20, 2008, Terra EOS (Earth Observation System) AM–1, a National Aeronautics and Space Administration-managed program for earth observation, experienced two or more minutes of interference
  - the responsible party achieved all steps required to command the satellite but did not issue commands
- On July 23, 2008, Landsat-7 experienced 12 or more minutes of interference
  - the responsible party did not achieve all steps required to command the satellite
- On October 22, 2008, Terra EOS AM–1 experienced nine or more minutes of interference
  - the responsible party achieved all steps required to command the satellite but did not issue commands



## Aftermath

- The above-mentioned affected US satellites are used for earth climate and terrain observation
- The attackers may have used the Internet connection to get into the ground station’s information systems
- Access to a satellite's controls could allow an attacker to damage or even destroy the satellite
- An attacker could also deny or degrade as well as forge or otherwise manipulate the satellite's transmission



## Conclusions

*Lessons learned and final thoughts*

## Final thoughts

- The world has changed:
  - everything is valuable for someone / we all have adversaries
  - attack potential has grown, cyber attacks are easier to do
- We cannot repeat with modern critical infrastructures the naive mistakes we made with earlier technologies:
  - lessons learned by ETACS and SCADA
  - systems need to be not only **safe** and **robust** but also **secure** (ie at least tamperproof)
- Always require “security by design”:
  - secure protocols based on mutual strong authentication
  - data/control channel protection (encryption)
  - redundancy, validation, integrity checks
  - secure coding, code review, security audits

CYBERSECURITY IN AIR AND SATELLITE NAVIGATION

## THANK YOU FOR YOUR ATTENTION

C.GIUSTOZZI@ACM.ORG