How do they do?

- Exploitation of Internet as for medium of communication:

  - "While YouTube channels and Facebook pages of terrorist supporters may radicalize Western-based sympathizers, they also provide a means for communication between these "lone wolf" actors and larger organized networks of terrorists."
  - " The decentralized nature of the Internet as a medium and the associated difficulty in responding to emerging threats can match the franchised nature of terrorist organizations and operations."

Tools they exploit

- "Extremists use:
  - chat rooms,
  - dedicated servers and,
  - websites, and,
  - social networking tools."
- "YouTube channels and Facebook pages"

Tools they exploit

- For a true cyber terrorist, the network is the method of attack. It is the weapon.
- It is through the network, internet, that messages and computer commands are transmitted, programs and malicious software be emplaced, fraudulent transactions take place, and information be available for exploitation.
- Defacing websites, crashing portions of a target network, accessing enemy information, denying network access to other groups, manipulating financial confidence and thus causing panic.

Tools they exploit

- Other methods are the manipulation, modification, and destruction of nonphysical items such as data, websites, or the perceptions and attitudes this information can influence.
- Attacks that would destroy electronic records of financial transactions, or permit large-scale electronic theft would cause significant economic damage to a country.
- Changing the information or appearance of an enemy's official web page allows the terrorist to spread negative perceptions or false information without physical intrusion.

Section #3 Some Cases & Cyber Exercises

Case #1 A Cyber

Attack to a US City.

Case #2 Stuxnet Worm.

Cyber Exercises

Dr. Ahmet Koltuksuz

Case #1

A Cyber-Attack On An American City

Bruce Perens | Apr. 25, 2009, 7:00 AM | 3,471 | 12 Print

Tags: Security, Big Tech

(This post was originally published on Perens.com)

Just after midnight on Thursday, April 9, unidentified attackers climbed down four manholes serving the Northern California city of Morgan Hill and cut eight fiber cables in what appears to have been an organized attack on the electronic infrastructure of an American city. Its implications, though startling, have gone almost un-reported.

That attack demonstrated a severe fault in American infrastructure: its centralization. The city of Morgan Hill and parts of three counties lost 911 service, cellular mobile telephone communications, land-line telephone, DSL internet and private networks, central station fire and burglar alarms, ATMs, credit card terminals, and monitoring of critical utilities. In addition, resources that should *not* have failed, like the local hospital's *internal* computer network, proved to be dependent on external

Case #2 STUXNET WORM

- **ICS:** Computer Assisted Industrial Control System. They have been in use for the last 40 years and typically they are in charge of the management & control of the devices in Critical Infrastructures.

- **Some Types of ICSs:**
  - supervisory control and data acquisition (SCADA) systems,
  - distributed control systems (DCS), and
  - Programmable Logic Controllers (PLC).

Case #2 STUXNET WORM

- **Date:** Stuxnet worm was first reported in June 2010 by a security company in Belarus.

- **The target:** SCADA systems and PLCs of nuclear reactors of Iran.

Case #2 STUXNET WORM

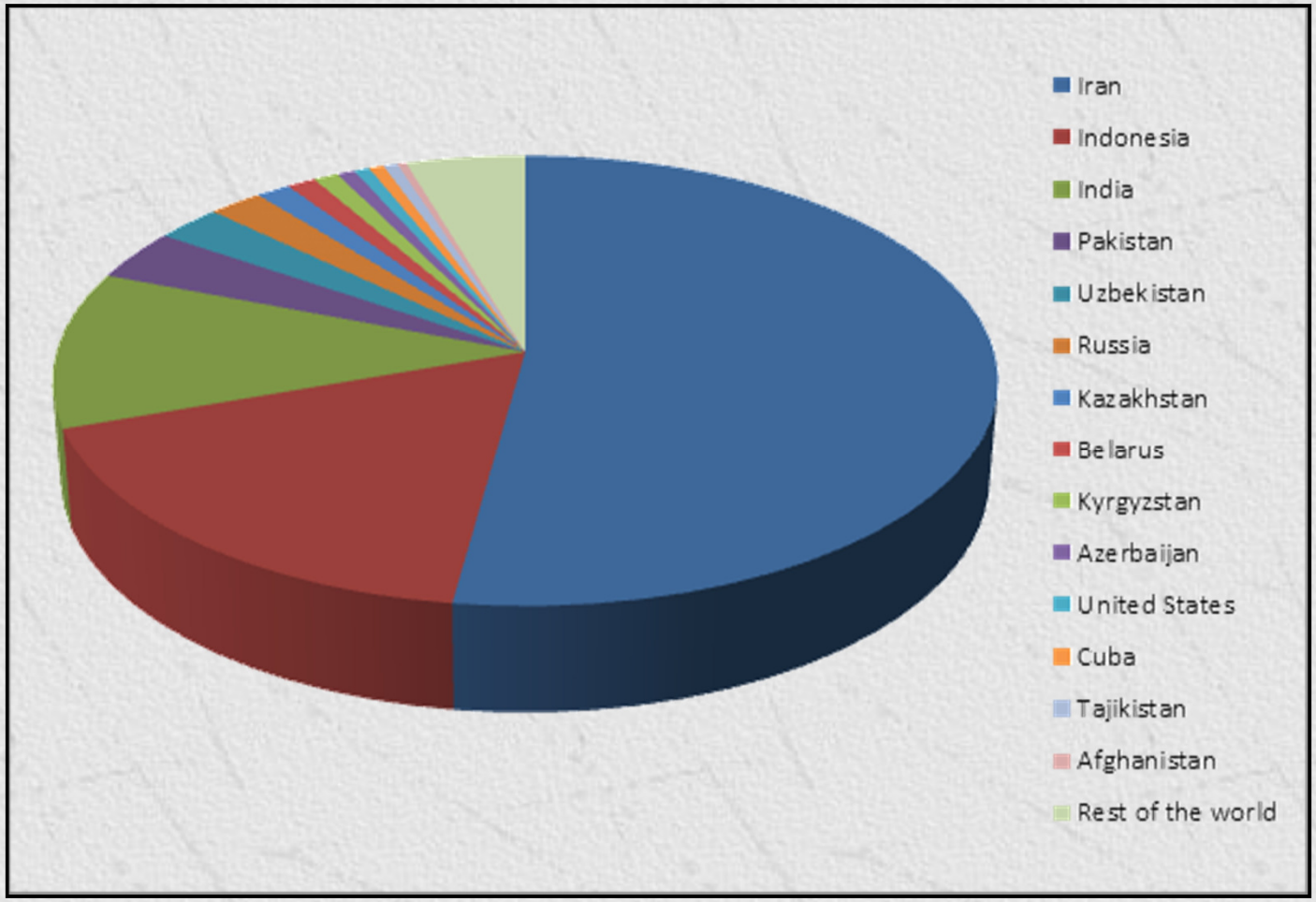
Analysis of the Code:

- The first malicious software (malware) designed specifically to attack a particular type of ICS: one that controls nuclear plants, whether for power or uranium enrichment.
- The malware attacks and disrupts a Microsoft Windows-based application that is employed by a particular ICS produced by the German company Siemens.
- The worm can be spread through an air-gapped network by a removable device, such as a thumb drive, and possibly through computers connected to the Internet.

Case #2 STUXNET WORM

- **Who did it?**
  - Some security analysts speculate that Stuxnet could have been developed by a Siemens insider who had direct access and knowledge of the system;
  - Others contend that the code's sophistication suggests that a nation state was behind the worm's development, either through proxy computer specialists or a government's own internal government and military capabilities.
  - Countries thought to have the expertise and motivation of developing the Stuxnet worm include the United States, Israel, United Kingdom, Russia, China, and France.

Case #2 STUXNET WORM



Global infection by Win32/Stuxnet
(Top 14 Countries) June – September 2010

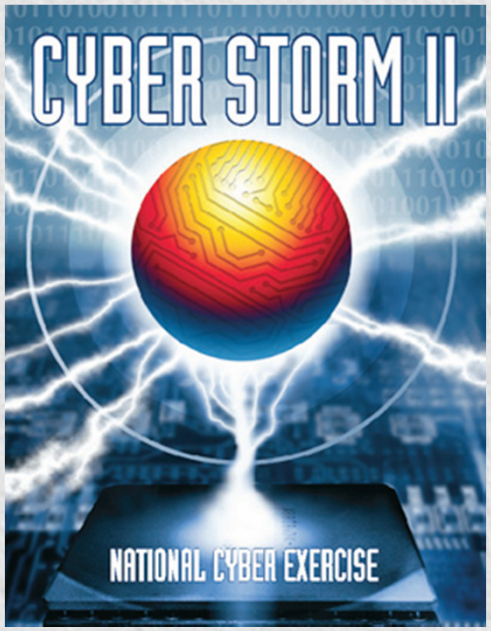
Case #2 STUXNET WORM

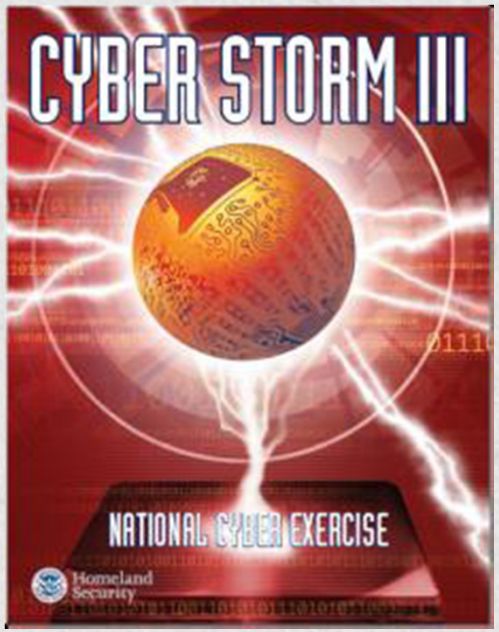
The Percentage Distribution of Infections by Region.

Iran	Indonesia	India	Pakistan	Uzbekistan	Russia	Kazakhstan	Belarus
52,2%	17,4%	11,3%	3,6%	2,6%	2,1%	1,3%	1,1%
Kyrgyzstan	Azerbaijan	United States	Cuba	Tajikistan	Afghanistan	Rest of the world	
1,0%	0,7%	0,6%	0,6%	0,5%	0,3%	4,6%	

US Dept. Of Homeland Security: CYBER STORM

- Cyber Storm I: February 2006,
- Cyber Storm II: March 2008,
- Cyber Storm III: September 2010.





NATO: CYBER COALITION

- November 2008, Full organs of NATO included,
- November 2009, All NATO countries,
- November 2010, Full organs of NATO , all NATO countries plus some observer countries like Japan.

European Union: CYBER EUROPA

- **CYBER EUROPA: November 2010**
  - 22 states as player, 8 states as observer.
  - Iceland, Norway and Switzerland separately joined.

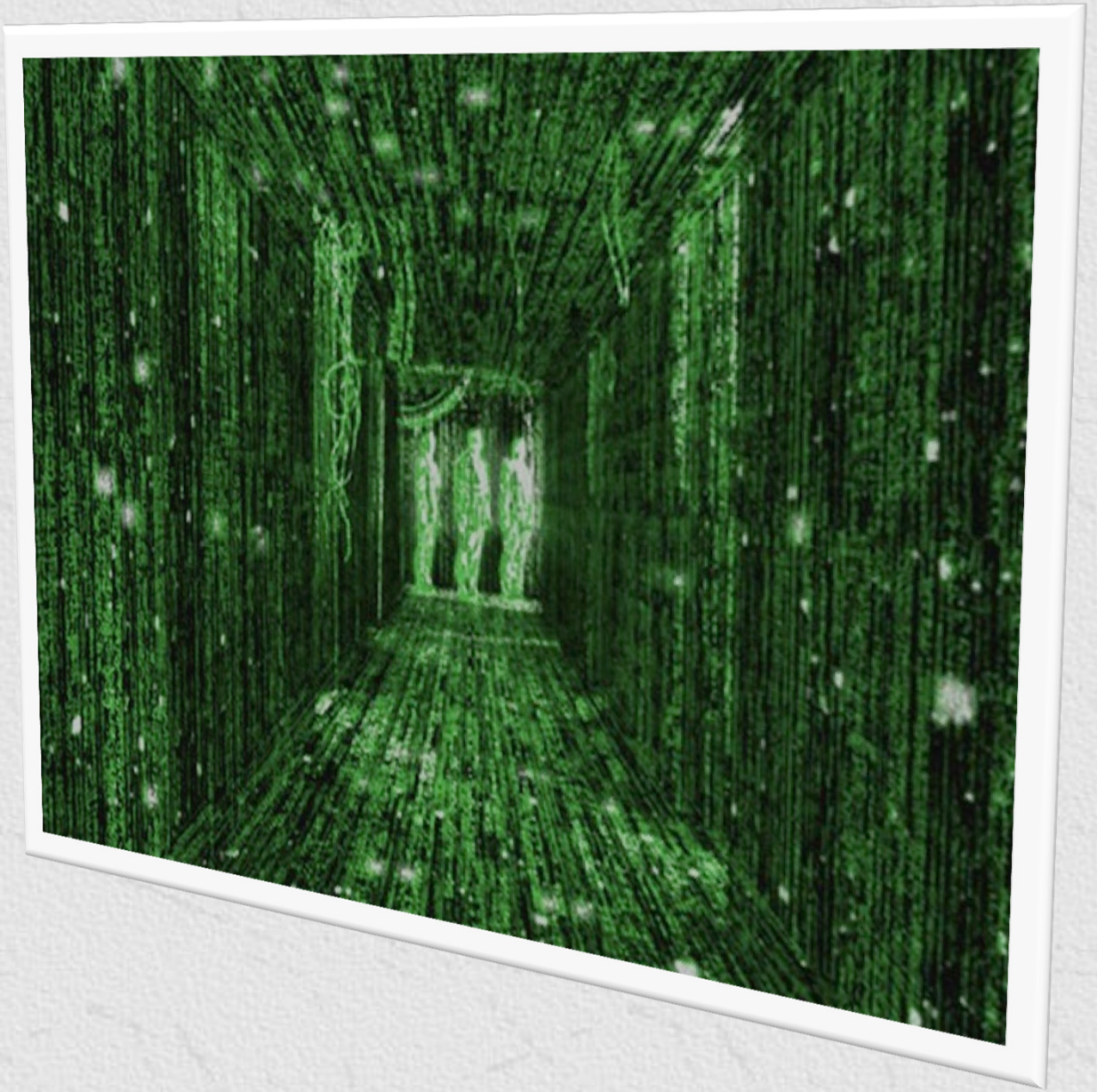
Turkish Cyber War Excercises

- November 20-21 2008, Tübitak, TR-BOME, BOME
- January 25-28 2011, Tübitak-BİLGEM, BTK

Conclusions

Some remarks

US DoD Strategy for Operating in Cyber Space, July 2011.



Dr. Ahmet Koltuksuz

Conclusions

- Stuxnet worm incident should be evaluated as a precursor to what is being cooking in the kitchen for sometime although it is not served yet!
- Remarks:
  - Anything and everything is going to be hooked to the internet.
  - Internet is independent of four dimensions and of political borders.
  - The network is the arena for cyber war.
  - Therefore, cyber war will be every where and every when.
  - It is not something that will go away in a foreseeable future.

Conclusions

- International cooperation is a must for a combat against cyber war, cyber terrorism and there are no greater pains than to achieve a full understanding & cooperation among nations.
- US DoD Cyber Space Operational Strategy is but a good example.

Conclusions: DoD as an Example

US DEPARTMENT OF DEFENSE
STRATEGY FOR OPERATING IN CYBERSPACE
July 2011

FIVE STRATEGIC INITIATIVES

- Strategic Initiative 1: Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential.
- Strategic Initiative 2: Employ new defense operating concepts to protect DoD networks and systems.
- Strategic Initiative 3: Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cyber security strategy.
- Strategic Initiative 4: Build robust relationships with U.S. Allies and international partners to strengthen collective cyber security.
- Strategic Initiative 5: Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

Conclusions

A new concept in NATO since 1960s: The perception of Cyber War along with asymmetric, conventional and nuclear threats.

References

- Raymond C. Parks and David P. Duggan, **"Principles of Cyber-Warfare"**, Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 5-6 June, 2001
- **"Cyber Operations and Cyber Terrorism, Handbook Number 1.02"**, US Army Training and Doctrine Command, Deputy Chief of Staff for Intelligence, Assistant Deputy Chief of Staff for Intelligence – Threats, Fort Leavenworth, Kansas, 15 August 2005.
- John Rollins, Clay Wilson, **"Terrorist Capabilities for Cyberattack: Overview and Policy Issues",** CRS Report for Congress: **RL33123**, January 22 2007.
- Paul K. Kerr, John Rollins, Catherine A. Theohary, **"The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability"**, CRS Report for Congress: **R41524**, December 9 2010.
- Catherine A. Theohary, John Rollins, **"Terrorist Use of the Internet: Information Operations in Cyberspace",** CRS Report for Congress, **R41674**, March 8 2011.
- Aleksandr Matrosov, Eugene Rodionov, David Harley, Juraj Malcho,**" Stuxnet_Under_the_Microscope, v.1.31"**, www.eset.com, white-papers, February 17 2011.
- US DoD, **"Strategy For Operating In Cyberspace",** July 2011.

Thank YOU for your time and patience.

Ahmet KOLTUKSUZ