INFOSECURITY MOSCOW 2016

Аутор Зоран Живковић
Председник Друштва за информациону безбедност Србије

Cyber peace or Cyber war

The status of Cyber security in Western Balkan area in correlation with real cyber terrorism treats

ZORAN ŽIVKOVIĆ
PRESIDENT OF SERBIAN ASSOCIATION FOR CYBER SECURITY

Cyber space and Cyber power

It is indisputable that INFORMATION TECHNOLOGY has done a very strong positive impact on all aspects of human life and work causing extensive and profound changes which is often difficult to understand.

EVIDENCE

The most powerfull countries are the biggest consumers of information technologies

They are developed because they use IT
and not vice versa

Cyber space

A tremendous amount of diverse data and information is placed this virtual space by those who have money, goods and intellectual property and by individuals, business, organizations, companies, groups and state bodies,
which are classified to different
types of secrecy and confidentiality levels.

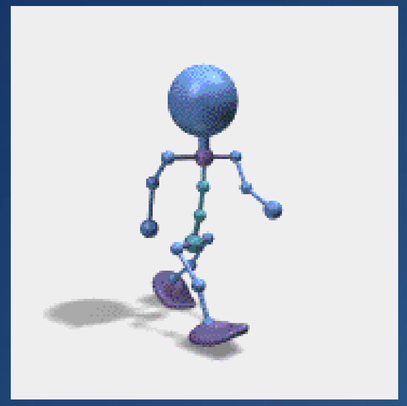
CYBER SPACE IS A LEGITIME SOURCE OF POWER

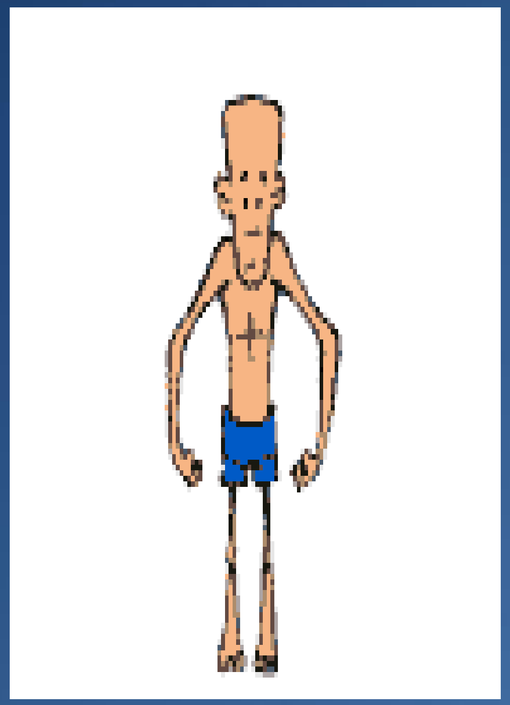
Internet - a safe harbor for terrorists?

CONSECQUNCIES

Difference in power between “WEEK and STRONG “ and

between “BIG and SMALL” slowly disappearing.





Cyber Power – what it is?

The ability to use cyberspace
to create advantages and to get INFORMATION
across.

POWER to influence events in cyber space and
other operational environments.

Attacks in energy industry
or
just shortlist of well known cyber attacks in the post Stuxnet era

Saudi Aramco, August 2012.

- Shamoon malware was infiltrated in the system by a malicious link placed in an e-mail (social engineering + phishing attack).
- Around 35.000 computers have been harmed. In some computers the data was deleted while some of them had their hard disks damaged.
- The first thing employees did was to disconnect the internet cables in order to prevent malware from spreading through the network.
- Damage: 5 months of work without internet connection, replacement of hard disks on all machines in the company, financial loss.

Energy industry in Norway

- Malware infiltration by malicious e-mail attachment (social engineering + phishing attack).
- KeyLogger Trojan malware type was infiltrated in the system for the purpose of intellectual property theft.
- More than 50 companies have been attacked and additional 250 companies were potential victims. Norway authorities informed possible victims of the attack so each of the companies had to check the integrity of their network.

Attack on energy system of Turkey, March 2015.

- Control system of electricity network in a part of Turkey was disabled, which caused a complete power outage in the territory of Ancara, Istanbul and three other major cities in Turkey.
- Around 40 000 000 citizens were left without electricity and the failure lasted for about 12 hours.
- Damage: Transportation system in the cities collapsed (metro), traffic collapsed due to failure of traffic lights, large number of people were stuck in elevators…
- There were indications of a cyber attack, but that was not confirmed.

Attack on energy system of Ukraine, December 2015.

- The first confirmed cyber attack which resulted in power outage.
- Black Energy malware was used to cut connection of three regional substations, causing power failure.
- About half of the Ivano-Frankivsk region population (around 80 000) was left without electricity.
- The blackout lasted for several hours.
- Black Energy malware exists since 2007 but with constant upgrades it still can be very destructive. There are indications that a malware used vulnerabilities in macro functions of MS office program.

Attack on Ministry of energy Israel, Januar 2016.

- It was a massive, frequently repeated attack.
- As a prevention some parts of power network have been forced to shout down
- Malware Black Energy is a suspected for the attack, there is still no damage report.

Attack on energy system of Serbia, March 2016.

- New generation of STUXNET is discovered inside of information network of Serbian energy system.
- Till today no reports or signs of correlated damage
- It could be just a training for potential attackers?

Cyber terrorism in Balkan region

- Recruitment of young people for participation in ISIL terrorist activities (approximately more than 500 people from Western Balkan region participated as a member of ISIL, mostly from Bosnian and Herzegovina, Kosovo and FYRM).
- Spreading mass panic with threatening public statements.
- Attacks on public internet services – mostly media websites.

Cyber attack on Serbian cyber space

14.10.-17.10.2014.

70 -100 Gbps

The most massive cyber attack so far

Basic facts about the attack

Tuesday, 14.10.2014.,

- Synchronized with the events at the football stadium (drone with Albanian flag appeared at central national stadium during footbool match Serbia – Albania) extremely massive and long-term DDoS attack was performed.
- Attack started at 21:30h and it lasted for a few hours with a huge power.
- The attack was stronger than 70 Gbps and that is the most massive cyber attack ever performed at Serbian cyber space.
- At the time of NATO bombing our cyber space was systematically attacked, but that, even at its worst, was few times smaller then this one.

Result

- The fact that all big media in Serbia were blocked for hours indicates that required security measurement weren`t applied.
- The systems and business based on internet cannot operate by relying on luck and famous fraise – it won’t come to us, we aren’t that interesting.
- Everybody is a potential target.
- There are no big or small targets, more or less interesting ones.

HOW TO PROTECT CYBER SPACE FROM TERORIST CYBER ATTACKS

- Cyber attacks have become a physical threat and they aren’t performed only in cyber space.
- Should we considered ourselves lucky for not having a nuclear power plant and so nobody can send us all into heaven via a cyber attack?
- Cyber war is a war and if one state or terrorist group performs cyber attacks against another then they are in war.

HOW TO PROTECT CYBER SPACE FROM TERORIST CYBER ATTACKS

- WE MUST HAVE ALL PROTECTION SOLUTIONS
- WE MUST HAVE CONSOLIDATED INTERNATIONAL LEGAL FRAME
- WE MUST COOPERATE

HOW TO PROTECT CYBER SPACE FROM TERORIST CYBER ATTACKS

IT IS A TIME FOR CYBER SPACE

UNATED NATIONS

INFOSECURITY MOSCOW 2016

Zoran ŽIVKOVIĆ
PRESIDENT OF SERBIAN ASSOCIATION FOR CYBER SECURITY
z.zivkovic@towersnet.rs
www.dibs.rs www.towersnet.rs

INFOSECURITY MOSCOW 2016

THANK YOU