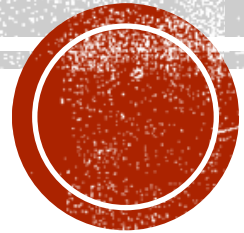
CYBER CONFLICT



DEFiNiTiON

- **Today, conflict is essentially borderless.**
- Cyber Conflict may be defined as “Any act intended to compel an opponent to fulfill our national will, executed against the software controlling processes within an opponent's system.”
- Military attack in the form of a cyber network attack is irregular in nature. It is extremely **cheap**, is **very fast**, can be carried out **anonymously**, and can disrupt or deny critical services precisely at the moment of maximum peril.
- Unlike traditional warfare, cyber warfare makes it difficult, if not impossible, to know who the attacker is. Even if an attack can be traced back to its origin, it doesn't mean that country was behind the attack.

[the history of]

/cyber warfare;

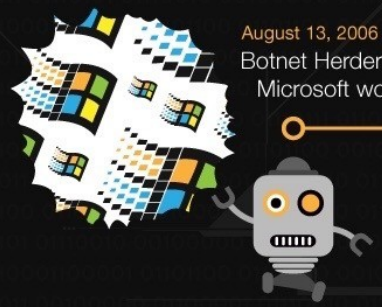
1970's
Worm attacks go back to the 1970s' "ancestor worms" which are highly evolved and sophisticated today.

2003-2006
Worm viruses created in 2003-2006 compromise computers which become members of the Botnet farms.

2005-2007
Internet Mafias like the Russian Business Network (RBN) proliferate their reign on the web.

2005-Present
Hackers in China attack computers in the U.S. Attacks of this nature are still continuing even today.

August 13, 2006
Botnet Herders attack Microsoft wormhole.

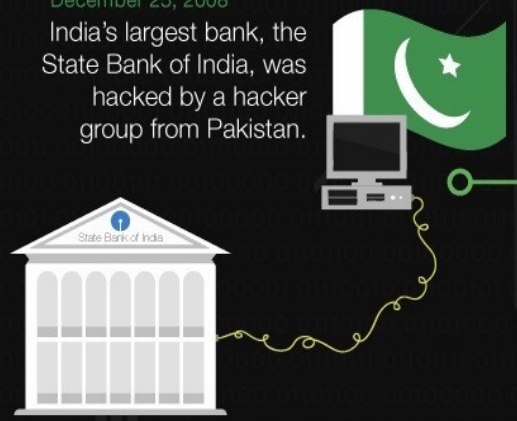


January 2007
1 million computers remotely controlled network of "zombie" computers that has been linked by the Storm Worm, a Trojan horse spread through e-mail spam.

June 13, 2007
FBI operation called "Bot Roast". The FBI goes after Botnet farms.

August 27, 2008
NASA confirmed that a worm was discovered on laptops on the International Space Station.

December 25, 2008
India's largest bank, the State Bank of India, was hacked by a hacker group from Pakistan.



December 2009
Along with a Zero day attack on IE 6, 34 American companies were compromised including Google. During these attacks, intellectual property was stolen. China denies being involved in the attacks.

September 7, 2007
Multi-stage Botnet attack on E-bay.

November 30, 2008
Pentagon computers were hacked by computer hackers suspected of working from Russia.

January 8, 2009
Israeli students developed a program that allows Israeli citizens' computers to be controlled by an Israeli Hacker group that targets Pro-Hamas websites.

Summer 2009
Insurgents compromise U.S. Drones. $26 off-the-shelf Russian software was used by the insurgents to intercept live video feeds.

THE HiSTORY OF CYBER WARFARE

- 1991 Gulf War: An Early Cyber Conflict. The first major U.S. conflict involving computer warfare was the 1991 war against Iraq. The Pentagon does not offer specific details as to what was done, but reports have asserted that Baghdad's air defense radar and other systems were targeted by U.S. cyber warriors.
- In 1998, the United States hacked into Serbia's air defense system to compromise air traffic control and facilitate the bombing of Serbian targets.
- In 2006, Russian Mafia group Russian Business Network （RBN） began using malware for identity theft.
- In 2007, RBN completely monopolized online identity theft. By September 2007, their Storm Worm was estimated to be running on roughly one million computers, sending millions of infected emails each day.
- In 2007, in Estonia, a botnet of over a million computers brought down government, business and media websites across the country. The attack was suspected to have originated in Russia, motivated by political tension between the two countries.
- Also in 2007, an unknown foreign party hacked into high tech and military agencies in the United States and downloaded terabytes of information.
- In 2008, cyber-attacks moved from personal computers to government institutions. On August 27, 2008 NASA confirmed a worm had been found on laptops in the International Space Station; three months later Pentagon computers were hacked, allegedly by Russian hackers.
- Financial institutions were next. The State Bank of India （India's largest bank） was attacked by hackers located in Pakistan on December 25, 2008. While no data was lost, the attack forced SBI to temporarily shut down their website and resolve the issue.
- In 2009, a cyber spy network called "GhostNet" accessed confidential information belonging to both governmental and private organizations in over 100 countries around the world. GhostNet was reported to originate in China, although that country denied responsibility.

- ***We are at risk. Increasingly, America depends on computers. […] Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb.***

(National Academy of Sciences 1991: 7)

- ***We did find widespread capability to exploit infrastructure vulnerabilities. The capability to do harm – particularly through information networks – is real; it is growing at an alarming rate; and we have little defense against it.***

(President's Commission on Critical Infrastructure Protection 1997: i)

- ***Our nation is at grave risk of a cyberattack that could devastate the national psyche and economy more broadly than did the 9/11 attacks.***

(Statement in a letter sent to President Bush by former White House adviser Richard Clarke and more than 50 top computer scientists, quoted in Fitzpatrick 2003)

UNITED STATES

- In February of 2010, the United States launched Cyber ShockWave, a cyber war game to see how the nation would be able to respond after a serious cyber-attack. The result showed that the US was not well-prepared for such an attack. A number of things need to be done to get the country up to par.

DEFENSE?

"America's response to the challenges and opportunities of the cyber era will determine our future prosperity and security."

National Security Strategy *of the United States of America* (December 2017)

Priority Actions

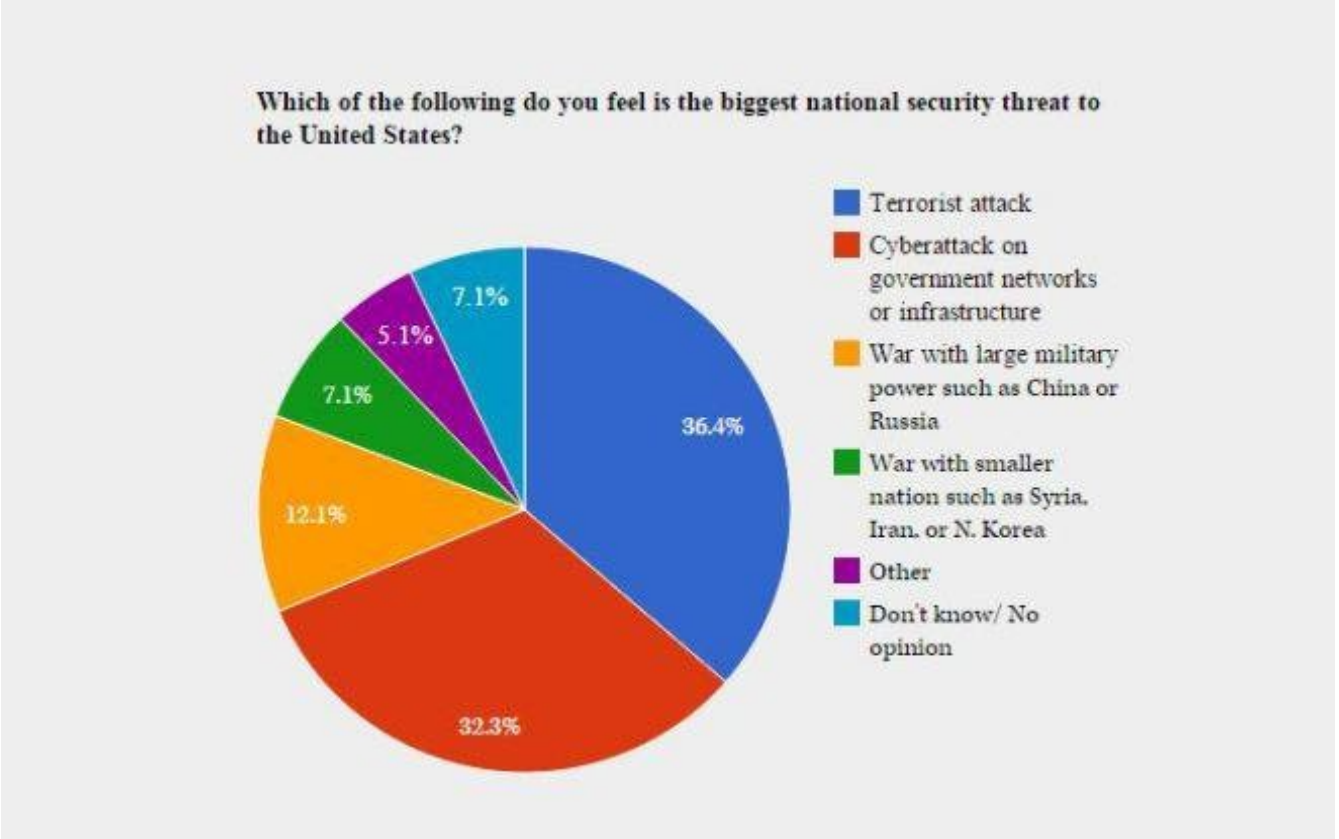
1. IDENTIFY AND PRIORITIZE RISK
2. BUILD DEFENSIBLE GOVERNMENT NETWORKS
3. DETER AND DISRUPT MALICIOUS CYBER ACTORS
4. IMPROVE INFORMATION SHARING AND SENSING
5. DEPLOY LAYERED DEFENSES

REASONS FOR CYBER SECURITY

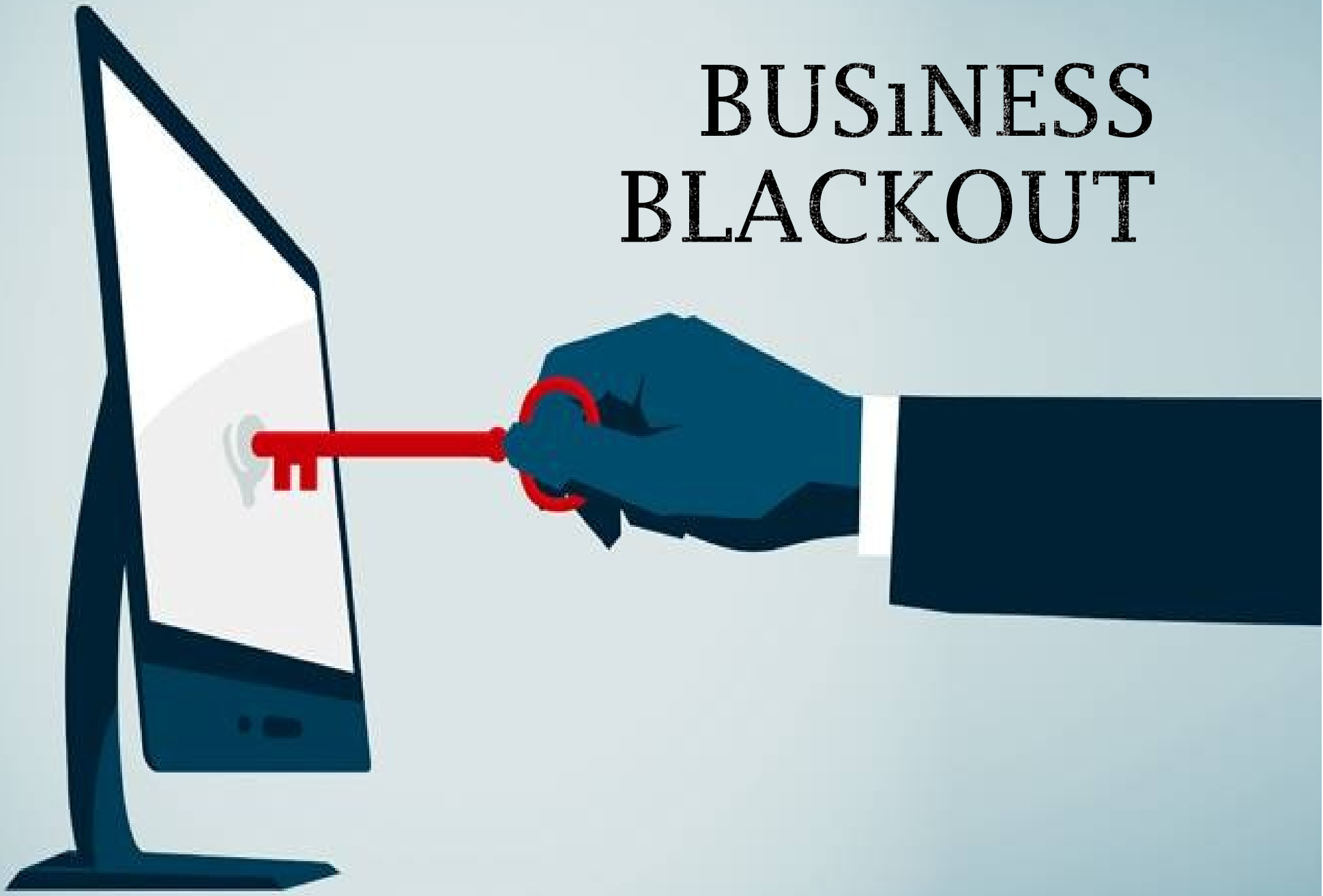
- The increase role of information technology
- The growth of the e-commerce sector
- Protection of infrastructure systems like national power grid

Former Defense Secretary Leon Panetta stated in October 2012 that *"a cyber attack processed by nation states or violent extremist groups could be as destructive as the terrorist attack of 9/11.... Such a destructive cyber terrorist attack could paralyze the nation."*

WHAT WILL HAPPEN IF HACKERS WILL HIT CRITICAL INFRASTRUCTURE IN THE US?



BUSiNESS BLACKOUT



POWER CUT IN ECONOMY…

WHY THE U.S. ROLE ON CYBER CONFLICT IS IMPORTANT FOR GLOBAL ECONOMY?

i. Largest economy

ii. Global economy and US economy go hand in hand

iii. Important export destination

iv. Power of US dollar

CONCLUSION

- Cyber-attacks are going to continue.
- They are cheap, near-anonymous, and can be very effective.
- When used alongside military action, propaganda, or civil unrest, the effect multiplies; people used to their computer services don't like to lose them.
- With the Internet linking up almost every computer, important infrastructure and government computers are at risk as well.
- In most developed nations, the consequences of a cyber-attack can be so great that the threat of an attack may be able to deter military or political action.
- Because of this, governments and private citizens and companies have started working together to implement active cyber defenses.
- With this collaboration, the Internet will hopefully remain safe for everyone.

THANK YOU FOR YOUR ATTENTION ☺

- EMRE AR
- MELİS SABANCI