Cybersecurity & International Relations

Assist. Prof. D. ARIKAN AÇAR, Ph.D.
Department of International Relations,
Yaşar University, Turkey.

Cybersecurity & IR

- This part of the IWOSI aims to link the Information Technology to International Relations discipline.
- Make use of the theoretical background provided at the first day course ‘Introduction to International Relations Theory and Strategy’.

Cybersecurity & IR

- Focus of attention will be on the interstate & state and non-state actor conflicts
- International Security and Shaping of Cybersecurity Policies
- Priorities, strategies and implementation of policies during different cases

Information Technology, Security and International Relations

- National security is essential and at the core of state interests. State centric approach to security.
- Early references to Cyberwar's Coming and Preparing for Conflict in the Information Age as new mode of conflict.
- Contemporary political and strategic context is important to consider cyber threats.
- Militarization of cybersecurity? Is cyberspace a "war fighting domain" to be defended?
- Cyberwar: Its definition is problematic and turns into a metaphor rather than actual act of war.

Information Technology, Security and International Relations

- Differences in perception of possible impacts of the cybersecurity threats
- States trying to develop *modus operandi* and relevant strategies towards their operation in the cyberspace in order to secure their interests.
- Debate is going on in IR and Security Studies about the existence and the impact of the cyberwar in international affairs.
- Cyberwar concept criticized from a *Clausewitzian* perspective of war with reference to war's violent and instrumental characters and its political nature. (pp. 3-4)

Information Technology, Security and International Relations

- Non-state actors' increasing involvement in the security realm, increase in politically motivated cyber attacks
- Terrorist threats and potential of asymmetric impacts of cyber attacks
- Outsourcing cyber attacks / governments use of private cyber attackers
- Unmanned Aerial Vehicles / Drones
- Military organizations' conceptualizations and doctrine formation related to technological advancements: network-centric warfare, C^4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance)

Cyber-weapon

- **Computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings.**
- **Generic Cyber-weapon: relatively simple, commercially available and not aim specific target**
- **Specific Cyber-weapon: Sophisticated and purpose built, may function with autonomous software**

(Rid and McBurney, Cyber-weapons, The RUSI Journal, vol. 157, no.1, p.7).

Cyber Threats to States: Vulnerabilities of National Critical Infrastructures

- **Energy**
- **Transportation**
- **Communication**
- **Water and Sanitation**
- **Finance**
- **Industrial Processes**
- **Government Administrations**

Threats directed to the Supervisory Control and Data Acquisition (SCADA) systems that are used to monitor and control processes in various critical infrastructure facilities by changing or stopping them. [Trans-Siberian Pipeline Explosion]

Important Cases that Drew the Attention of the International Relations Community to Cyber Threats

- Late April-mid May 2007, Estonia Distributed Denial of Service Attacks (DDoS).
- 6 September 2007, Neutralizing air defense network during Israeli air strike to Syrian nuclear facilities.
- August 2008, DDoS Attacks and acts of hacking websites during Georgia-Russia conflict.
- July 2009 and March 2011 South Korea faced DDoS attacks that targeted government, news media and financial websites. North Korea was suspected to conduct such campaigns.

The Unknown Soldier, Russian WWII Memorial moved from Tallinn centre to outskirts (27-28 April 2007) leading to social unrest, diplomatic tension and distributed denial of service (DDoS) attacks for three weeks via botnets. Very limited physical impact. Russia denied official involvement.

Estonia Cyber Attacks

- Sharply raised the awareness for cybersecurity among states and decision makers especially in the West.
- States focused their attention to create or develop indigenous cyber security capabilities.
- Contributed to the intensification of efforts to institutionalize cooperation in the field of cybersecurity.

Estonia Cyber Attacks

- NATO opened its Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn in May 2008 which was accredited by October 2008.

- NATO recognized cyber attacks as one of the threats existing within the contemporary 'Security Environment' in its new Strategic Concept of November 2010.
- NATO commit itself to "develop further [its] ability to prevent, detect, defend against and recover from cyber attacks" and "better integrating NATO cyber awareness, warning and response with member nations".

Israeli Attack to Syria (6 September 2007)

- Israel claimed that with the air assault it aimed Syrian nuclear facilities and program (Israel had also stroked Iraq's Osirak nuclear reactor in).
- During the Israeli Air Force's Operation Orchard, Syrian radars could not pick any enemy signals and air defense systems could not be activated (pp. 4-7).
- Cyber weapons proved to be a useful element in supporting the conventional military operations.

Georgia-Russia Conflict of August 2008

- Georgia-Russia fought for Georgian control over South Ossetia and Abkhazia
- Distributed Denial of Service Attacks (DDoS) accompanied Russian military operations.
- Cyber attacks targeted Georgian government and media web sites leading to problems related to dissemination information to Georgian people.
- Georgian experience with cyber attacks were similar to Estonian case.

Important Cases that Drew the Attention of the International Relations Community to Cyber Threats

- September 2010, Stuxnet damaging Iranian nuclear program
- March 2011, discussion to use cyber weapons during NATO Operation to Libya
- October 2011, German government / domestic law enforcement use of a trojan (Bundestrojaner, R2D2) to spy on criminal suspects and intelligence gathering.

Iran Related Cyber Attack and Cyber Espionage News

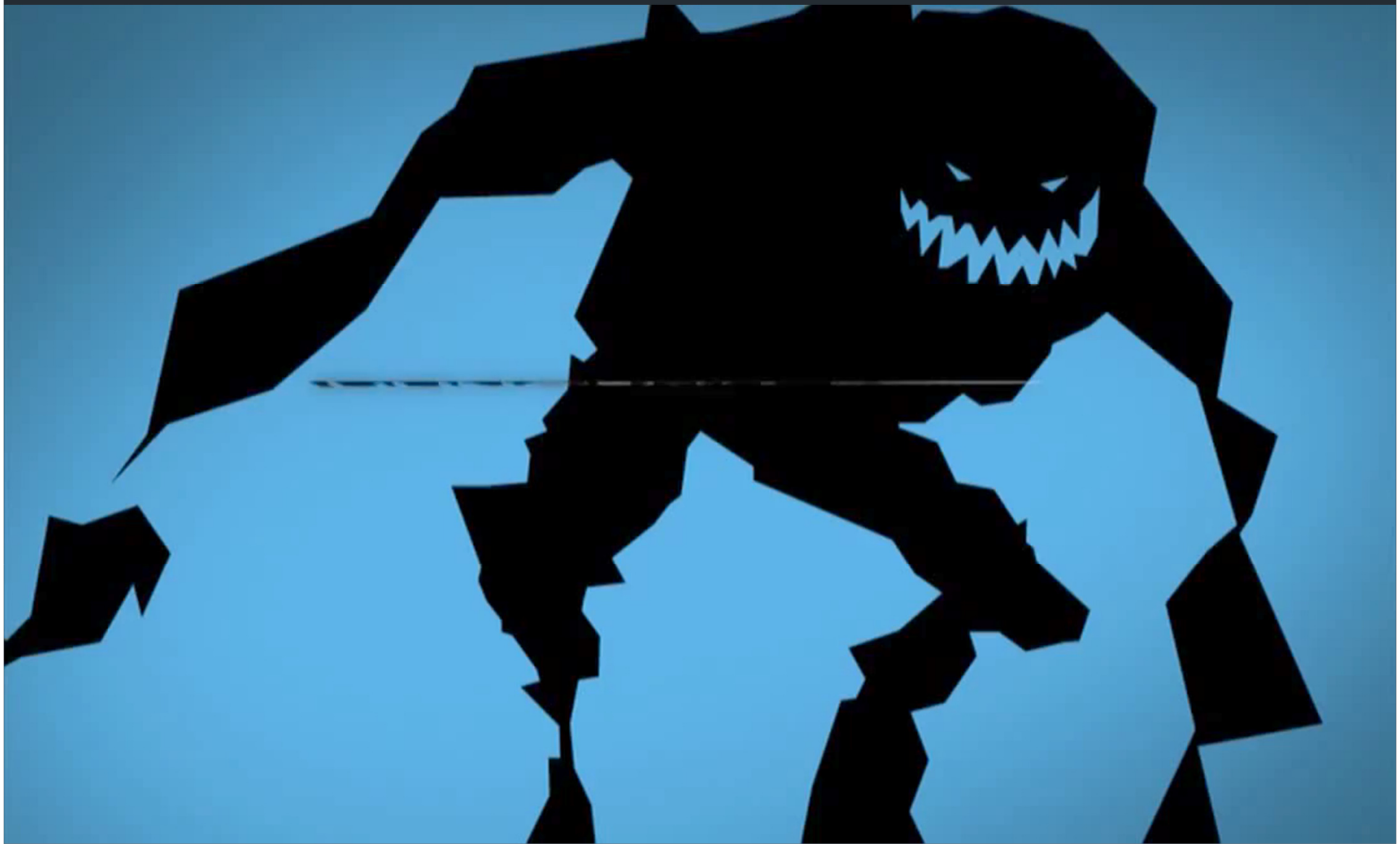
- **“Iranian oil terminal ‘offline’ after ‘malware attack’”**
  BBC News, 23 April 2012

- **“Iran says it has 'controlled' Duqu malware attack”**
  BBC News, 14 November 2011

- **“Iran 'uncovers Stars espionage virus’”**
  BBC News, 25 April 2011

- **“Stuxnet worm hits Iran nuclear plant staff computers”**
  BBC News, 26 September 2010

From Australian TV ABC1 Program Hungry Beast.
Stuxnet: Anatomy of a Computer Virus, 8 June 2011.



STUXNET

- Stuxnet is a threat targeting a specific industrial control system likely in Iran, such as a gas pipeline or power plant.

- The ultimate goal of Stuxnet is to sabotage that facility by reprogramming programmable logic controllers (PLCs) to operate as the attackers intend them to, most likely out of their specified boundaries.

Symantec Security Response W32.Stuxnet Dossier, Version 1.4, February 2011, p. 2. Stuxnet Redux: Questions and Answers, F-Secure, 23 November 2010.

- [Siemens SCADA Equipment are in use in Iranian industrial plants]

WHY STUXNET TARGETED IRAN?

Nuclear Non-Proliferation Regime

- Treaty on the Non-Proliferation of Nuclear Weapons (NPT), 5 March 1970. International Atomic Energy Agency (IAEA) safeguards the non-proliferation system. Iran is a party to the Treaty. Israel, India and Pakistan did not signed, N. Korea withdrew.
- Article II of NPT: Each non-nuclear-weapon State Party to the Treaty undertakes not to receive the transfer from any transfer or whatsoever of nuclear weapons or other nuclear explosive devices or of control over such weapons or explosive devices directly, or indirectly; not to manufacture or otherwise acquire nuclear weapons or other nuclear explosive devices; and not to seek or receive any assistance in the manufacture of nuclear weapons or other nuclear explosive

WHY STUXNET TARGETED IRAN?

Nuclear Non-Proliferation Regime

- Treaty on the Non-Proliferation of Nuclear Weapons
- Article IV of NPT: 1. Nothing in this Treaty shall be interpreted as affecting the inalienable right of all the Parties to the Treaty to develop research, production and use of nuclear energy for peaceful purposes without discrimination and in conformity with Articles I and II of this Treaty.

Cyber-weapons and Espionage Tools

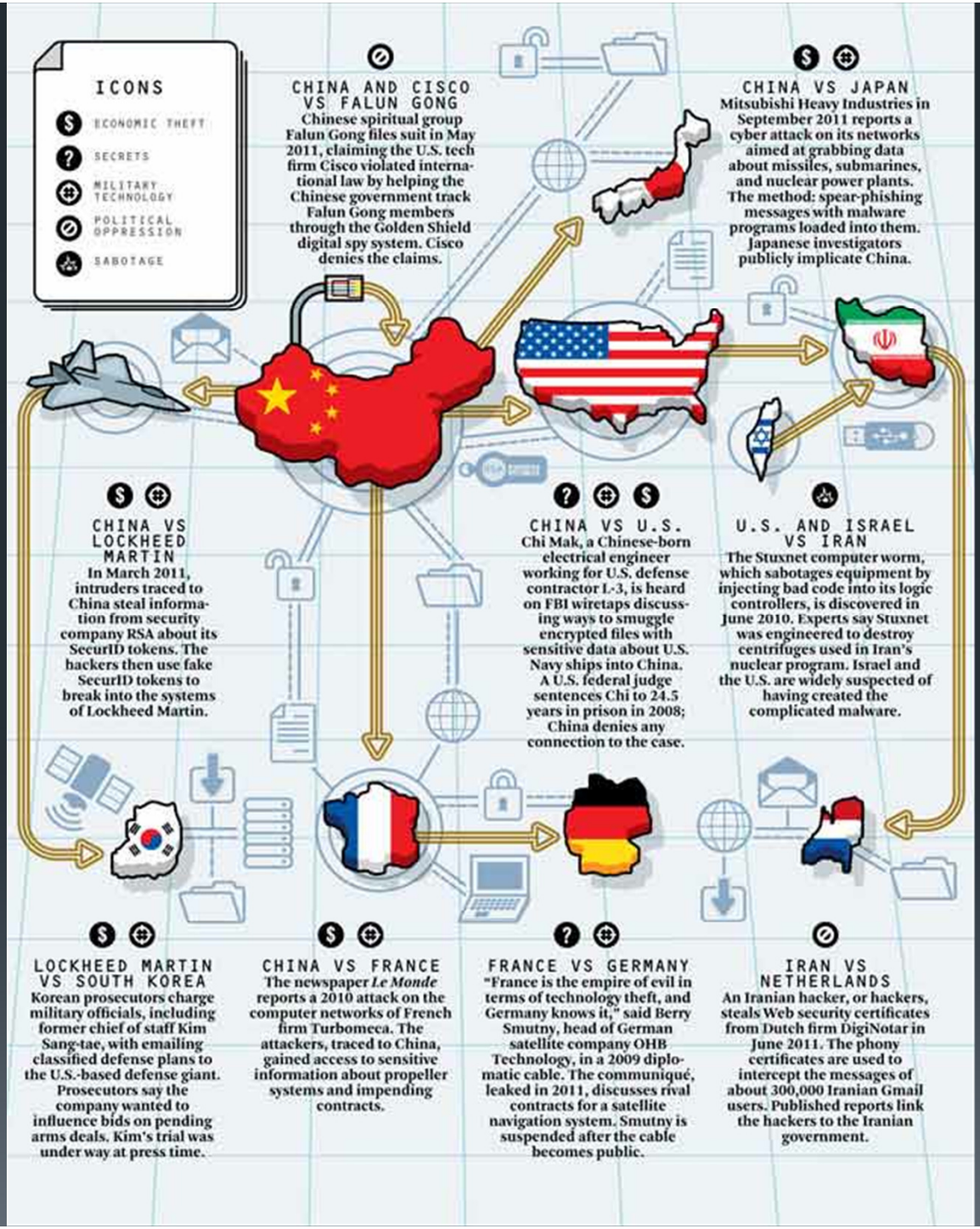
- Stuxnet is a weapon aims to physical harm.
- Stuxnet is a sophisticated and specific cyber-weapon. However it is argued that it used “off-the-shelf code and tradecraft” and thus quickly and effectively disarmed. (p. 27)
- It is argued that Stuxnet caused at least few years of delay in Iranian nuclear program.
- Duqu is a information and intelligence gathering tool.
- Cybersecurity threats has psychological effects as well as physical impacts.
- Iranian government could not direct its reaction to any state depending on physical evidence.

Sabotage, Espionage and Subversion

- Inter-state relations witness various ways of use of information technology and cyberspace for political, economic other purposes such as;

- Information theft related to economic interests
- Stealing military and civilian technology
- Espionage and counterespionage
- Means of political oppression

- Sabotage, Espionage and Subversion (pp.12-23).



- [Who's Spying on Whom? A Map of Digital Subterfuge]

Popular Mechanics,

THANK YOU FOR YOUR ATTENTION

Bibliography