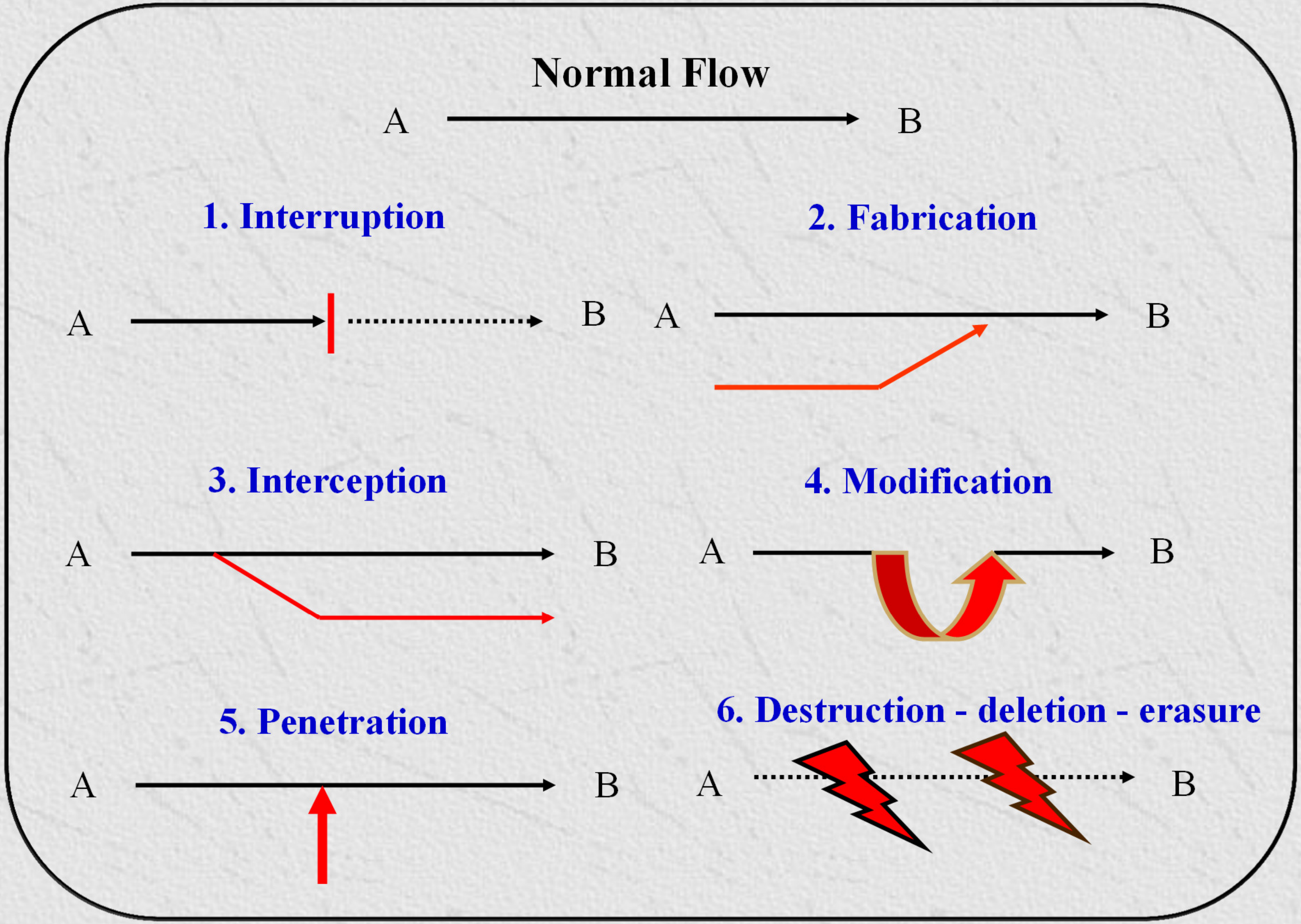
The *modis operandi* of a Cyber Attack



Dr. Ahmet Koltuksuz

Section #2 Exploitation of Internet by Terrorism

Who are they?

Why cyber space?

What are the targets?

What do they do?

How do they do?

Tools they exploit.

Who are they?

- International terrorist groups
- Transnational cybercrime organizations
- Individual extremists, insurgents
- Lone wolves
- Individual national or international terrorists

Anatomy of a Computer Criminal-PROFILING

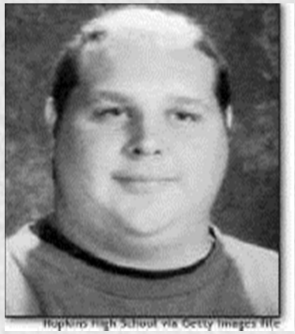
There are three distinctive periods.

1. Pre-Internet, Romantic Period: 1950-1980
2. Internet Period: 1980-2000
3. Digital Society: 2000s and beyond

1. Pre-Internet, Romantic Period: 1950-1980

- Young, aged 14-34, dynamic, higly educated, bright & successful.
- Smart, trustworthy, well behaved manners, respectful.
- Healty, white, mostly males.
- Mostly no criminal records of any kind.
- Having difficulties when establishing contacts with other people. No permanent girl friends
- Feels that he has to prove himself.
- Thinks that he is undervalued, underestimated by the society.
- Feels no remporse at all since he acts against societal bodies & governments but not against any particular person.
- Agile, unpatient, highly motivated & competitive, over ambitious.
- Able to justify his existance only by computer. Computer addicts.

1. Pre-Internet, Romantic Period: 1950-1980



Hopkins High School via Getty Images file

No Commercial Interest !!!

Kevin Mitnick in his younger days.

Kevin Mitnick

1. Pre-Internet, Romantic Period: 1950-1980

Name: Peiter Mudge Zatko
Handle(s): Mudge, PeiterZ
Marital status: Single
Current residence: New England, USA
Job: Chief Scientist, Intrusic
First computer: Tektronix 4051
Best known for: Creating L0phtCrack
Area(s) of expertise: "Thinking outside of the box"

Pieter Mudge Zatko

1. Pre-Internet, Romantic Period: 1950-1980

Name: Raven Alder
Handle(s): Raven
Age: 28
Place of birth: Mississippi, USA
Marital status: Single
Current residence: Maryland, USA
Job: Security consultant, True North Solutions
First computer: Home-built 8088 machine in 1988
Best known for: Tracing spoofed distributed denial of service attacks
Area(s) of expertise: ISP backbone networking, protocol decoding and design, Linux/BSD security, and cryptography

Raven Alder

2. Internet Period: 1980-2000

Untargeted, unconsciously aggressive

No target of any kind.

Lacks of techical knowledge & information.

Easy to pursuit & easy to catch.

Dangerous, represents the majority of the aggressive group.

Targeted, but unconsciously aggressive

With an aim, however no plans or programs.

Moderate information, usually thru friends.

Utilizes software of others.

Leaves too many evidences

Untargeted, but consciously aggressive

Random targets.

Dangerous armed with technical information & skill.

Utilizes specially created hardware & software.

Fells anxiety of being caught, hides away.

Targeted AND consciously aggressive

Has an aim, plan & program.

Very dangerous and armed with a high technological info and very high degree of various skills.

Deliberately hides away.

Uses very special devices of both hardware & software.

2. Internet Period: 1980-2000

Hackers

Best there is, Black Hat – White Hat

Crackers

Usually negative, up to being a hacker. Code cracking.

Lamers

After fame, think that they are hackers, usually utilize viruses and other ready-made software.

Script-Kid / Cyber-Punks

Experts in computer technology, young and have a high ego, trying to prove themselves.

Hobbists– Users

Mostlyt harm the systems without knowing, unhappy employees.

3. Digital Society: 2000s and beyond

The one and only motivation is **MONEY**.

Expert & career computer criminals.

Even subexpertise areas such as

> Linux, Windows, Mac, Android Operating systems
> Virus & Worm writers, Botnet Herders,
> PinPad, Skimmer, Collectors...

Crime groups with future projections and plans...

3. Digital Society: 2000s and beyond

3. Digital Society: 2000s and beyond

Underground goods and services

Rank	Last	Goods and services	Current	Previous	Prices
1	2	Bank accounts	22%	21%	$10-1000
2	1	Credit cards	13%	22%	$0.40-$20
3	7	Full identity	9%	6%	$1-15
4	N/R	Online auction site accounts	7%	N/A	$1-8
5	8	Scams	7%	6%	$2.50/wk - $50/wk (hosting); $25 design
6	4	Mailers	6%	8%	$1-10
7	5	Email Addresses	5%	6%	$0.83-$10/MB
8	3	Email Passwords	5%	8%	$4-30
9	N/R	Drop (request or offer)	5%	N/A	10-50% of drop amount
10	6	Proxies	5%	6%	$1.50-$30

3. Digital Society: 2000s and beyond

A Typical Botherder: 0x80

High school dropout

“…most of these people I infect are so stupid they really ain't got no business being on the Internet in the first place.“

Working hours: approx. 2 minutes/day to manage Botnet

Monthly earnings: $6,800 on average

Daily Activities:

Chatting with people while his bots make him money

Recently paid $800 for an hour alone in a VIP room with several dancers

Job Description:

Controls 13,000+ computers in more than 20 countries

Infected Bot PCs download Adware then search for new victim PCs

Adware displays ads and mines data on victim's online browsing habits.

Bots collect password, e-mail address, SS#, credit and banking data

Gets paid by companies like TopConverting.com, GammaCash.com, Loudcash, or 180Solutions.

Why Cyber Space?

- Anonymity
- Abundance of diverse targets
- Low risk of detection
- Low risk of personal injury
- Low investment
- Operate from nearly any location
- Few resources are needed

What are Their Possible Targets?

- Destruction of hardware and/or software, or physical damage to personnel or equipment using information technology as the medium.
- The chaos and destruction caused by disrupting a nation's air traffic control system.
- Crashing two trains together by overriding the railroad signal and switching system.
- Interfering with the control systems for water or electricity.
- Blocking and falsifying commercial communications to cause economic disruption.

What do they do?

- Using of Internet as means of

1. radicalization & of propaganda distribution machine,
2. of recruitment and organization,
3. for training grounds,
4. for fund-raising through cybercrime,
5. and of communication.

How do they do?

- Exploitation of Internet as means of a propaganda distribution machine, as of recruitment and organization:
  - “They exploit the Internet medium to raise awareness for their cause, to spread propaganda, and to inspire potential operatives across the globe.”
  - “Websites operated by terrorist groups can contain graphic images of supposed successful terrorist attacks, lists and biographies of celebrated martyrs, and forums for discussing ideology and methodology.”

How do they do?

- Exploitation of Internet for a training ground:
  - “The websites can also carry step-by-step instructions on how to build and detonate weapons, including cyber weapons.”
  - “One website reportedly carries a downloadable “e-jihad” application, through which a user can choose an Internet target and launch a low-level cyberattack, overwhelming the targeted website with traffic in order to deny its service.”
  - “The websites may also contain instructions for building kinetic weapons, such as bombs and improvised explosive devices, as well as for conducting surveillance and target acquisition.”

How do they do?

- Exploitation of Internet for a training ground:
  - “The Internet can also be used to transmit information and material support for planned acts of terrorism.”
  - “A recent case involving a U.S. citizen residing in Pennsylvania alleges that a woman using the nickname “JihadJane” posted messages on YouTube and used jihadist websites and chat rooms to plan and facilitate an overseas attack.”

How do they do?

- Exploitation of Internet for fund-raising through cybercrime:
  - “Several recent terrorist events appear to have been funded partially through online credit card fraud which is a cyber crime.”
  - “Extremist hackers have reportedly used identity theft and credit card fraud to support terrorist activities.”
  - “When terrorist groups do not have the internal technical capability, they hire organized crime syndicates and cybercriminals through underground digital chat rooms.”

How do they do?

- Exploitation of Internet for fund-raising through cybercrime:
  - "Reports indicate that terrorists and extremists in the Middle East and South Asia may be increasingly collaborating with cybercriminals for the international movement of money and for the smuggling of arms and illegal drugs."
  - "These links with hackers and cybercriminals may be examples of the terrorists' desire to refine their computer skills."
  - "The relationships forged through collaborative drug trafficking efforts may also provide terrorists with access to highly skilled computer programmers."

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.”