On the Imbalance of the Security Problem Space and its Expected Consequences

Konstantin (Kosta) Beznosov
Electrical and Computer Engineering

Olga Beznosova
Political Science

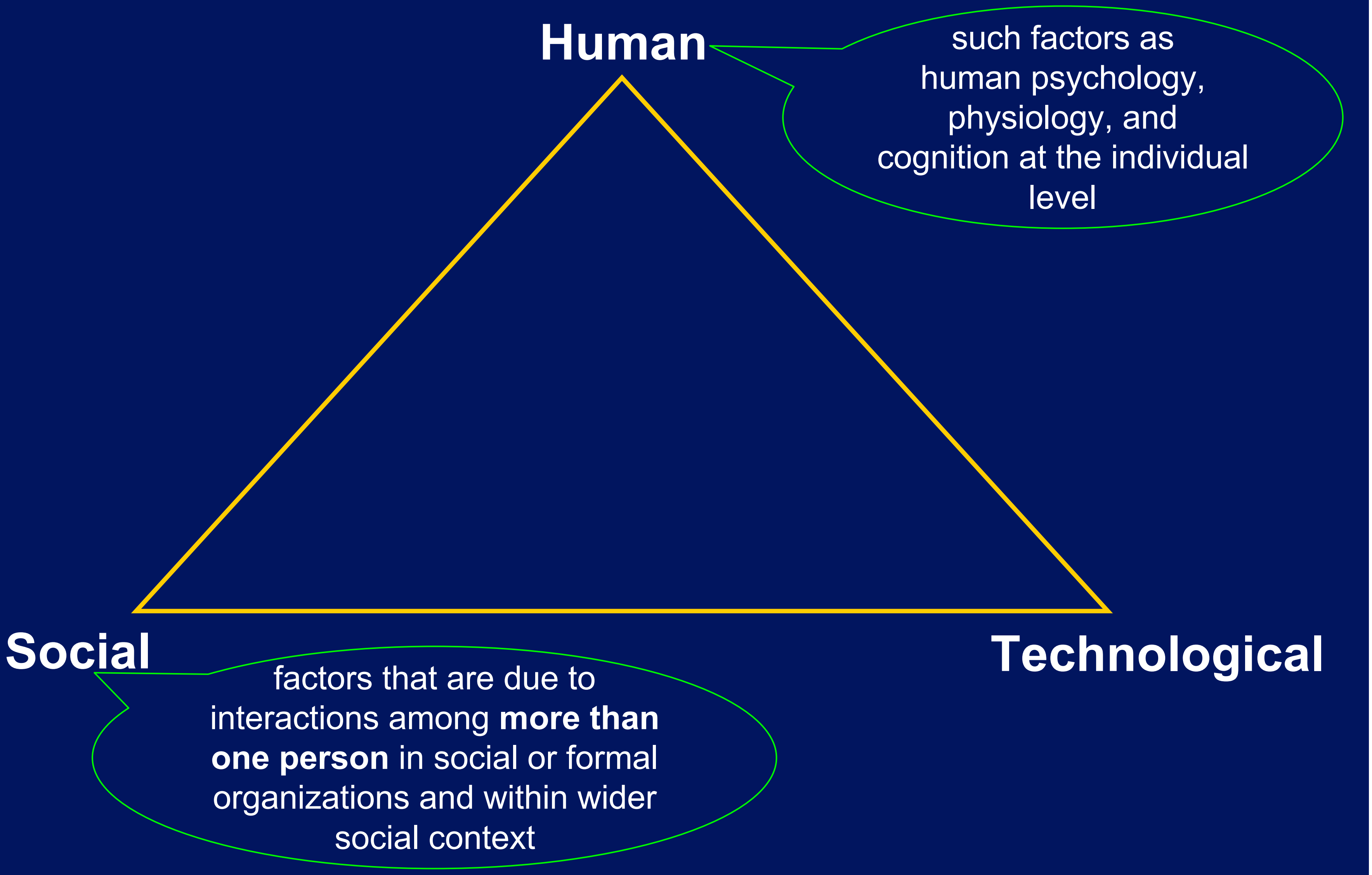
University of British Columbia
Vancouver, Canada

Outline

- where and how large the imbalance
- why should defenders care
- how attackers use social aspects
- where to go
  - Looking outside of today security
  - Questions for future research

Where and How Large the Imbalance?

Decomposed Problem Space



Human

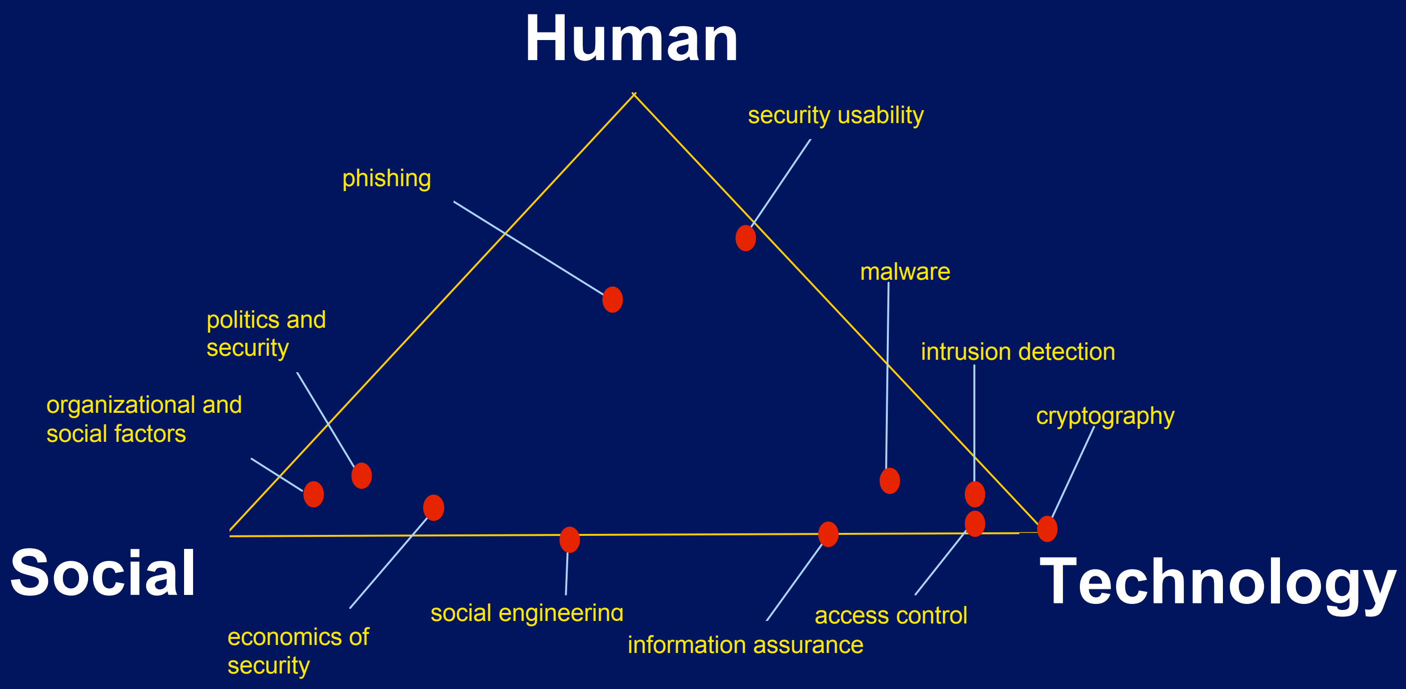
such factors as human psychology, physiology, and cognition at the individual level

Social

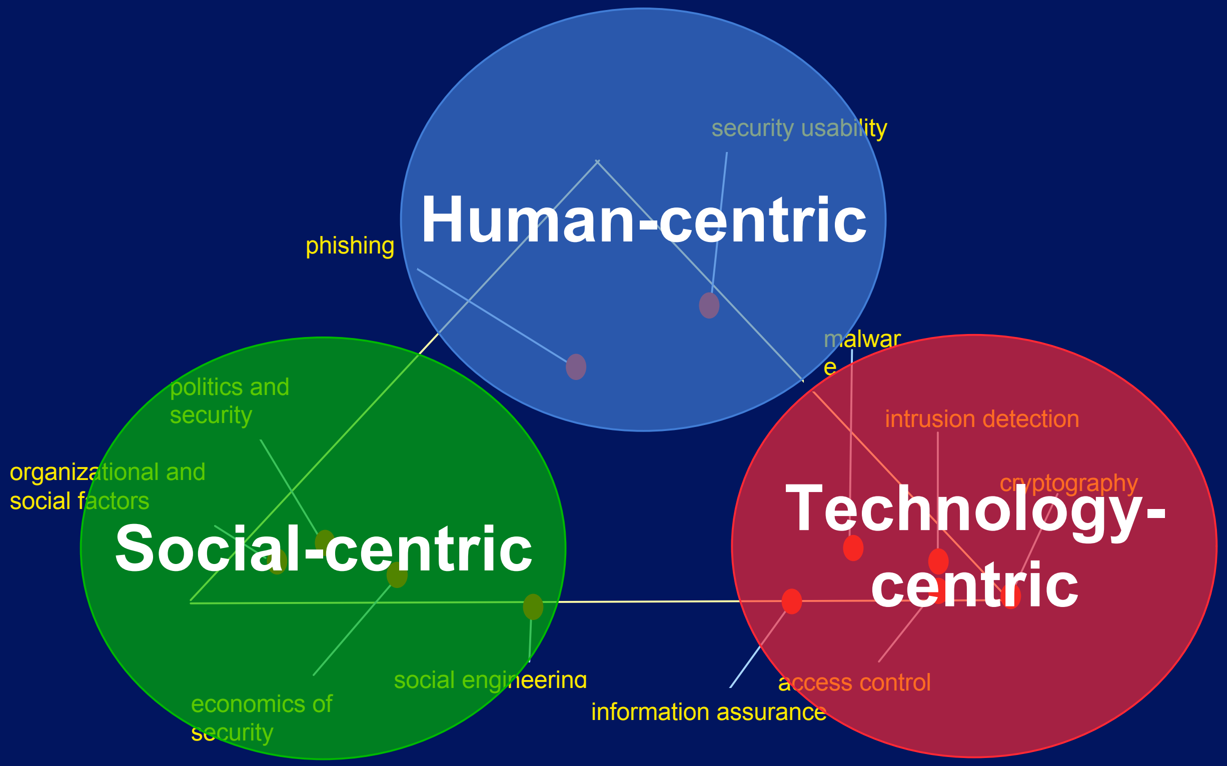
factors that are due to interactions among **more than one person** in social or formal organizations and within wider social context

Technological

Mapped Subareas Of Security



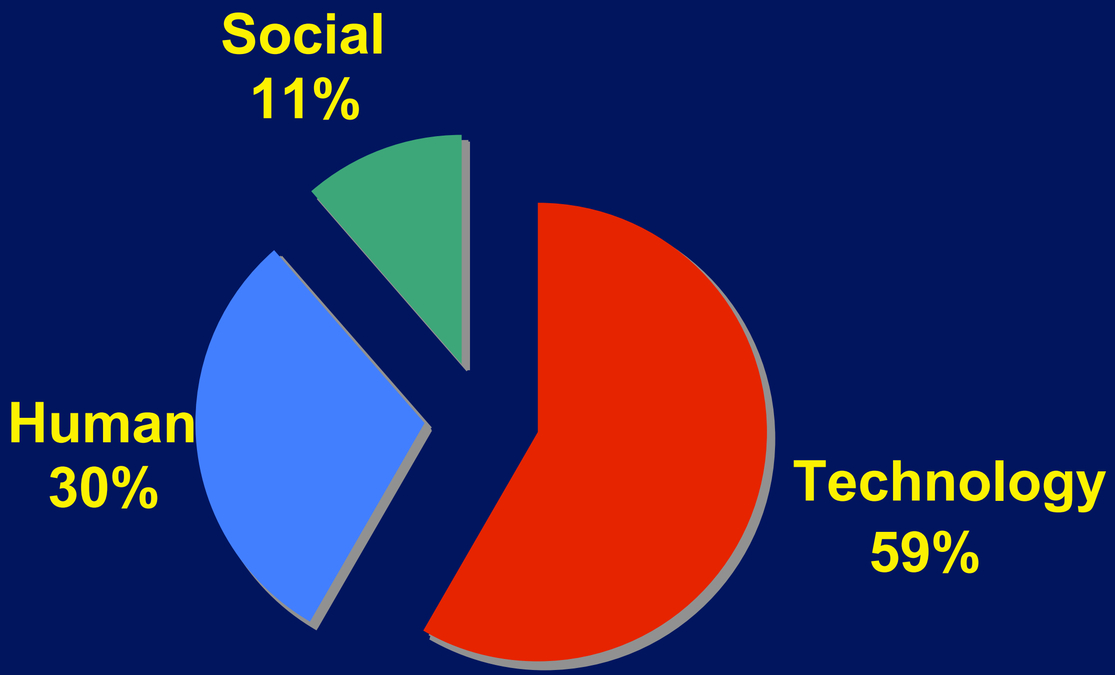
Grouped Sub-areas



Performed Searches

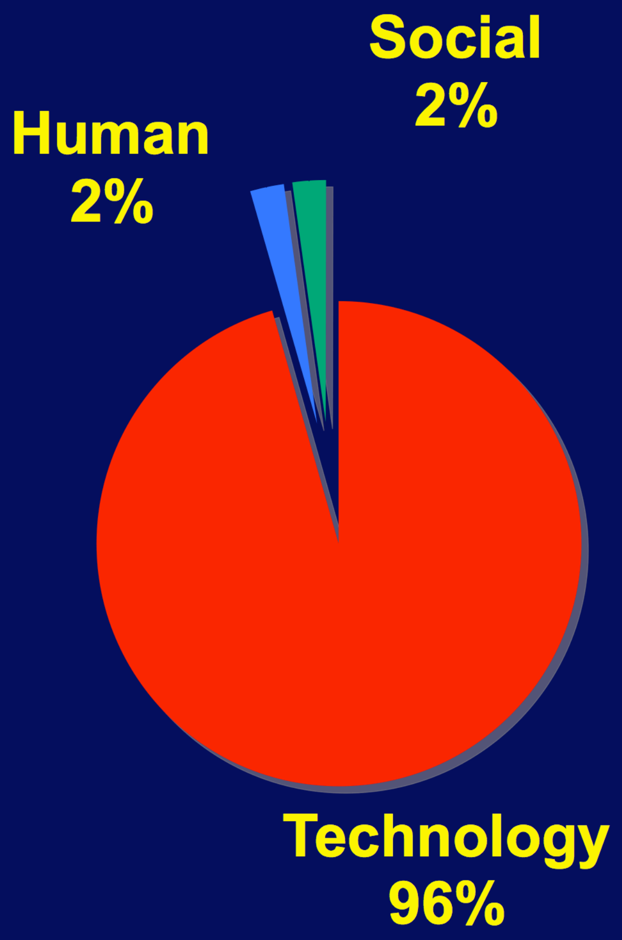
Category/sub-area	Query
Technology-centric	
Cryptography	cryptography OR cryptographic OR encryption OR decryption
Access Control	("access control" OR authorization) AND computer AND security
Intrusion detection	intrusion AND detection AND computer AND security
information assurance	computer ("security assurance" OR "information assurance") -financial -social
malware	malware OR "computer worm" OR "computer virus" OR "malicious software"
Human-centric	
security usability	security AND (usability OR usable OR HCI)
phishing	phishing
Social-centric	
social engineering	"social engineering"
economics of security	(economics AND ("information security" OR "computer security")) OR "security economics"
politics and security	(politics OR bill OR legislation OR regulation) and ("information security" OR "computer security")
human factors	(security AND "human factor") OR "security awareness" OR "security training" OR "security culture" AND (computer OR information)

Google News



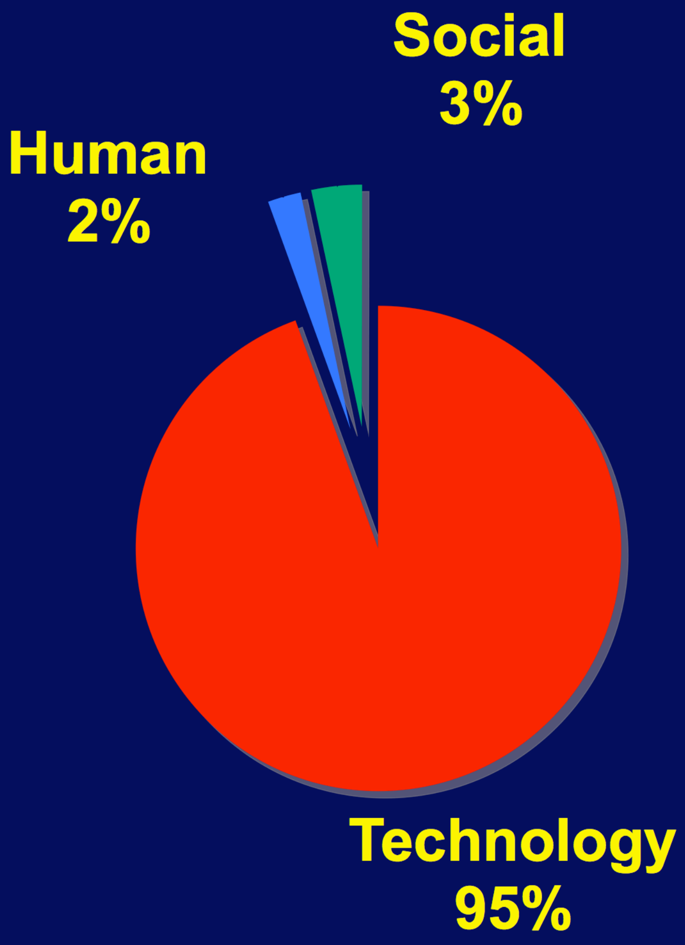
news.google.com

Engineering Village



engineeringvillage2.org
Compendex -- 9M engineering references and abstracts
Inspec -- 8M records from scientific and technical journals and conferences

Web of Science



isiknowledge.com
8,700 research journals

So What?

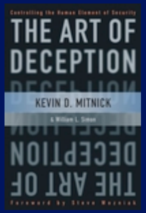
Attackers Increasingly Aware of Human and Social Aspects

- "Most users encounter PC security issues because they fall for social engineering tactics ..."

Fathi, Microsoft's vice president for the
Windows core operating system (Hines 2007)

- "I was so successful in that [social engineering] line of attack that I rarely had to resort to a technical attack."

Kevin Mitnick in testimony before the U.S. Congress
(The Associated Press 2000)



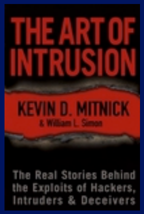
Controlling the Human Element of Security

THE ART OF DECEPTION

KEVIN D. MITNICK

& William L. Simon

Foreword by Steve Wozniak



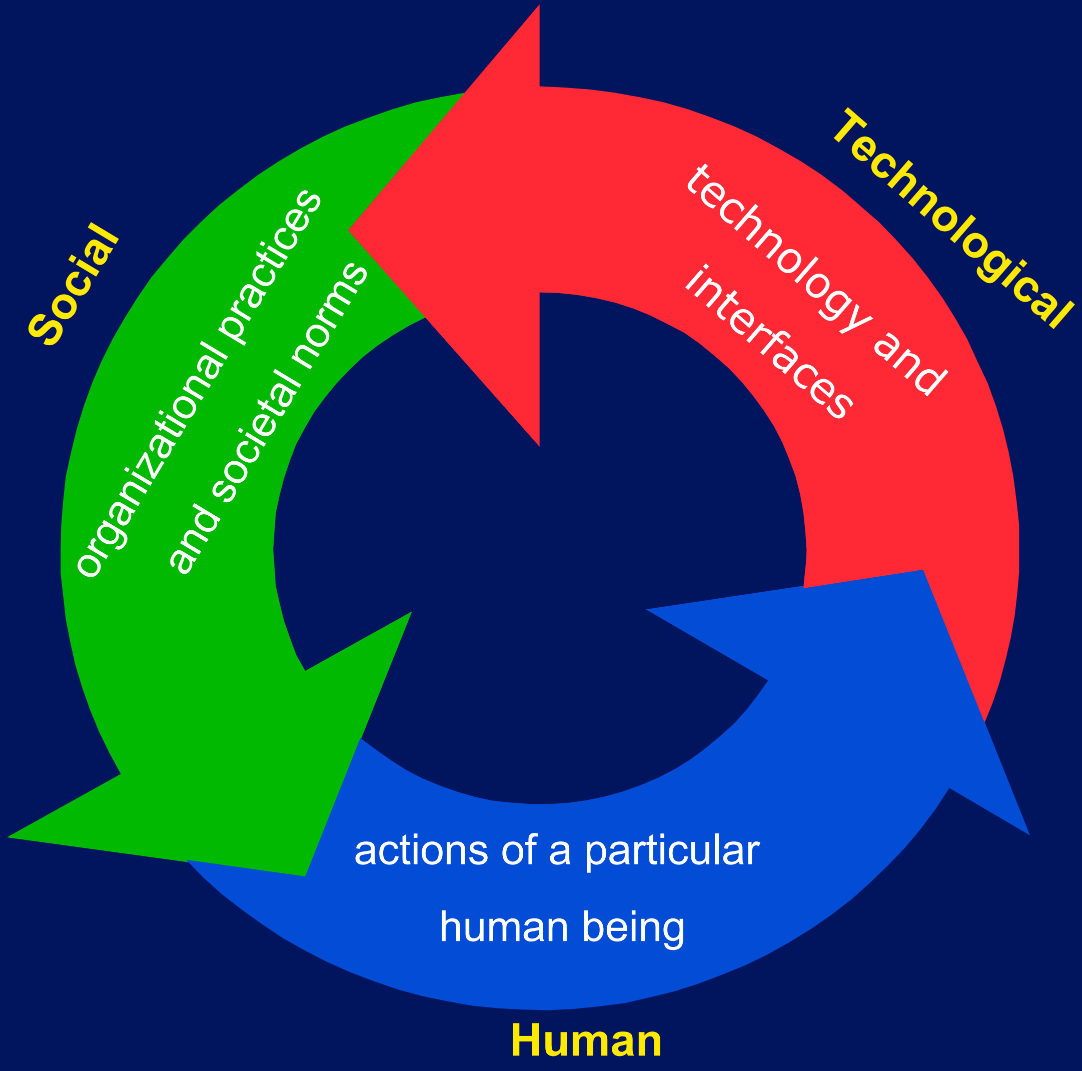
THE ART OF INTRUSION

KEVIN D. MITNICK

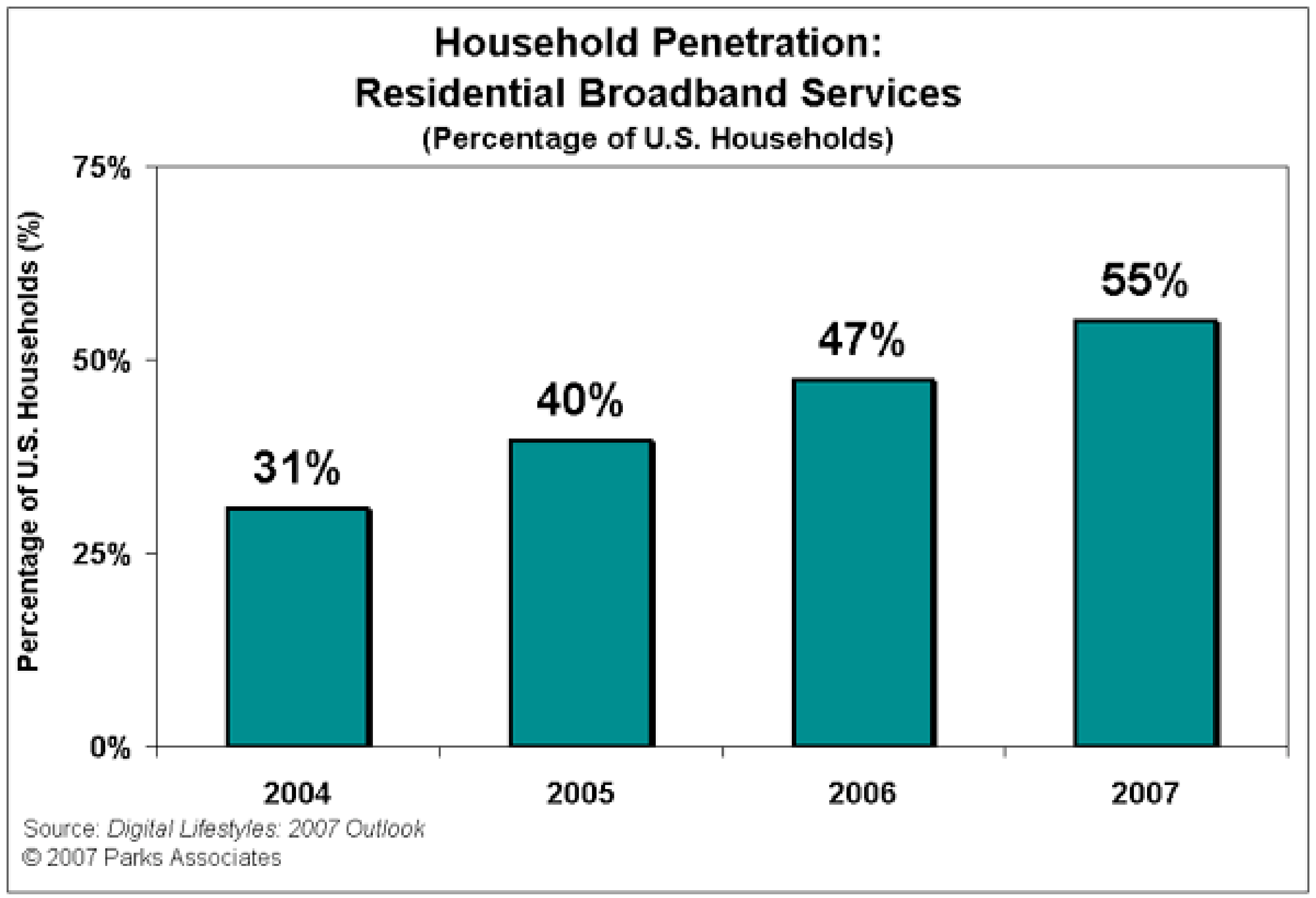
& William L. Simon

The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers

Social Engineering Attacks



Level of User Security Knowledge Declines



Source: *Digital Lifestyles: 2007 Outlook*
© 2007 Parks Associates

Ought to Explore the Social Aspects To Achieve Results Not Possible Otherwise

"If the enemy leaves a door open, you must rush in."
(Sun Tzu, *The Art of War*, ca. 515 BC)

Case Study: Cyber War In Estonia

source: slate.com

Estonia 2007

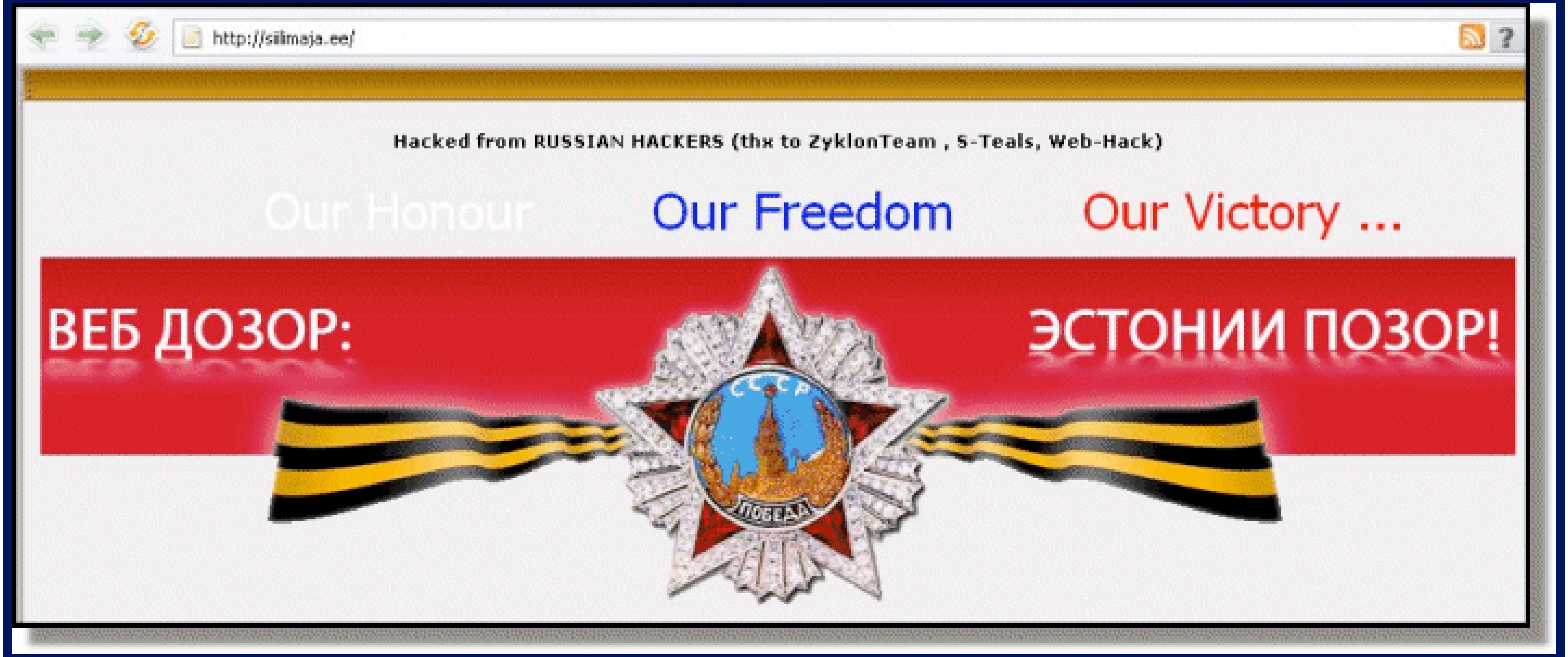
- Highly dependant on computers
  - parking payments
  - Wi-Fi
  - national elections
- Political Incident
  - Estonia's embassy sealed and attacked
  - Cyber attacks continued …

source: economist.com

"Police arrested 600 people and 96 were injured in a second night of clashes in Estonia's capital over the removal of a disputed World War Two Red Army monument …
Russia has reacted furiously to the moving of the monument …
Estonia has said the monument had become a public order menace as a focus for Estonian and Russian nationalists."

CNN

Defacing Estonian Websites …



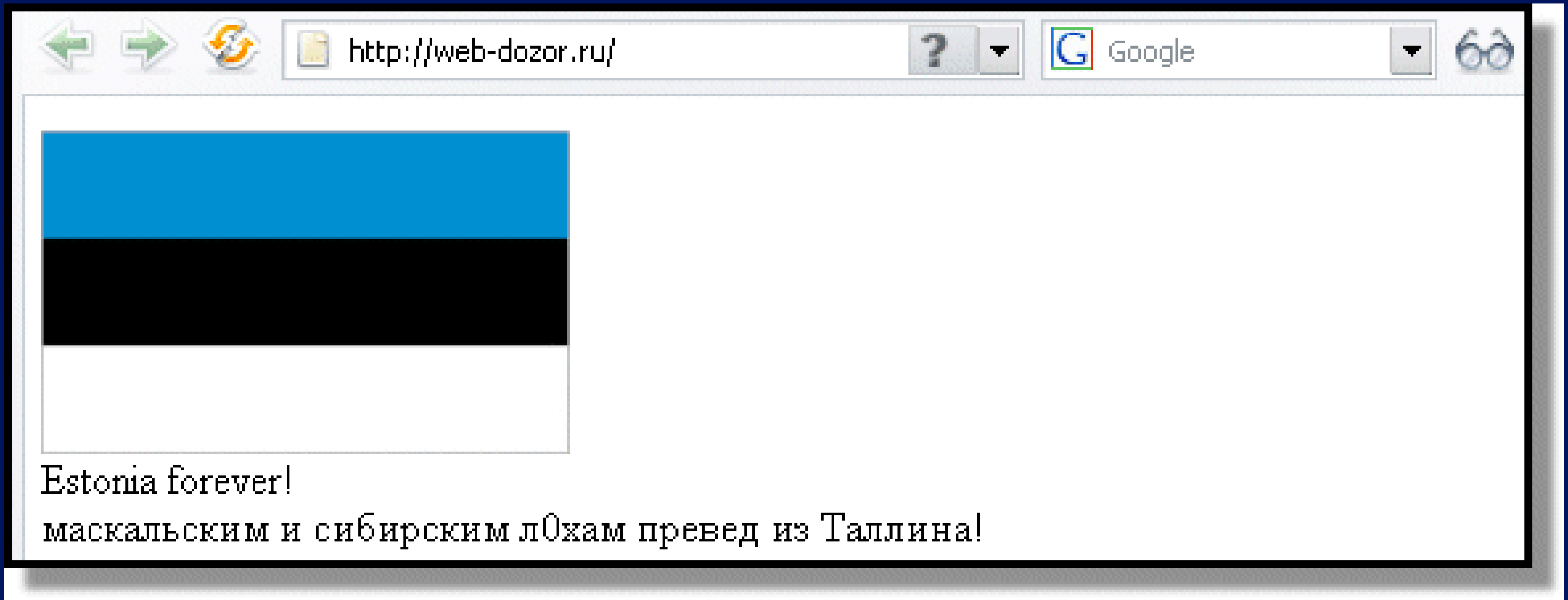
Hacked from RUSSIAN HACKERS (thx to ZyklonTeam , 5-Teals, Web-Hack)

Our Honour Our Freedom Our Victory ...

ВЕБ ДОЗОР: ЭСТОНИИ ПОЗОР!

source: f-secure.com

Some times experiencing reciprocity



Estonia forever!

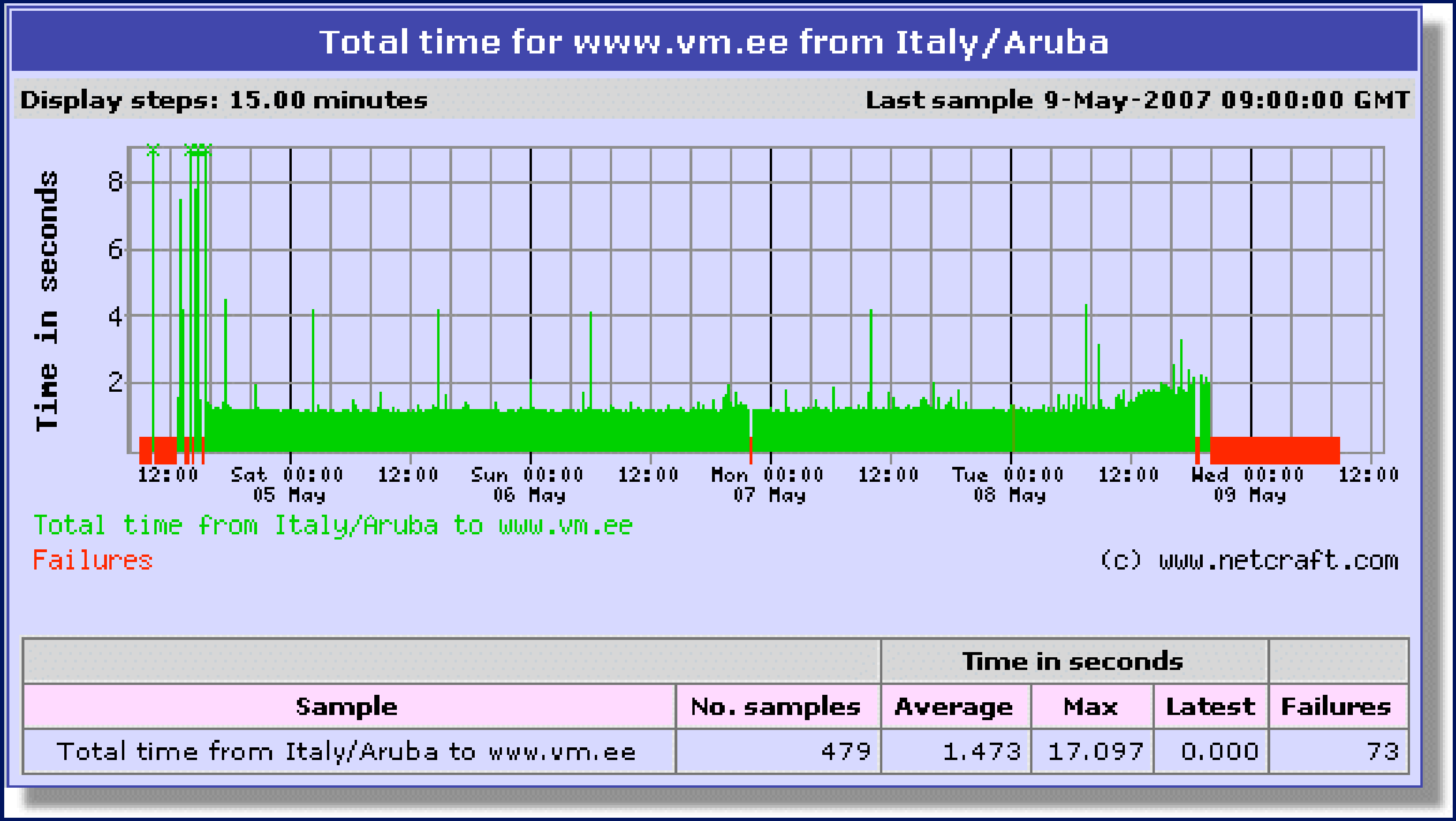
маскальским и сибирским л0хам превед из Таллина!

source: f-secure.com

But most importantly …

Bringing Critical Sites Down …

Availability of Estonian Ministry of Foreign Affairs Web site
May 5-9, 2007



Total time for www.vm.ee from Italy/Aruba

Display steps: 15.00 minutes

Last sample 9-May-2007 09:00:00 GMT

Total time from Italy/Aruba to www.vm.ee

Failures

(c) www.netcraft.com

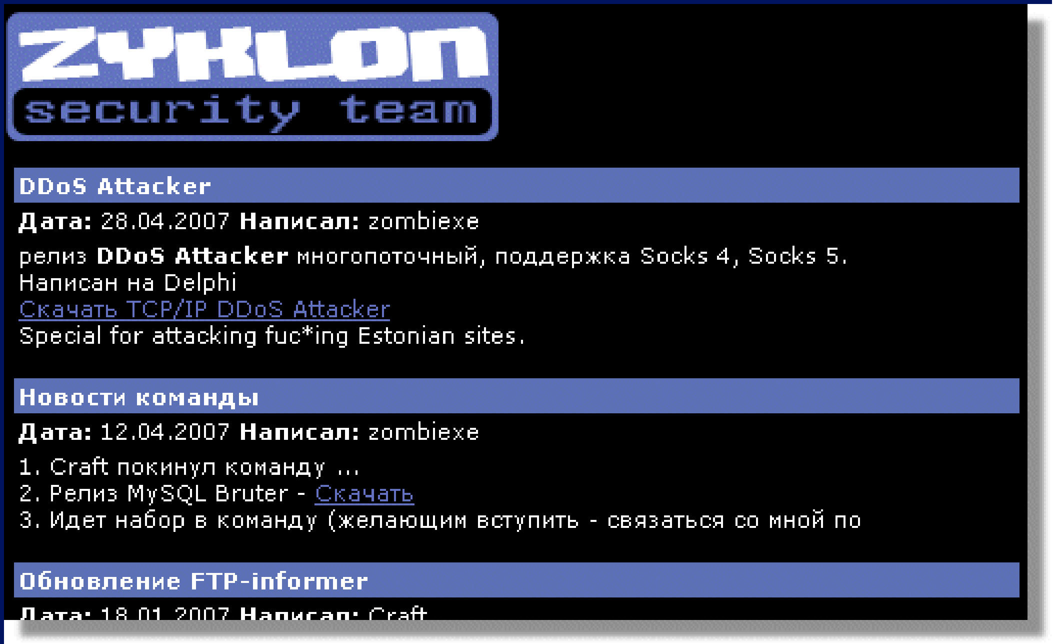
		Time in seconds			
Sample	No. samples	Average	Max	Latest	Failures
Total time from Italy/Aruba to www.vm.ee	479	1.473	17.097	0.000	73

source: f-secure.com

Through Distributed Denial of Service Attacks

- protesters running DoS programs
- botnets
- 128 attacks
  - 115 were ICMP floods
  - 4 TCP SYN floods
  - 9 generic traffic floods
- maxing to 95 Mbps
- up to 10 hours
- shutting 58 sites at once

source: asert.arbornetworks.com



DDoS Attacker

Дата: 28.04.2007 **Написал:** zombiexe

релиз **DDoS Attacker** многопоточный, поддержка Socks 4, Socks 5.
Написан на Delphi
Скачать TCP/IP DDoS Attacker
Special for attacking fuc*ing Estonian sites.

Новости команды

Дата: 12.04.2007 **Написал:** zombiexe

1. Craft покинул команду ...
2. Релиз MySQL Bruter - Скачать
3. Идет набор в команду (желающим вступить - связаться со мной по

Обновление FTP-informer

Дата: 18.01.2007 **Написал:** Craft

source: f-secure.com

"at its peak over one million computers were involved"
www.crime-research.org

Case Study Social Aspects

Attackers employed

- simple DoS attacks
- mobilization of activists
- botnet rentals
- flexible communications

Defenders could’ve

- avoided/reduced sentiments
- disrupted mobilization
- employed deception
- built up social capital
- rented anti-botnets
- made botnets not feasible

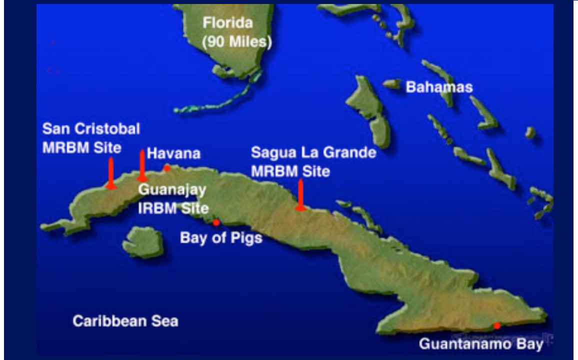
Where to go?

Organizational Processes and Behavior

behavioral school (Simon and March, 1950s)

- individuals and organizations have to rely upon programmed behavior in making decisions

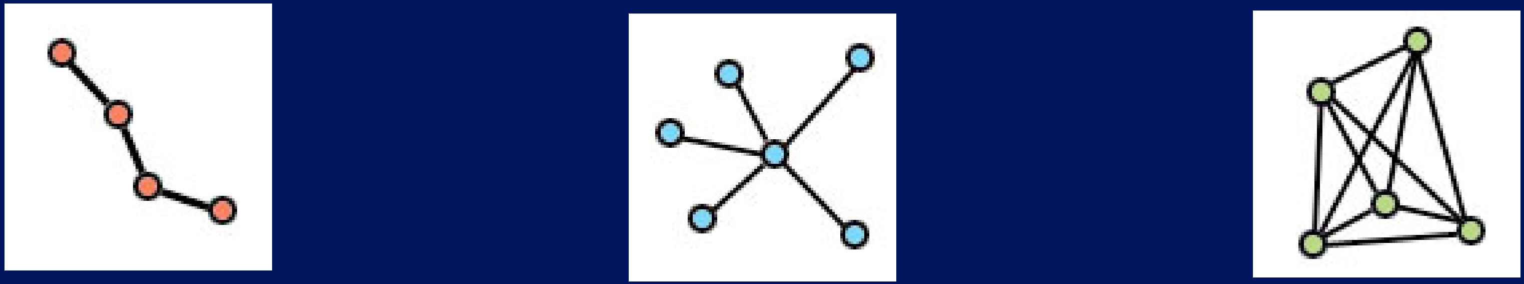
Example: Cuban Missile Crisis



[Meeting of Ex-COMM 18, October, l962.]Source: The National Security Archives. Reprinted with permission.]

Organizational Structure

- Netwar (Arquilla and Ronfeldt, RAND Corporation)
  - organizational purposes affect the suitability and effectiveness of various types of social structures



source: wikipedia.org

- agile networks and virtual organizations
  - flexible internal communication networks
  - strategic connections
  - responding rapidly to external opportunities and challenges
  - rapid information processing
  - quick decision making

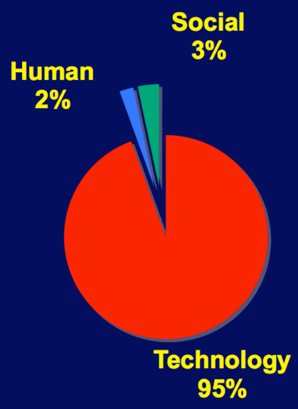
Social Capital

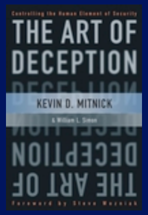
- what is it?
  - social networks and norms of social cooperation
- organizations with higher levels of trust, horizontal cooperation, and loyalty show better performance and efficiency
- ‘modern classic example’
  - difference between Northern (civic) and Southern Italy (parochial) (Putnam 1993)

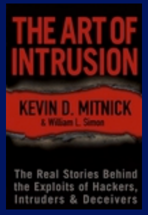
Suggestions for Further Research

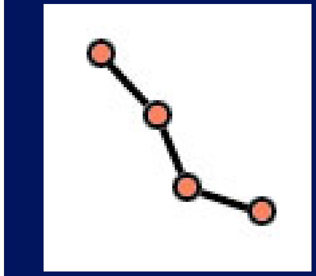
- relationship between organizational processes and behavior and the effectiveness of security defenses
- relationship between organizational structures and security
- models of attackers' organizations
- relationship between organizational cultures, norms, and social capital and the effectiveness of organizational security strategies and programs
- societal aspects of security promotion mechanisms
  - education, awareness building, and policy
  - recycling, seat belt use, as well as drinking and smoking

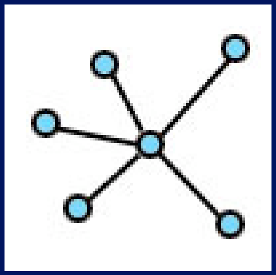
Summary

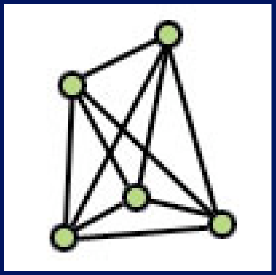


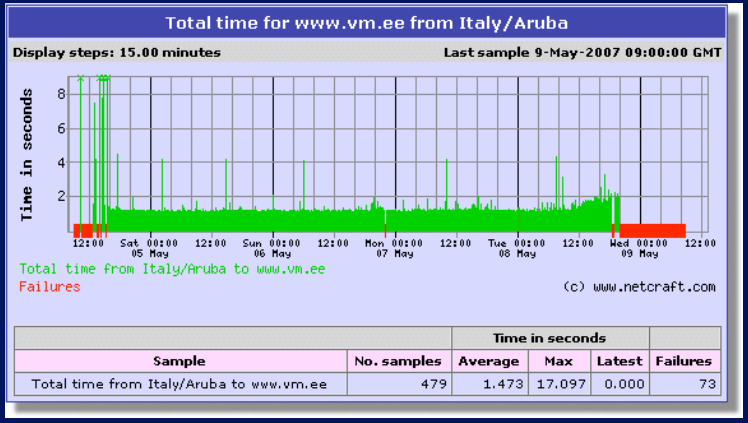



THE ART OF INTRUSION
KEVIN D. MITNICK
The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers









Total time for www.vm.ee from Italy/Aruba

Display steps: 15.00 minutes

Last sample 9-May-2007 09:00:00 GMT

		Time in seconds			
Sample	No. samples	Average	Max	Latest	Failures
Total time from Italy/Aruba to www.vm.ee	479	1.473	17.097	0.000	73

“*people who think their security problem can be solved with only* ***technology*** *do not understand the problem and do not understand the* ***technology***”

(Konstantin Beznosov & Olga Beznosova, 2007)

lersse.ece.ubc.ca

hotadmin.org

ubc.ca