THE AUSTRALIAN NATIONAL UNIVERSITY

Cybercrime and its Future

Regulatory Institutions Network
College of Asia and the Pacific

Cybercrime and its Future

Peter Grabosky
Professor Emeritus
Regulatory Institutions Network
College of Asia and the Pacific
The Australian National University

1. Introduction

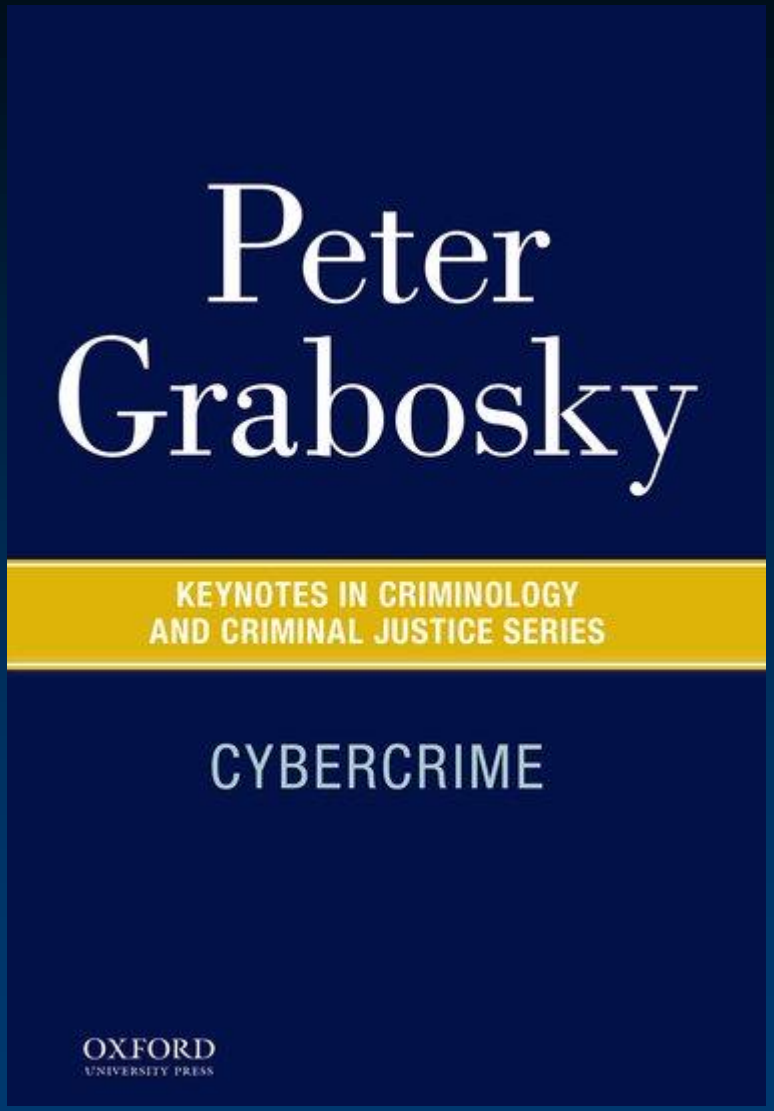
2. Trends in Cybercrime

3. Recent Technological Developments

4. Conclusions

1. Introduction

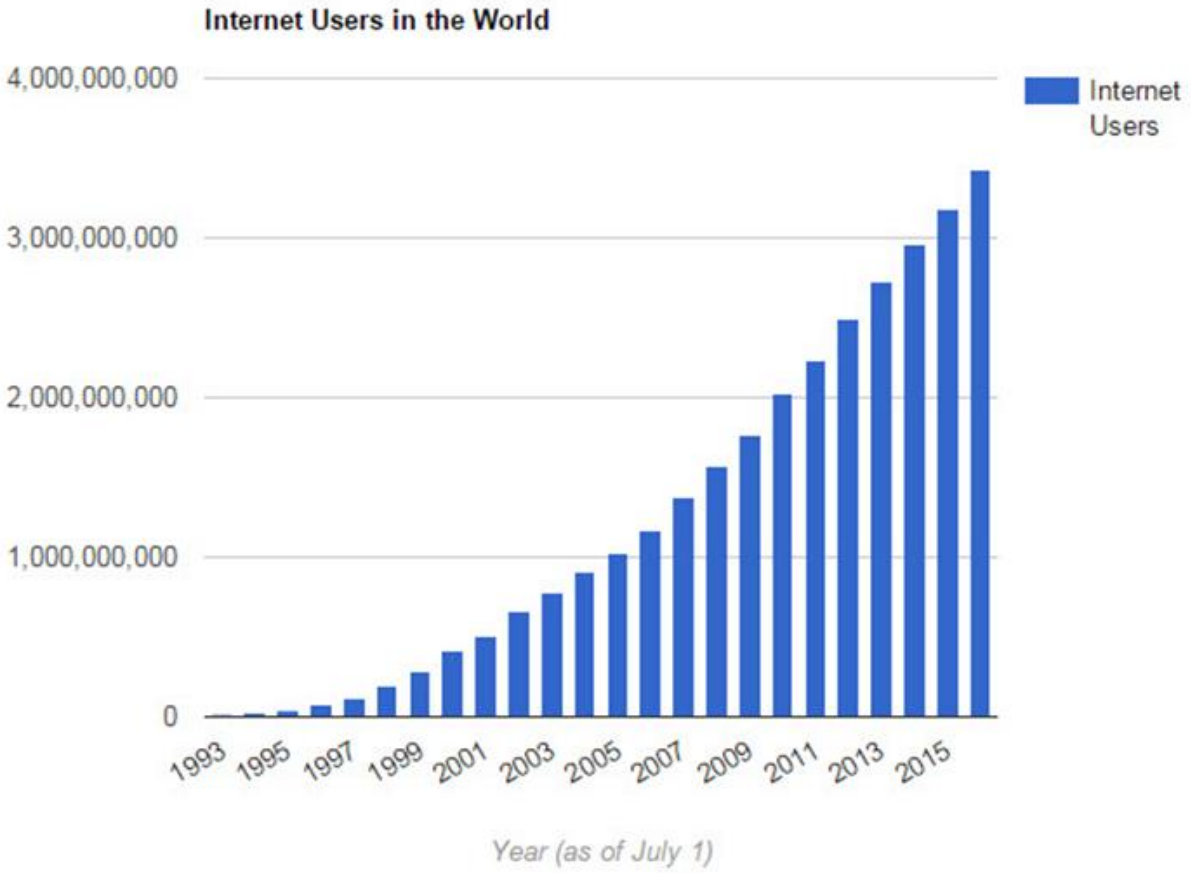
ANU


Peter
Grabosky
KEYNOTES IN CRIMINOLOGY
AND CRIMINAL JUSTICE SERIES
CYBERCRIME
OXFORD
UNIVERSITY PRESS

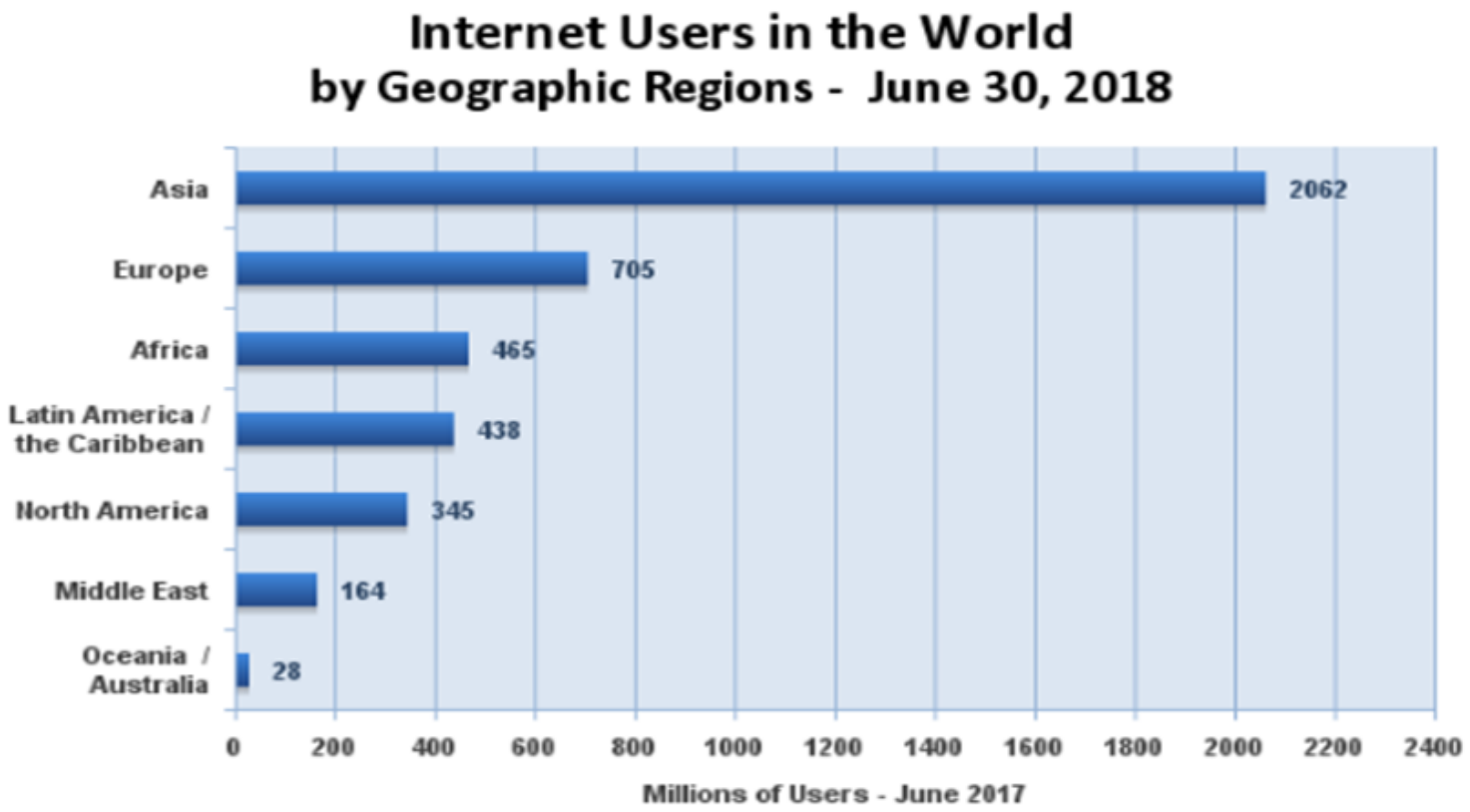
Motives
Opportunities
Guardians

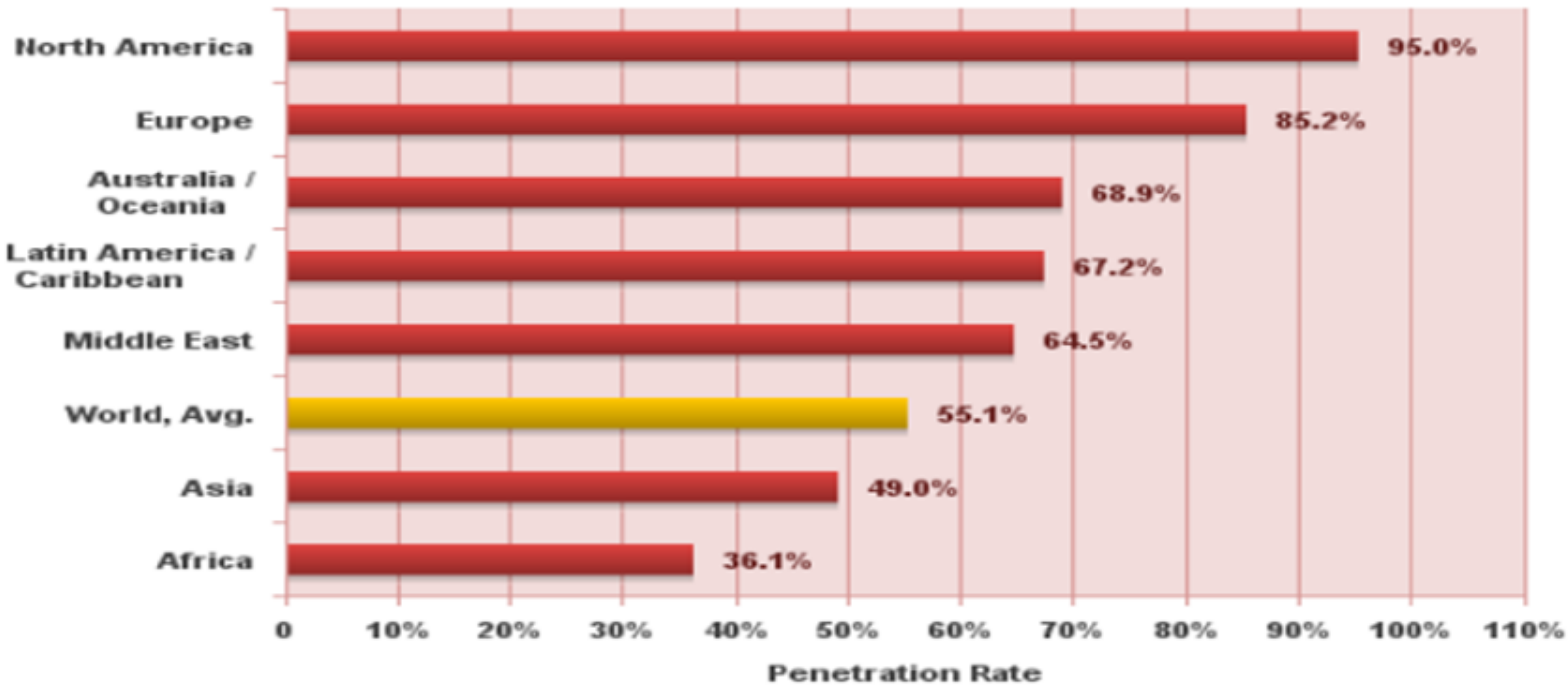
Motives for cybercrime are hardly new:

- Greed
- Lust
- Power
- Revenge
- Curiosity
- Excitement
- Rebellion
- Intellectual Challenge
- Self Defence
- Ideology



Source: Internet Live Stats


Internet Users in the World
by Geographic Regions - June 30, 2018
Asia
2062
Europe
705
Africa
465
Latin America / the Caribbean
438
North America
345
Middle East
164
Oceania / Australia
28
0
200
400
600
800
1000
1200
1400
1600
1800
2000
2200
2400
Millions of Users - June 2017
Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 4,208,571,287 Internet users estimated in June 30, 2018
Copyright © 2018, Miniwatts Marketing Group



Source: Internet World Stats - www.internetworldstats.com/stats.htm
Penetration Rates are based on a world population of 7,634,758,428 and 4,208,571,287 estimated Internet users in June 30, 2018.

Human Guardianship

- Parents
- Teachers
- Systems Administrators
- Individual Users

Technological Guardianship

- Filtering Software
- Anti-Virus Software
- Authentication Technologies
- Credit Card Algorithms

What is Cybercrime?

Regulatory Institutions Network
College of Asia and the Pacific

Unauthorised Access
Interference with Lawful Use
Prohibited Content
Theft/Destruction of Data
Damage to Systems

Regulatory Institutions Network
College of Asia and the Pacific

Unauthorized access (Hacking)


The 50 Most Used Passwords
1. 123456
2. password
3. 12345678
4. qwerty
5. 123456789
6. 12345
7. 1234
8. 111111
9. 1234567
10. dragon
11. 123123
12. baseball
13. abc123
14. football
15. monkey
16. letmein
17. shadow
18. master
19. 696969
20. michael
21. mustang
22. 666666
23. qwertyuiop
24. 123321
25. 1234...890
26. p*s*y
27. superman
28. 270
29. 654321
30. 1qaz2wsx
31. 7777777
32. f*cky*u
33. qazwsx
34. jordan
35. jennifer
36. 123qwe
37. 121212
38. killer
39. trustno1
40. hunter
41. harley
42. zxcvbnm
43. asdfgh
44. buster
45. andrew
46. batman
47. soccer
48. tigger
49. charlie
50. robert

Regulatory Institutions Network
College of Asia and the Pacific

Theft of Information Services

Regulatory Institutions Network
College of Asia and the Pacific

Identity Theft

Regulatory Institutions Network
College of Asia and the Pacific

Information Piracy
Counterfeiting
Forgery


Pappy Van Winkle's
Family Reserve
20 years old
FAKE

Regulatory Institutions Network
College of Asia and the Pacific


西安市公安局集中销毁淫秽制品现场会
XGMA

Possession/Dissemination of Offensive Materials


CHINA : FREE FALUN GONG
PRACTITIONERS NOW
立刻停止殘殺迫害法輪功學員
法輪大法好
法 輪 大 法
FALUN DAFA
眞 善 忍
Truthfulness Compassion

Regulatory Institutions Network
College of Asia and the Pacific

Online Child Exploitation

Regulatory Institutions Network
College of Asia and the Pacific

Stalking & Bullying

Regulatory Institutions Network
College of Asia and the Pacific

Extortion

1. Communicate a threat
2. Target computer systems
3. Medium of blackmail
4. Digital payment
5. Intelligence about victims

Regulatory Institutions Network
College of Asia and the Pacific

Electronic Funds Transfer Fraud

2016 Theft of **US$81,000,000**

Bangladeshi funds deposited in US Federal Reserve system

Regulatory Institutions Network
College of Asia and the Pacific

Electronic Money Laundering

Philippines

Bank secrecy laws-strong

Cash transaction reporting-weak
Casinos *exempt* !!

Regulatory Institutions Network
College of Asia and the Pacific

Advance Fee Fraud

WESTERN UNION

moving money for better®

Dear Email Beneficiary,

We wish to inform you that you are one of the seven email beneficiaries approved to receive the sum of $1,500,000.00 USD in the on-going UN Humanitarian aid / Poverty Alleviation Program (UNPAP) 2016.

The United Nation's Organisation has deposited your funds with us at the Western Union Payout Center in Malaysia ,and they have contracted us to take full responsibility in the transfer process of the funds to all seven beneficiaries. They have now ordered us to take full responsibility in the transfer process of your funds and thus commence the immediate remittance of your funds to you. Be strongly informed that because of our Western Union transfer policy, your funds will be paid to you via our Western Union Daily Transfer limit of $7,600USD. This means that you will continuously receive a daily amount of $7,600USD USD from us, and this amount can be collected from any of our numerous Western Union outlets in your current location.

To begin receiving your daily payment as stated above, we need you to provide us with; Your Full Name, Address, and Phone Number. Upon receipt of the requested details.

Your first transaction will be activated and we shall then proceed to provide you with the Money Transfer Control Number (MTCN) for the first installment, and we will continue to email you others after 24 hours of receiving each payment.

For more information on your payment status: Call Tony Yung on our 24 hours phone helpline @ +601-02484297 and reply to this message via: wumtaccess09@my.com for inquiries on this message.

Yours truly,
Western Union Malaysia

APPROVED

Regulatory Institutions Network
College of Asia and the Pacific

Romance Fraud

Gavin kkariper@konya.edu.tr

My name is Gavin. I'm 45 years old, from the US. I'm in Syria right now fighting IS. I want to get to know you better, if I may be so bold. I consider myself an easy-going man, and I am currently looking for a relationship in which I feel loved. Please tell me more about yourself, if you don't mind.

Regulatory Institutions Network
College of Asia and the Pacific

Sales and Investment Fraud

Business Interest

William Leung kchengc@cuhk.edu.hk

I have a business for you worth 24.5m usd, reply (willieleu2@gmail.com) for more details.

Regulatory Institutions Network
College of Asia and the Pacific

Ransomware Fraud
(Fraud+Extortion)


NSA INTERNET SURVEILANCE PROGRAM
PRISM
COMPUTER CRIME PROSECUTION SECTION
POLICE
YOUR COMPUTER HAS BEEN LOCKED!
Your computer has been locked due to suspicion of illegal content downloading and distribution.
The illegal content (414 Mb of photo and video files) was automatically classified as child pornographic materials.
The downloading and ditribution of illigal content, in whole or in part, violate following U.S. Federal Laws:
18 U.S.C. § 2251 Sexual exploitation of children (Production of child pornography)
18 U.S.C. § 2252 Ceratin activities relating to material involving the sexual explotation of minors (Possession, distribution and receipt of child pornography)
18 U.S.C. § 2252A Ceratin activites relating to material constituing or containing child pornography
Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 6 month to 10 years and shall be fined up to $250,000.
Collected technical data
Your IP address:
Your host name:
Source or intermediary sites:
Location:
Illegal content found:
ALL SUSPICIOUS FILES FROM YOUR COMPUTER WERE TRANSMITTED TO A SPECIAL SERVER AND SHALL BE USED AS EVIDENCES. DON'T TRY TO CORRUPT ANY DATA OR UNBLOCK YOUR COMPUTER IN AN UNAUTHORIZED WAY.
Your case can be classified as occasional/unmotivated, according to 17 (U.S. Code) §512
Thus it may be closed without prosecution.
Your computer will be unblocked automatically.
In order to resolve the situation in an above-mentioned way you should pay a fine of $300
green dot MoneyPak
Exchange your cash for a MoneyPak voucher and use your voucher code in the form below:
Code:
1 2 3 4 5 6 7 8 9 0
SUBMIT
Status: Waiting for payment
Permanent lock on 09/28/2013 8:46 p.m. EST
Where can I buy MoneyPak
RITE AID PHARMACY
CVS pharmacy
kmart
7 ELEVEN
Walgreens
Walmart

AFP
AUSTRALIAN FEDERAL POLICE

The Australian Federal Police is a progressive and multi-faceted law enforcement organisation taking a strong lead in the fight against 21st century crime.

You've received a subpoena

You are invited to the law court by the judge because of crime commitment.

Case: #256101
Date: 01/03/2016

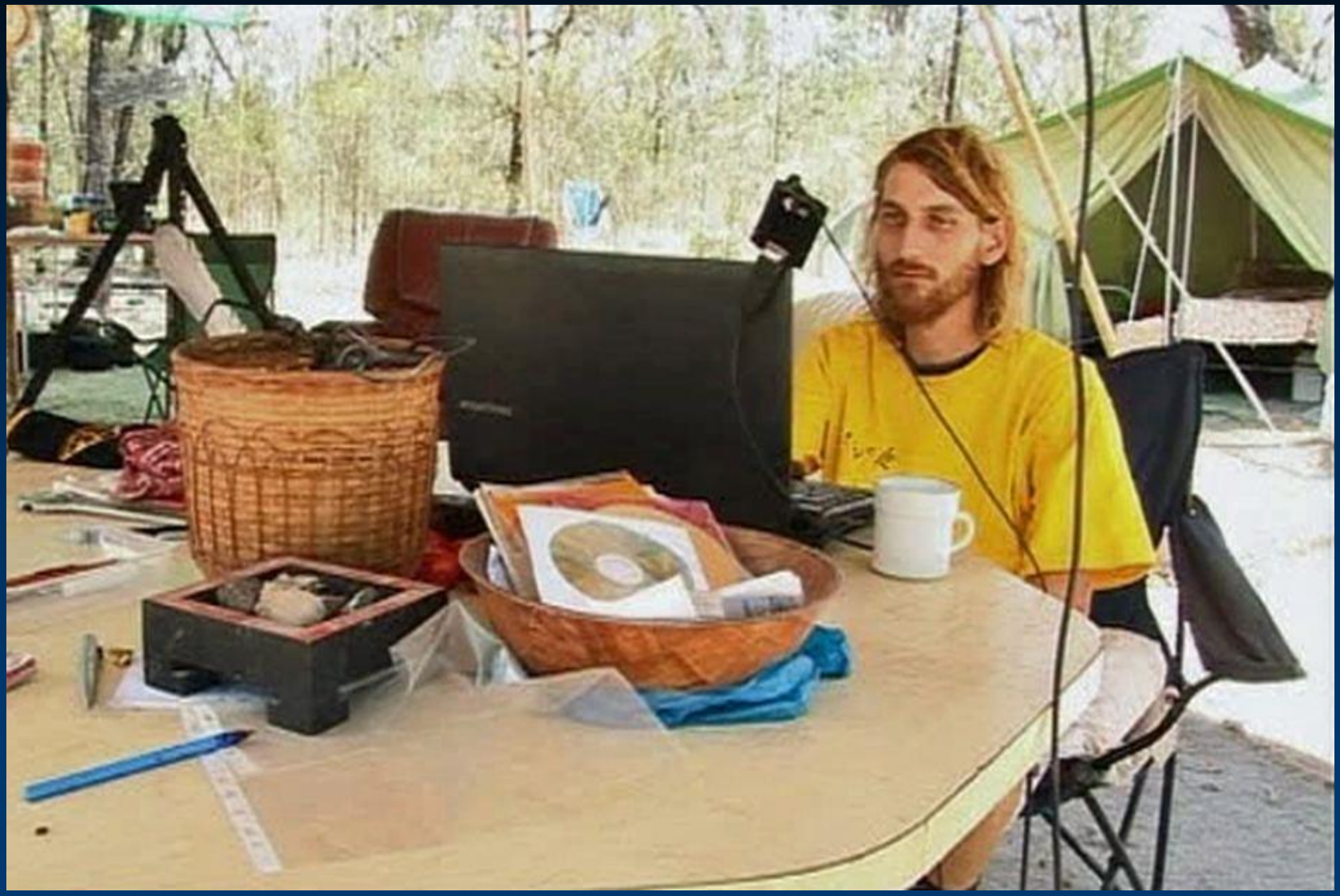
Please visit nearest police office or view case notices.

Down load case info

You must provide all the necessary information to the Court within 15 days, starting from the time at which this message was received. If the information is not provided, the court can take place without your participation.

Regulatory Institutions Network
College of Asia and the Pacific

Financial Hoaxes



Regulatory Institutions Network
College of Asia and the Pacific

Illegal Interception or Disclosure of Information

Regulatory Institutions Network
College of Asia and the Pacific

Regulatory Institutions Network
College of Asia and the Pacific

Communications in Furtherance of Criminal Conspiracies

Regulatory Institutions Network
College of Asia and the Pacific

Electronic Vandalism & Terrorism

Cyber Warfare

What's New?

Greater diversity of activity within these generic crime types

Greater diversity of targets and attack vectors

2. Trends

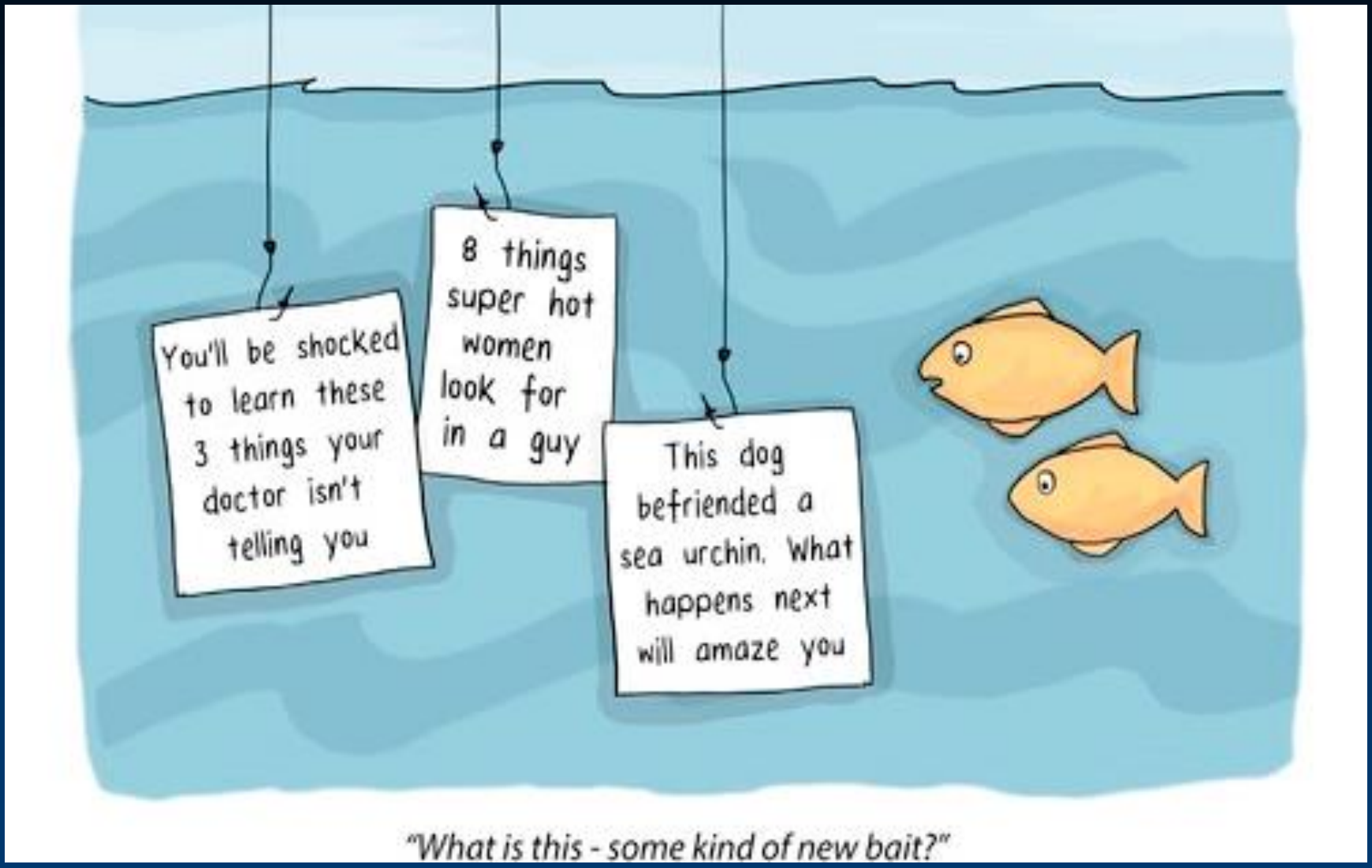
What's New?

Sophisticated
Commercialized
Diversity of Organizational Form

State and State-Sponsored

Sophistication:

More skillful exploitation of trust



"What is this - some kind of new bait?"

More skillful exploitation of trust

Bigger, Better Botnets

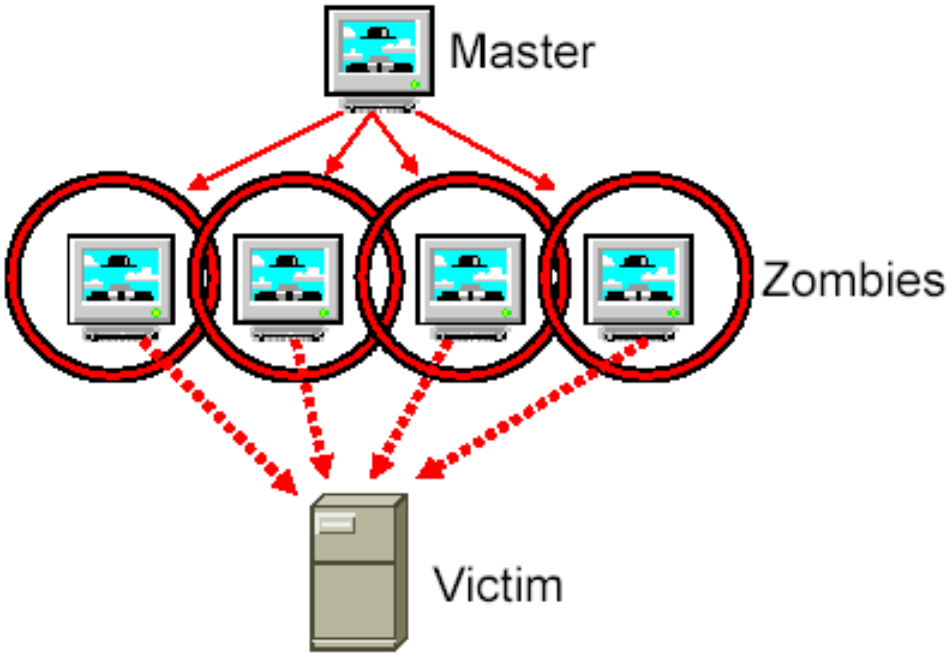


Figure 1-1: DDOS attack architecture

More skillful exploitation of trust

Bigger, Better Botnets

Greatly Improved Malware

More skillful exploitation of trust

Bigger, Better Botnets

Greatly Improved Malware

Crime on a Much Larger Scale

Regulatory Institutions Network
College of Asia and the Pacific

Skillful use of digital technology by terrorist groups and by organized criminal groups

Islamic State (*Wired*, April 2016); Zetas

Regulatory Institutions Network
College of Asia and the Pacific

Recruitment
Propaganda
Fundraising
Tactical Communications


U.S. Central Command
@CENTCOM
Following
In the name of Allah, the Most Gracious, the Most Merciful,
the CyberCaliphate continues its CyberJihad.
Army General Officer
Public Roster (By Rank)
2 January 2014

"Los Zetas are deploying their own teams of computer experts to track those individuals involved in the online anti-cartel campaign…"

(Stratfor 2011)

Regulatory Institutions Network
College of Asia and the Pacific

Offensive countermeasures

Cyber-operations
Psychological warfare


لا إله إلا
الله
رسول
محمد

Regulatory Institutions Network
College of Asia and the Pacific

Commercialization:

Regulatory Institutions Network
College of Asia and the Pacific

Hackers for Hire

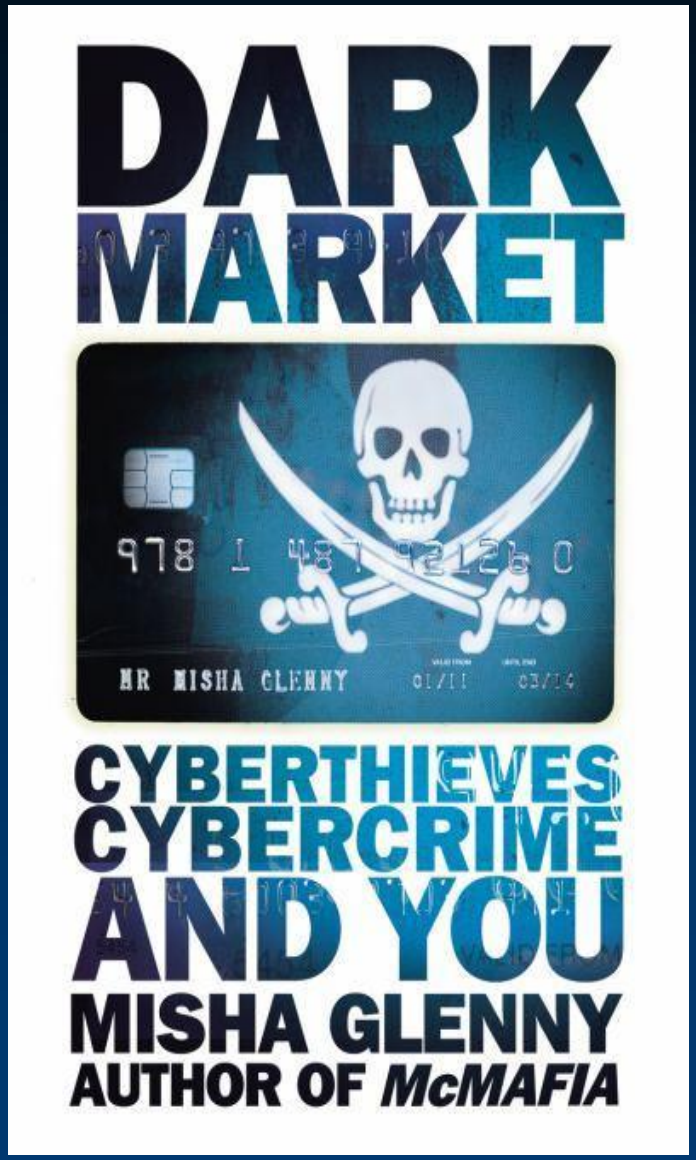
Regulatory Institutions Network
College of Asia and the Pacific

Hackers for Hire
Botnets for Rent

Regulatory Institutions Network
College of Asia and the Pacific

Hackers for Hire
Botnets for Rent
Malware Bazaars

Regulatory Institutions Network
College of Asia and the Pacific



Regulatory Institutions Network
College of Asia and the Pacific

Hackers for Hire
Botnets for Rent
Malware Bazaars
DDoS Services

Regulatory Institutions Network
College of Asia and the Pacific

Updates and User Support for Exploit kits

Regulatory Institutions Network
College of Asia and the Pacific

Updates and User Support for Exploit Kits

Markets for Undiscovered Flaws in Computer Code (Zero Day Exploits)

Regulatory Institutions Network
College of Asia and the Pacific

Diversity of Organizational Structures:

Regulatory Institutions Network
College of Asia and the Pacific

State and State-sponsored Cybercrime

Regulatory Institutions Network
College of Asia and the Pacific

Offensive Cyber Operations State, or State-Sponsored

Espionage
Sabotage
Disruption

School of Regulation and Global Governance (RegNet)
College of Asia and the Pacific

Estonia/Ukraine/Georgia/USA (Russia)
2007 2008 2015 2016

Stuxnet (USA + Israel) 2010

Saudi Aramco (Iran) 2012

Industrial/Economic Espionage (China) 2013

Sony Pictures (DPRK) 2014

Bangladesh Central Bank (DPRK) 2016

Wannacry (DPRK) 2016

North Korean Missile Tests (USA) 2017

Regulatory Institutions Network
College of Asia and the Pacific

"Stuxnet"

Stunning complexity and sophistication

Using 4 "zero day" exploits

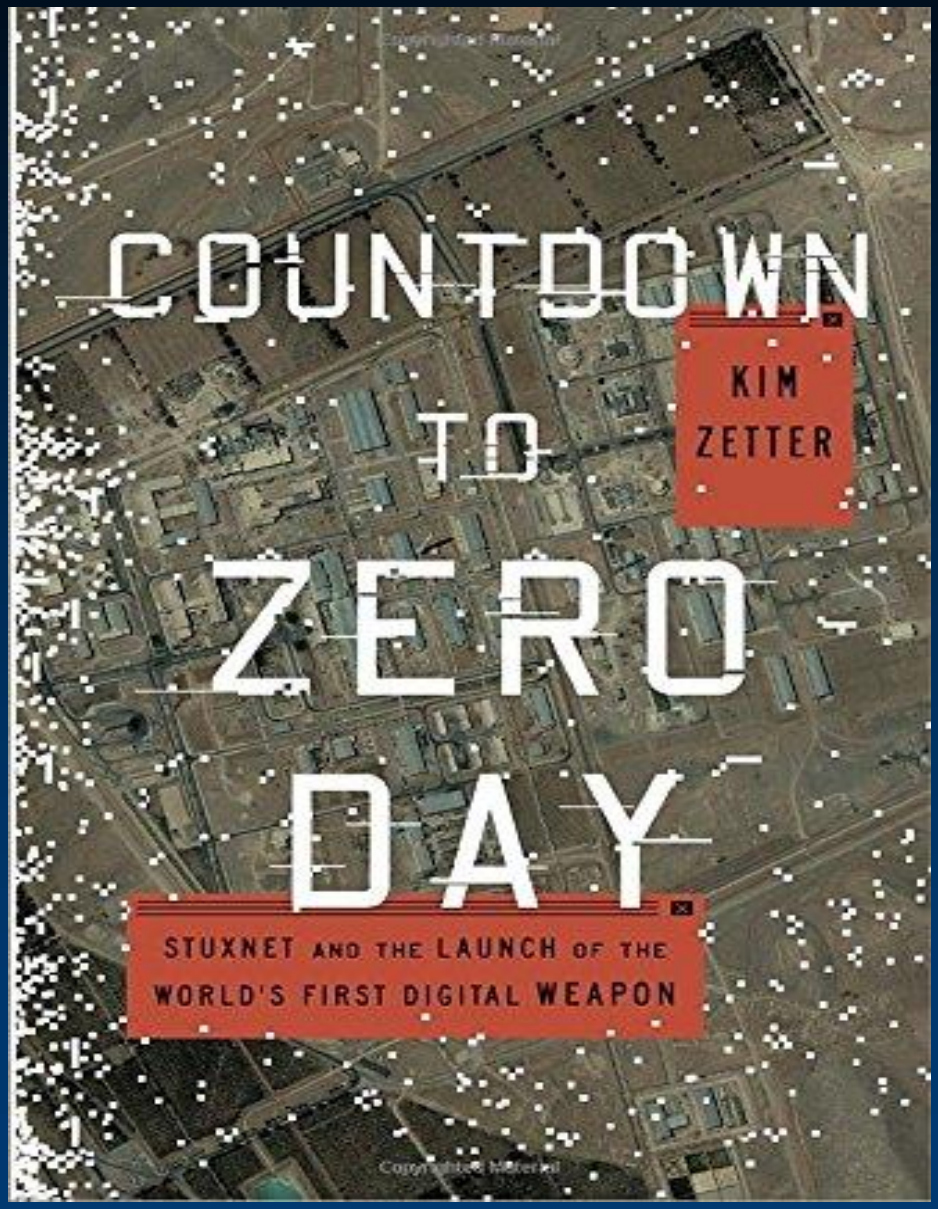
Commandeered industrial control system while hiding the fact

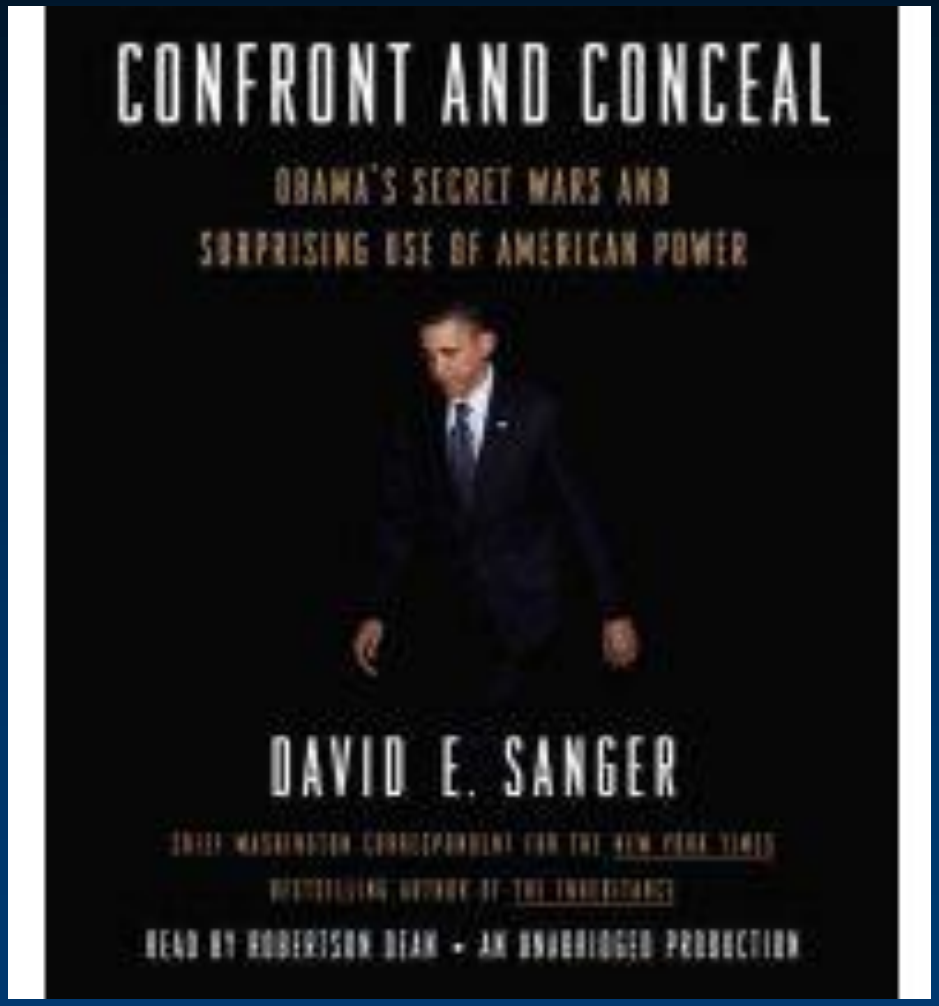
Disabled alarms while signalling that systems were operating normally.

A "game changer" in cyber security

ANU

Regulatory Institutions Network
College of Asia and the Pacific




CONFRONT AND CONCEAL
OBAMA'S SECRET WARS AND
SURPRISING USE OF AMERICAN POWER
DAVID E. SANGER
READ BY ROBERTSON DEAN • AN UNABRIDGED PRODUCTION

Regulatory Institutions Network
College of Asia and the Pacific

Regulatory Institutions Network
College of Asia and the Pacific

Regulatory Institutions Network
College of Asia and the Pacific

PLA Unit 61398

(APT 1)

APT1

Exposing One of China's Cyber Espionage Units

Regulatory Institutions Network
College of Asia and the Pacific

Regulatory Institutions Network
College of Asia and the Pacific

Regulatory Institutions Network
College of Asia and the Pacific

Regulatory Institutions Network
College of Asia and the Pacific

Regulatory Institutions Network
College of Asia and the Pacific

ANU

Regulatory Institutions Network
College of Asia and the Pacific

Regulatory Institutions Network
College of Asia and the Pacific

State- “Sponsored”:

Russian Hackers

1. Attack anything you like, as long as it is outside of Russia

2. If you encounter information that may be useful to the Russian State, please let us know.

3. When patriotic duty beckons, please heed the call.

Plausible Deniability

China
Estonia
Georgia
India
Iran
Saudi Arabia
South Korea
United States

Regulatory Institutions Network
College of Asia and the Pacific

United States of America

vs

Ahmed Fathi et al

https://www.justice.gov/opa/file/834996/download

Regulatory Institutions Network
College of Asia and the Pacific

State Ignorance
State Incapacity
“Blind Eye”
Tacit Encouragement
Active Sponsorship
Formal Collaboration
State Monopoly

4. Recent Technological Developments

Regulatory Institutions Network
College of Asia and the Pacific

Mobile Telephony
Wireless Internet
Cloud Computing
Voice-over Internet Protocol
Social Media

Further into the future:

"The Internet of Things"

Interconnectivity

50 Billion interconnected devices worldwide by 2020

Remote car hijacking

https://www.youtube.com/watch?v=MK0SrxBC1xs

Regulatory Institutions Network
College of Asia and the Pacific

Vulnerability of Weapons Systems

Regulatory Institutions Network
College of Asia and the Pacific

US Government Accountability Office

WEAPON SYSTEMS CYBERSECURITY:

DOD Just Beginning to Grapple with Scale of Vulnerabilities

GAO-19-128: Published: Oct 9, 2018.
Publicly Released: Oct 9, 2018.

https://www.gao.gov/products/GAO-19-128

“Big Data”

a tool for criminals

Further into the future:

“The Internet of Things”

Brain-machine Technology

Regulatory Institutions Network
College of Asia and the Pacific

Continued on Page 29, Column 2 Continued on Page 8, Column 4

'Matador' With a Radio Stops Wired Bull

Modified Behavior in Animals Subject of Brain Study

By JOHN A. OSMUNDSEN

Afternoon sunlight poured over the high wooden barriers into the ring as the brave bull bore down on the unarmed "matador" — a scientist who had never faced a fighting bull.

But the charging animal's horns never reached the man behind the heavy red cape. Moments before that could happen, Dr. José M. R. Delgado, the scientist, pressed a button on a small radio transmitter in his hand, and the bull braked to a halt.

Then, he pressed another button on the transmitter and the bull obediently turned to the right and trotted away.

The bull was obeying commands from his brain that had been called forth by electrical stimulation—by the radio signals—of certain regions in which fine wire electrodes had been painlessly implanted the day before.

The experiment, conducted last year in Cordova, Spain, by Dr. Delgado of Yale University's School of Medicine, was probably the most spectacular demonstration ever performed of the deliberate modification of animal behavior through external control of the brain.

Dr. Delgado was trying to find out what makes brave bulls brave — just as other of his experiments have aimed at finding the biological basis for emotions, personality and behavior in man and other animals through electrical stimulation of their brains.

Dr. José M. R. Delgado of Yale University's School of Medicine facing a charging bull

Bull, halted in mid-charge by command from Dr. Delgado's transmitter, raises dust cloud

He has been working in this field for more than 15 years. Techniques that he and other scientists have recently developed have been refined to the point where, he believes, "a turning point has been reached in the study of the mind."

"I do believe," he said in a recent lecture, "that an understanding of the biological bases of social and antisocial behavior and of mental activities, which for the first time in history can now be explored in a conscious brain, may be of decisive importance in the search for intelligent solutions to some of our present anxieties, frustrations and conflicts."

Dr. Delgado said in an interview recently that he was particularly concerned with what he called the "gap between our understanding of the atom and

Continued on Page 20, Column 3

Regulatory Institutions Network
College of Asia and the Pacific

Regulatory Institutions Network
College of Asia and the Pacific

Further into the future:

“The Internet of Things”

Brain-machine Technology

Brain-to-Brain Technology

Regulatory Institutions Network
College of Asia and the Pacific

5. Conclusions

Crime Follows Opportunity

Every New Technology
Every New Application

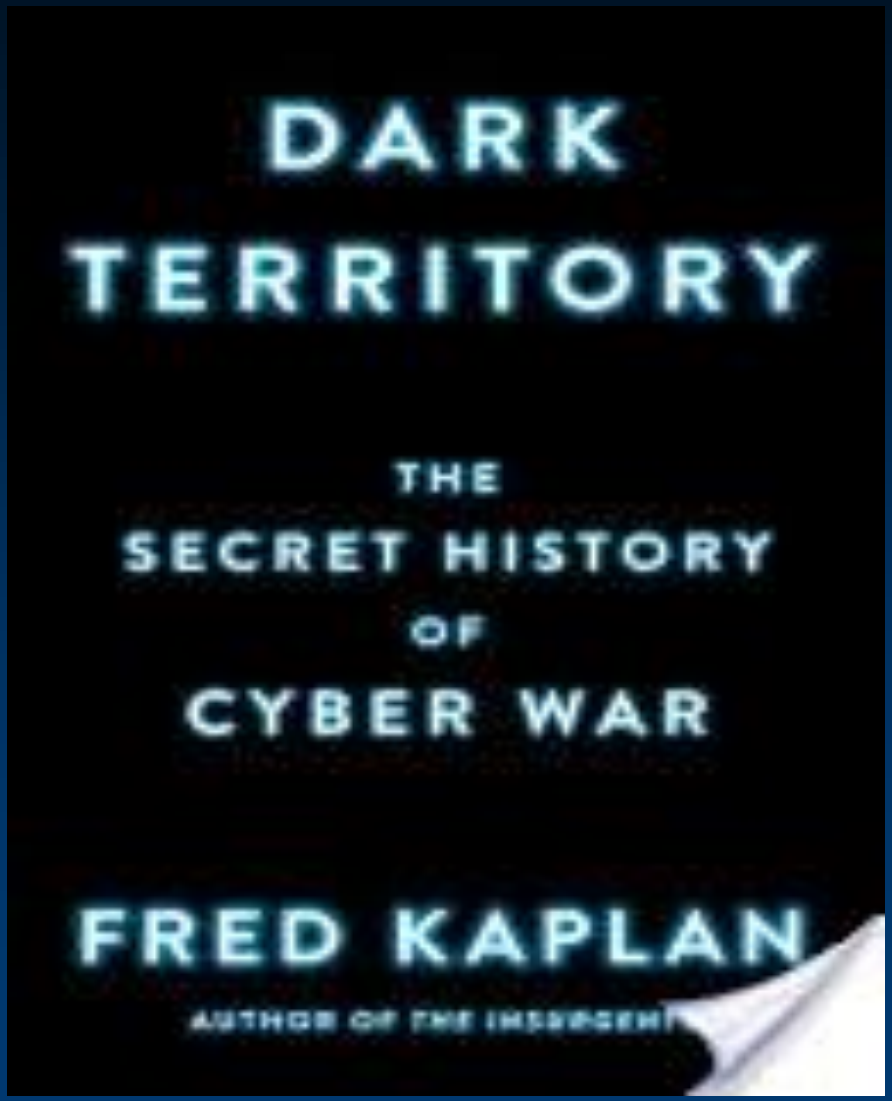
is vulnerable to criminal exploitation

It is theoretically possible for someone with just a laptop to:

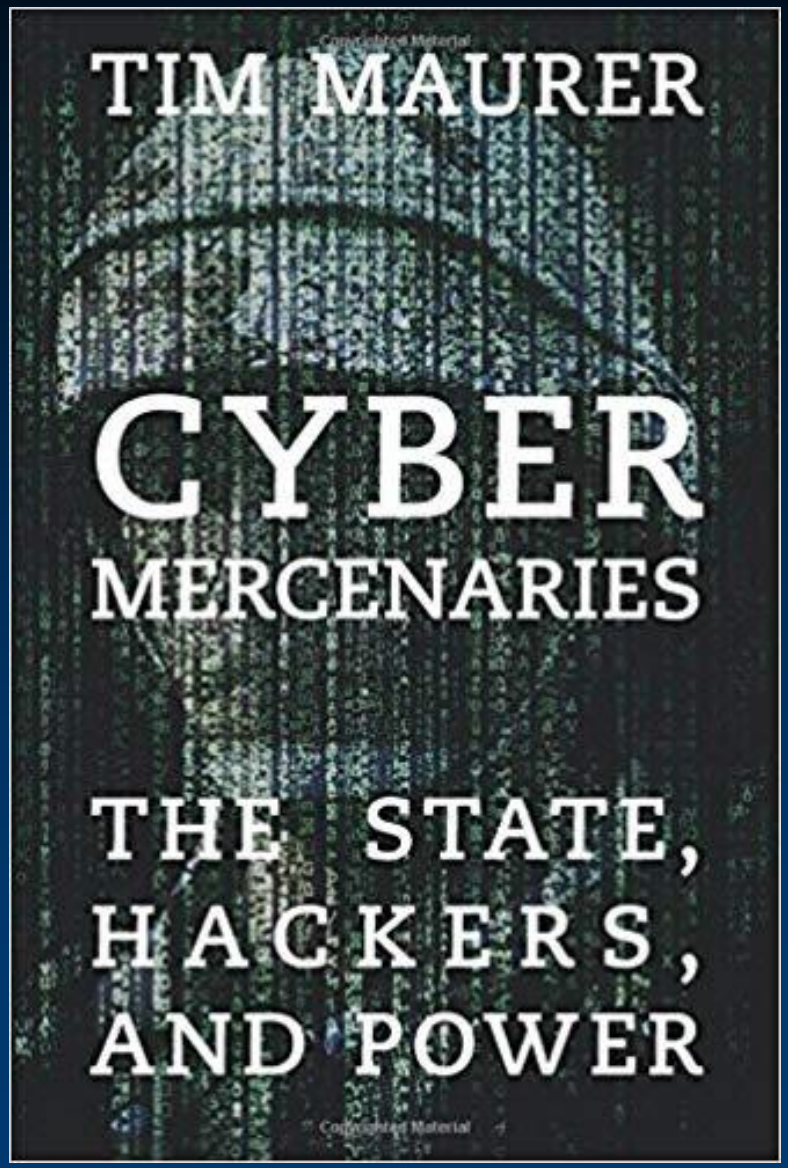
- Commandeer an aircraft
- Put a virus into flight control computers
- Jeopardize the safety of the flight by taking control of computers
- Take over the warning systems or even navigation systems

US Government Accountability Office 2015

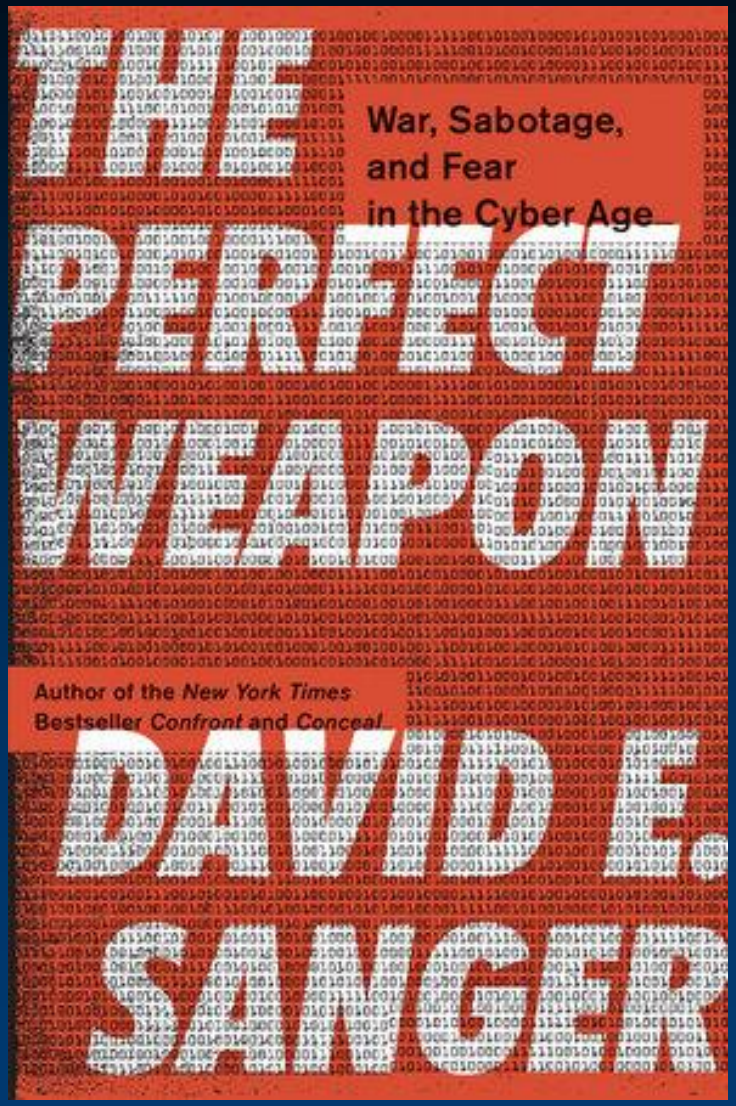
Regulatory Institutions Network
College of Asia and the Pacific


DARK
TERRITORY
THE
SECRET HISTORY
OF
CYBER WAR
FRED KAPLAN

School of Regulation and Global Governance (RegNet)
College of Asia and the Pacific



School of Regulation and Global Governance (RegNet)
College of Asia and the Pacific



Solutions:

Regulatory Institutions Network
College of Asia and the Pacific

How best to achieve security and prosperity in Cyberspace?

Security Consciousness

Regulatory Institutions Network
College of Asia and the Pacific

Security Consciousness Resources

Regulatory Institutions Network
College of Asia and the Pacific

Security Consciousness
Resources
International Co-operation

Security Consciousness
Resources
International Co-operation
Substantive Criminal law

Security Consciousness
Resources
International Co-operation
Substantive Criminal law
Laws of Criminal Procedure and Evidence

Budapest Convention

https://www.coe.int/en/web/cybercrime/the-budapest-convention

Regulatory Institutions Network
College of Asia and the Pacific

Successful models of Co-operation

Regulatory Institutions Network
College of Asia and the Pacific

China-Taiwan Fraud Investigation (2012)

Regulatory Institutions Network
College of Asia and the Pacific

Silk Road 2.0 Takedown (2014)

Bulgaria, Czech Republic, Finland, France, Germany, Hungary, Ireland, Latvia, Lithuania, Luxembourg, Netherlands, Romania, Spain, Sweden, Switzerland, United Kingdom, United States

Regulatory Institutions Network
College of Asia and the Pacific

Pluralistic Cybersecurity

Governments
Private Industry
Civil Society

(Better communication within and between these sectors)

More Secure Software

More training and education police; prosecutors; judges; citizens

More international cooperation

- Harmonization of laws (substantive criminal law; criminal procedure laws)
- Cross-border investigations
- Bridging the digital divide

Santayana (1863-1952):

Those who forget the past are condemned to repeat it.

Those who fail to anticipate the future are in for a rude shock when it arrives.

Regulatory Institutions Network
College of Asia and the Pacific

Thank You !

Regulatory Institutions Network
College of Asia and the Pacific

Peter.Grabosky@anu.edu.au

http://Regnet.anu.edu.au