Cybersecurity

Beirut, August 2016

Marilia Maciel

Digital Policy Senior Researcher

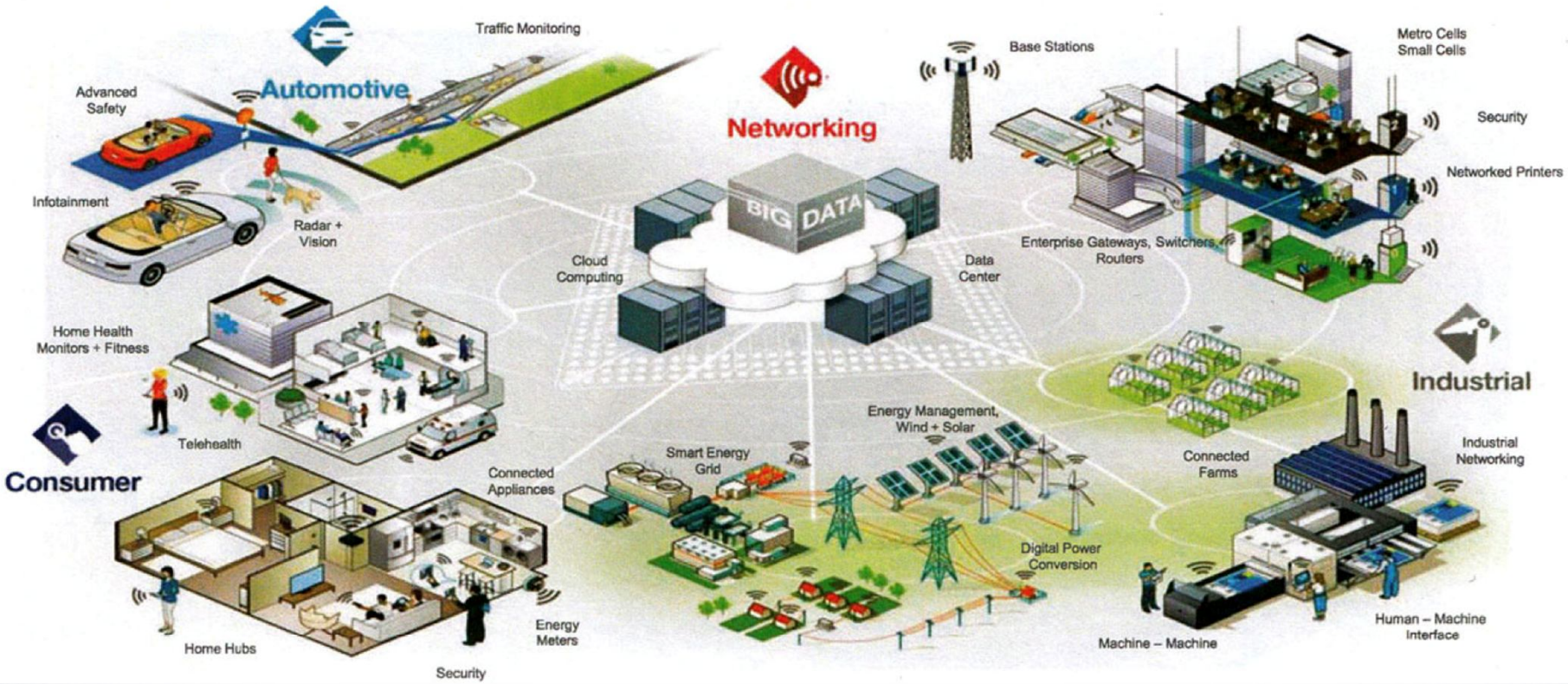
mariliam@diplomacy.edu

DiPLO

www.diplomacy.edu

DiPLO
www.diplomacy.edu

The Internet of Things



There can be
no security
where there
is fear.

Felix Frankfurter

meetville.com

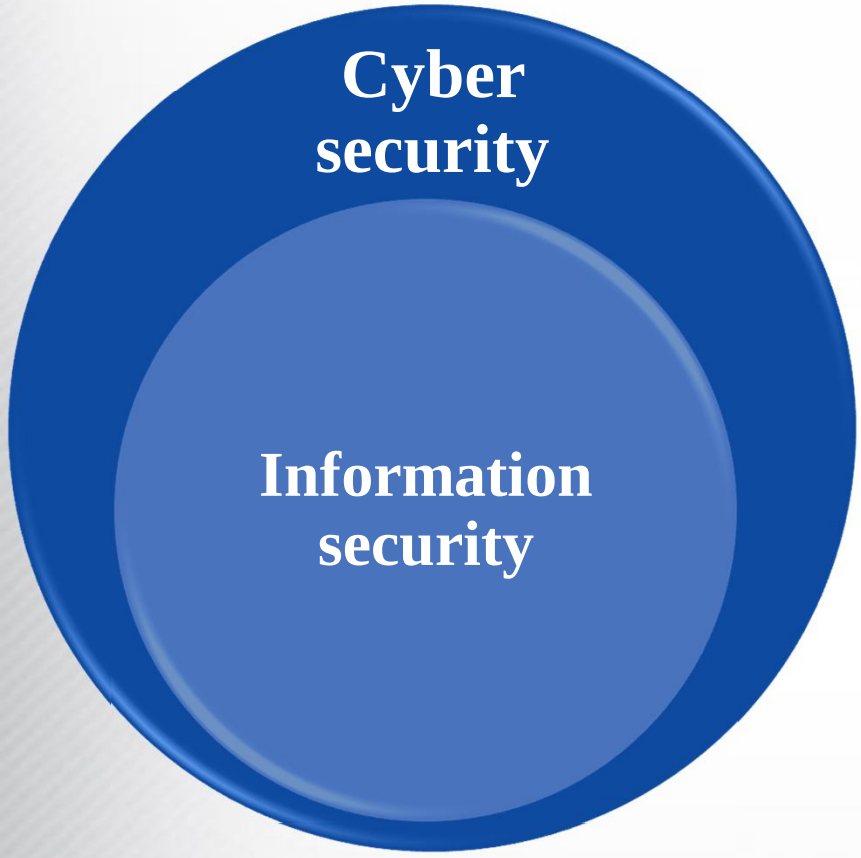
DiPLO
www.diplomacy.edu

Definition?

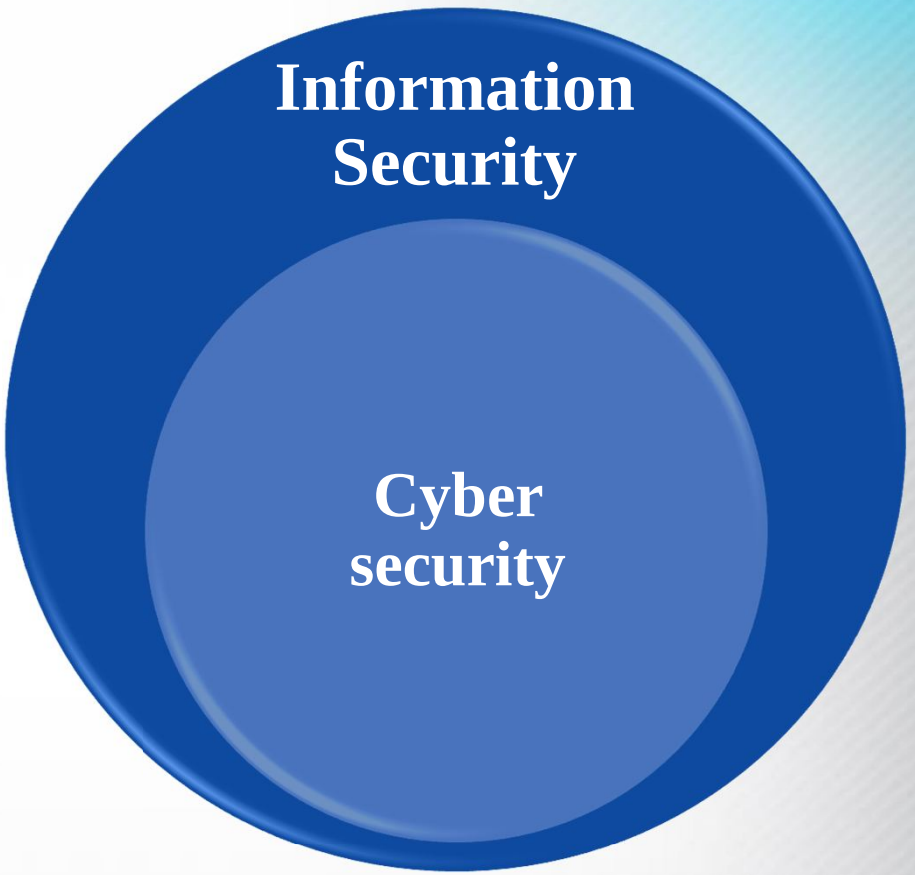
More than 900

What's your name?

- Information security
- Cyber-security
- Network security
- Data security
- Computer security



US and Euro-Atlantic Approach



Chinese-Russian Approach

Definitions?

Information security is ‘protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction’ in order to provide integrity, confidentiality, and availability
(USA Legal Information Institute, no date)

Cyber-security commonly refers to the **safeguards and actions that can be used to protect the cyber domain**, both in the **civilian and military** fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure.
(EU Cybersecurity Strategy 2013)

Theory

Confidentiality (unauthorised disclosure)

Integrity (unauthorised change)

Availability (measured)

DiPLO
www.diplomacy.edu

Vocabulary

- Adware
- Backdoor
- (Boot) virus
- Brute force, Dictionary attack
- Bot, Botnet, Sheppard, Zombie cp
- Cyberstalking
- Hacking, Cracking, Hactivism
- DDoS attack
- Defacing
- Exploit
- Jamming
- Money Mule
- Man-in-the-middle attack
- Grooming
- Information Warfare

Nigerian scam (adv. Fee)
(Packet) Sniffer, key logger
Pharming
Phishing
Ransom ware
Rootkit
Skimming
Spoofing
Smishing
Stepping Stone Attack
Trojan Horse
Typo Squatting
War dialing/driving
Worm

Complexity

Mapping the field

- Critical (information) infrastructure protection – C(I)IP
- Cybercrime
- Cyberconflicts

“Enemies”

Perpetrators

The enemy: state/non-state actors

Activists
Criminals
Separatists
Anarchists
Hacktivists
Revolutionaries
Terrorists
State sponsored

[redacted]

Cyber attack

Cyber attack concurrent with physical attack

Provided by Ed Gelbstein

DiPLO
www.diplomacy.edu

Motives

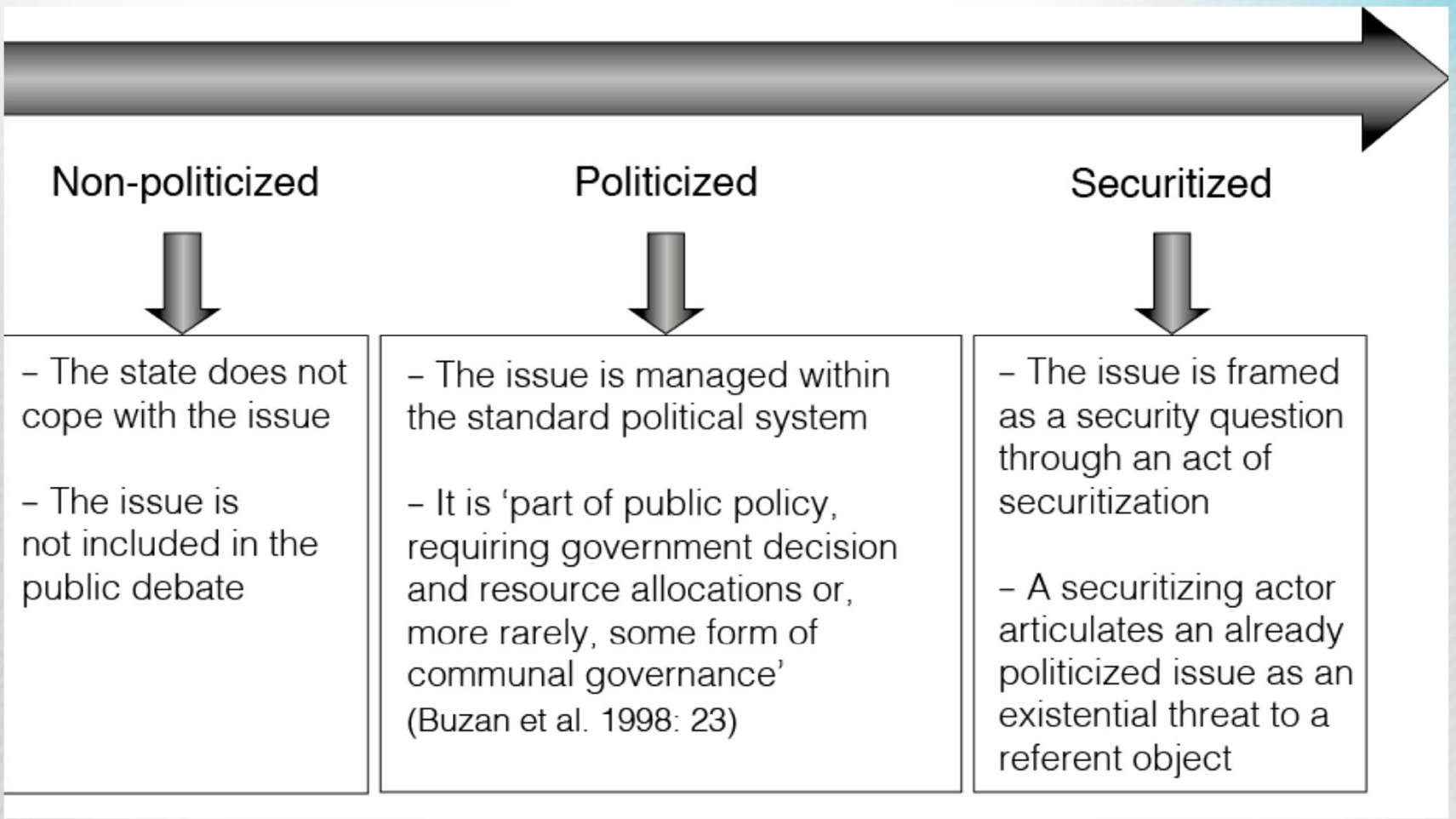
- Hacktivism
- Crime
- Espionage
- Terrorism
- Warfare

DiPLO
www.diplomacy.edu

Targets

- individuals (ID, zombies)
- business (SMEs, banks)
- civil society and NGOs (especially political activists)
- government (e-gov, databases)
- public institutions (databases)
- core Internet infrastructure (ISPs, IXPs, fusion centers, data centers)
- critical society infrastructure (power/industry facilities, traffic, …)
- military assets

Attention: Securitization



“Weapons”

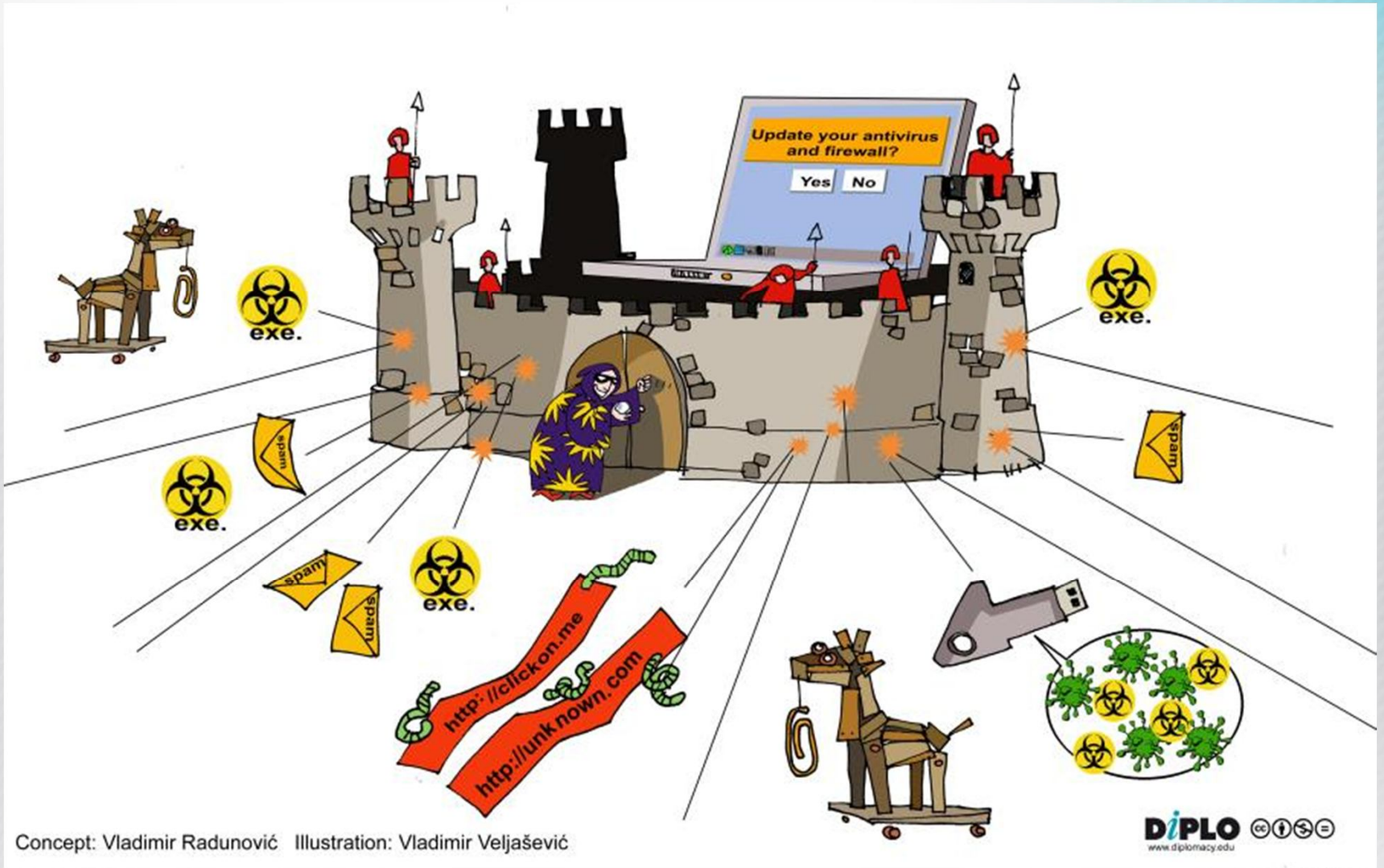
Main threats

- social engineering (phishing, scams)
- malware (viruses, warms, Trojans)
- botnets
- misconfigured open infrastructure
- data inspection
- IP spoofing
- data interception
- data interference
- illegal access
- malware distribution
- phishing and e-scams
- identity theft
- copyright and IPR theft
- DDoS attacks
- espionage (industrial, intelligence)

Weapons and tools

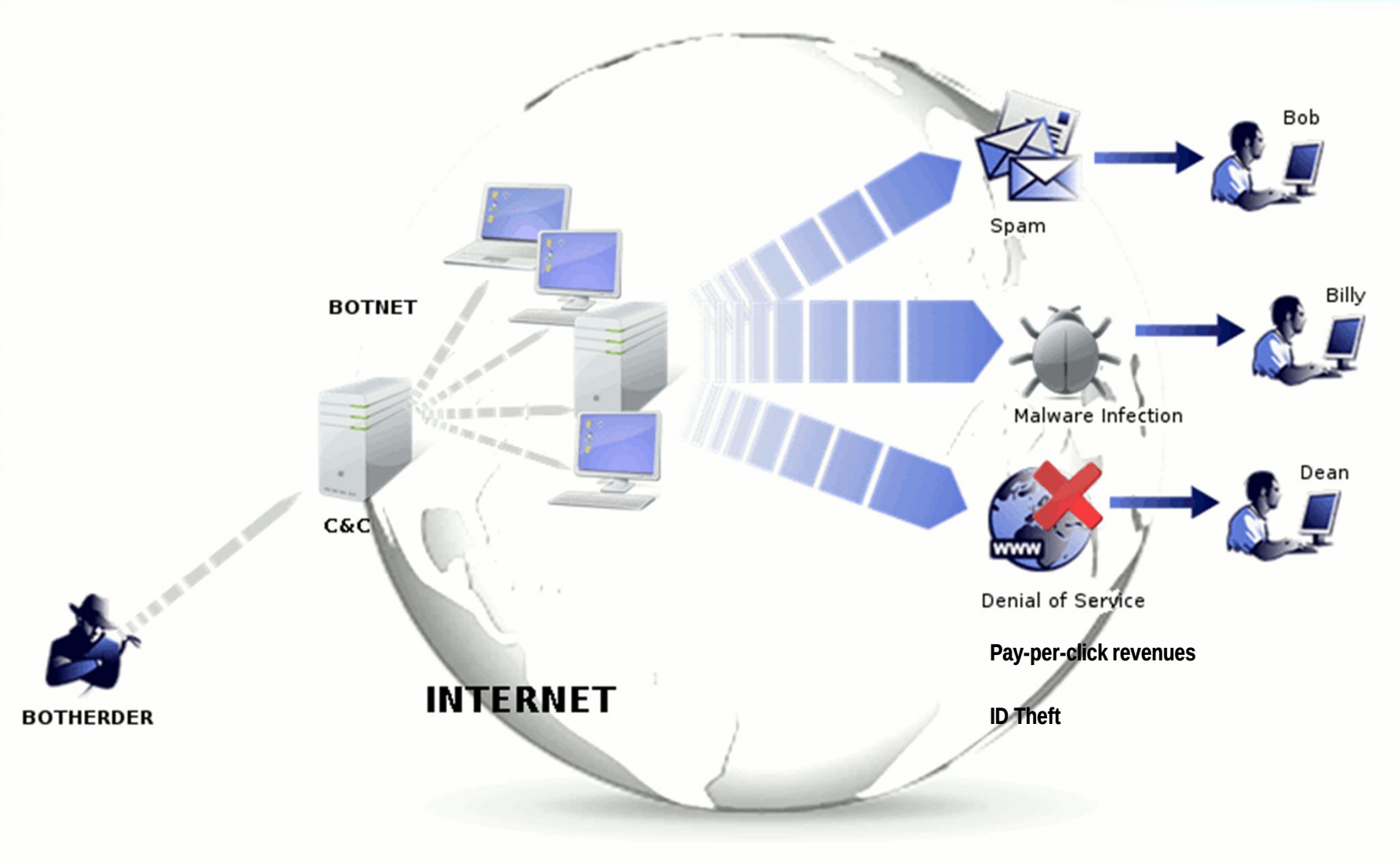
Software flaws	▸ **Malware** (viruses, trojans, worms)
Protocol flaws	▸ **Bot-nets** (DDoS, spam, infection, frauds)
Mind flaws	▸ **Social engineering** (phishing, scams)

Malware


Update your antivirus and firewall?
Yes
No
exe.
exe.
exe.
exe.
spam
spam
spam
spam
http://clickon.me
http://unknown.com
Concept: Vladimir Radunović Illustration: Vladimir Veljašević
DiPLO
www.diplomacy.edu

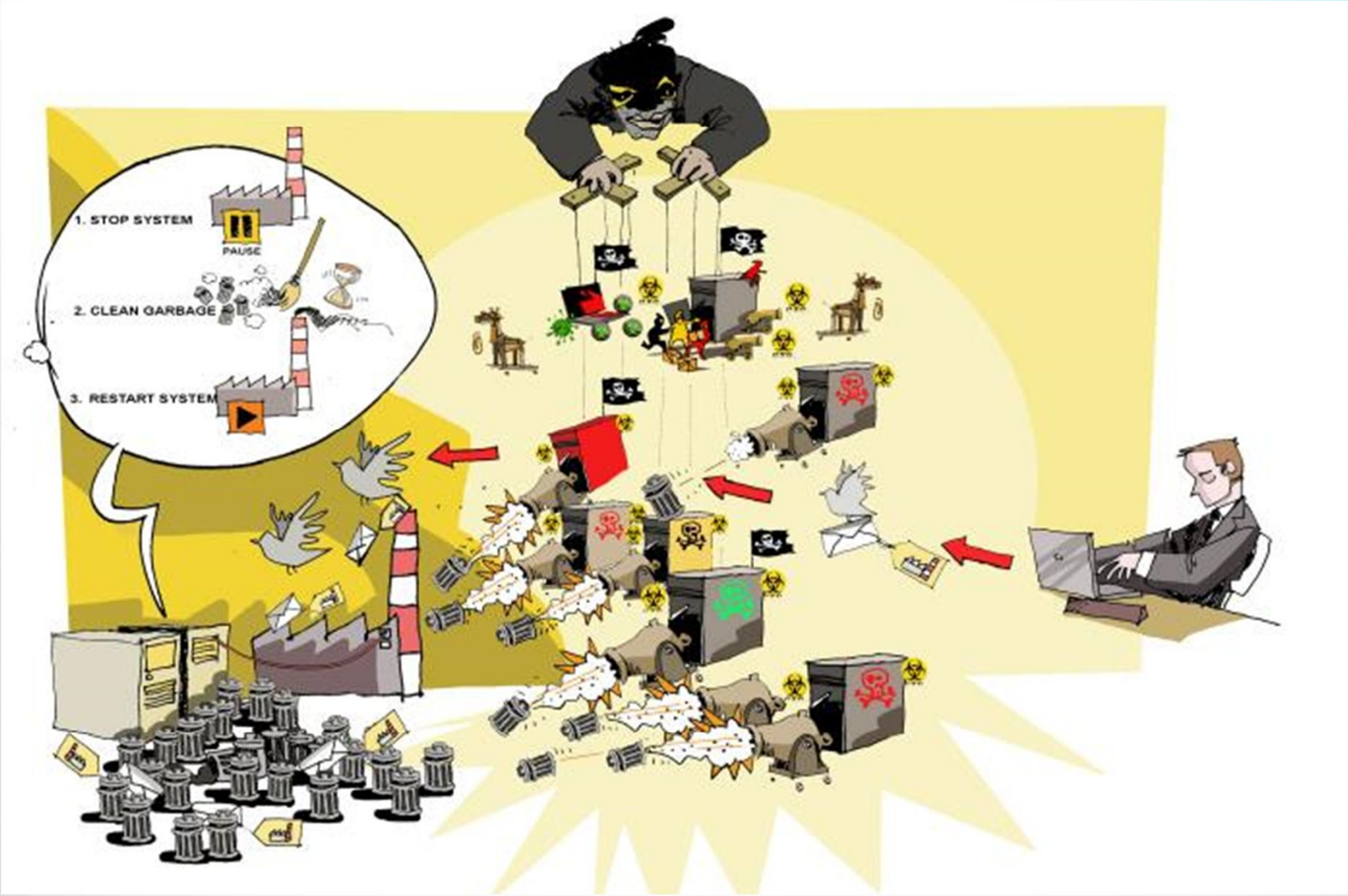
Botnets

Botnets

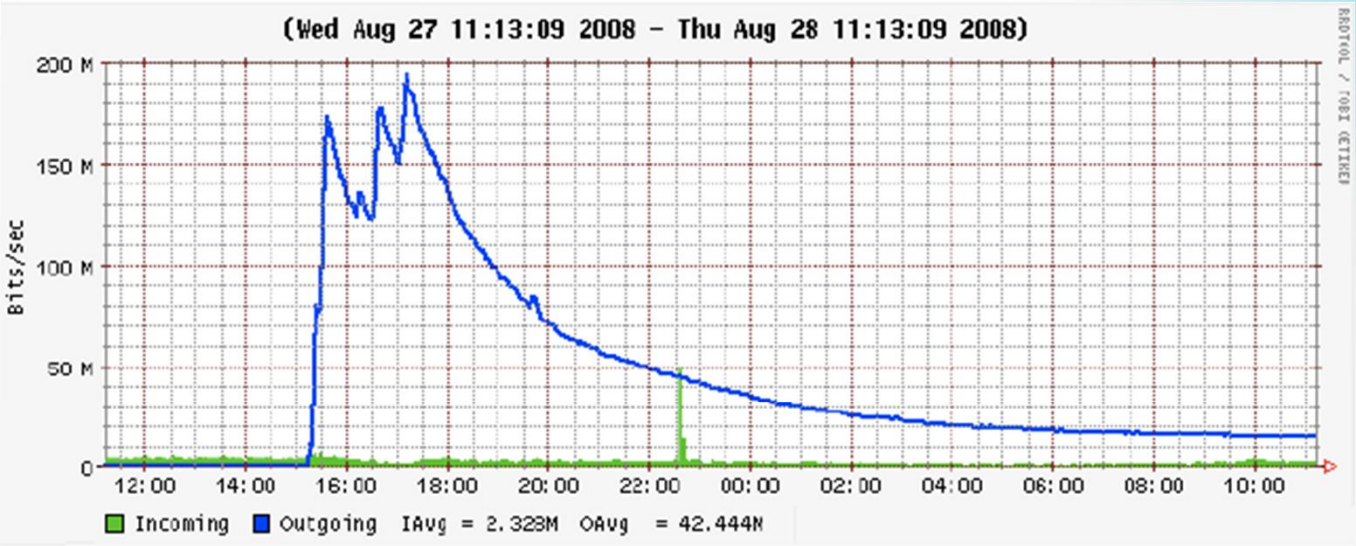


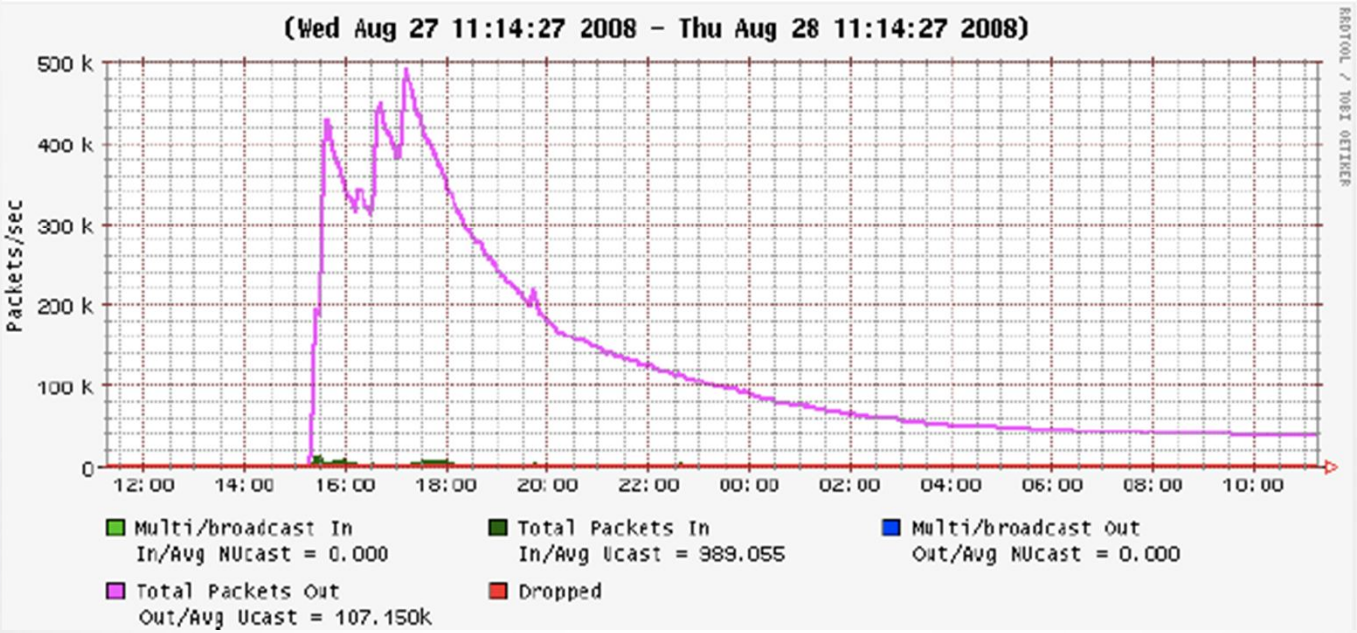
Source: F-Secure

DDoS



DDoS





DiPLO
www.diplomacy.edu

Botnets

Source: www.lessucettes.com

DiPLO
www.diplomacy.edu

DDoS

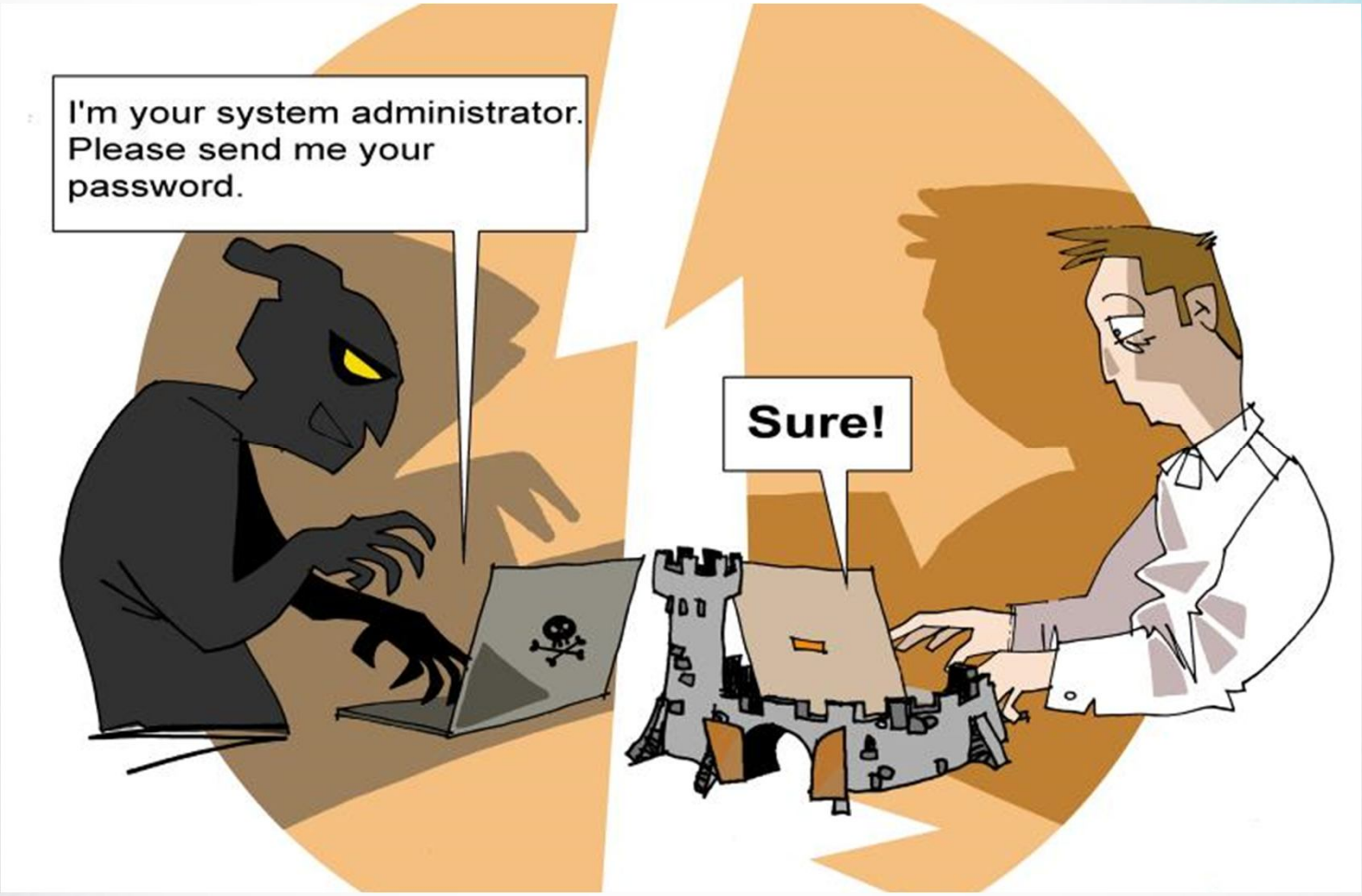
Digital Fears Emerge After Data Siege in Estonia

"It turned out to be a national security situation," Estonia's defense minister, Jaak Aaviksoo, said in an interview. "It can effectively be compared to when your ports are shut to the sea."

Reuters

Protesters in Tallinn confronted the police on April 26, after authorities announced plans to remove a Soviet-era memorial to World War II.

Phishing


I'm your system administrator. Please send me your password.
Sure!

SC Magazine > News > "Human error" contributes to nearly all cyber incidents, study finds

Surprised? Not really

Marcos Colón, Online Editor

Follow @turbomarcos

June 16, 2014

"Human error" contributes to nearly all cyber incidents, study finds

Share this article:

Even though organizations may have all of the bells and whistles needed in their data security arsenal, it's the human element that continues to fuel cyber incidents occurring, according to one recent study.

The "IBM Security Services 2014 Cyber Security Intelligence Index," a report that includes cyber security data on close to 1,000 of IBM Security Services' clients located in 133 countries, indicates that "human error" is involved in more than 95 percent of the security incidents investigated in 2013.

A new IBM report reveals that organizations experienced more than 91 million "security events" last year.

E-scams

I am contacting you in respect of a family treasure of Gold deposited in my name

From: **becky** (becky_time5001@rediffmail.com)

You may not know this sender

Sent: Wed 8/15/07 11:59 AM

To: becky_time5001@rediffmail.com

i am Becky Ofori a Ghanian from Asha
treasure of Gold deposited in my name
As a well known business man,and a
J.J. Rawlings the ex- president of the f
public against the government of the da
loving wife was abandoned after the de
mother carefull and stiff handling of my
benefitting from any of my fathers shar
left at the mercy of my elder brothers.
Right now we are passing through gr
father while he was alive, deposited a c
outfit in my country.We have made all
and i have decided to sell this consignm
proceeds to put our lives on course aga
I want you to come to Ghana and see
the sale overseas .We are prepared to
help , and we are very much prepared
On the contrary, if you are a potential
transaction.
I am looking forward to hear from you

Subject: **Protect your Visa card online with a personal password**
From: Visa Inc. <vbv@visaeurope.com>
Reply-To: vbv@visaeurope.com
Date: 29/03/2008 6:31 PM
To: undisclosed-recipients::

VISA

Protect your Visa card online with a personal password

Solution

Create an additional password to protect your existing card for online purchases

We are proud to announce that Visa Europe in association with all European and
just for enroll and secure your card. Your personal bonus code is VISA-884AM-44
use your code twice, for more info please visit our Privacy and Policy)

Please enroll now by clinking the Global Visa Site select your country and follow t

- Global Visa Sites

Do not be the next victim and fight with us against credit card fraud.

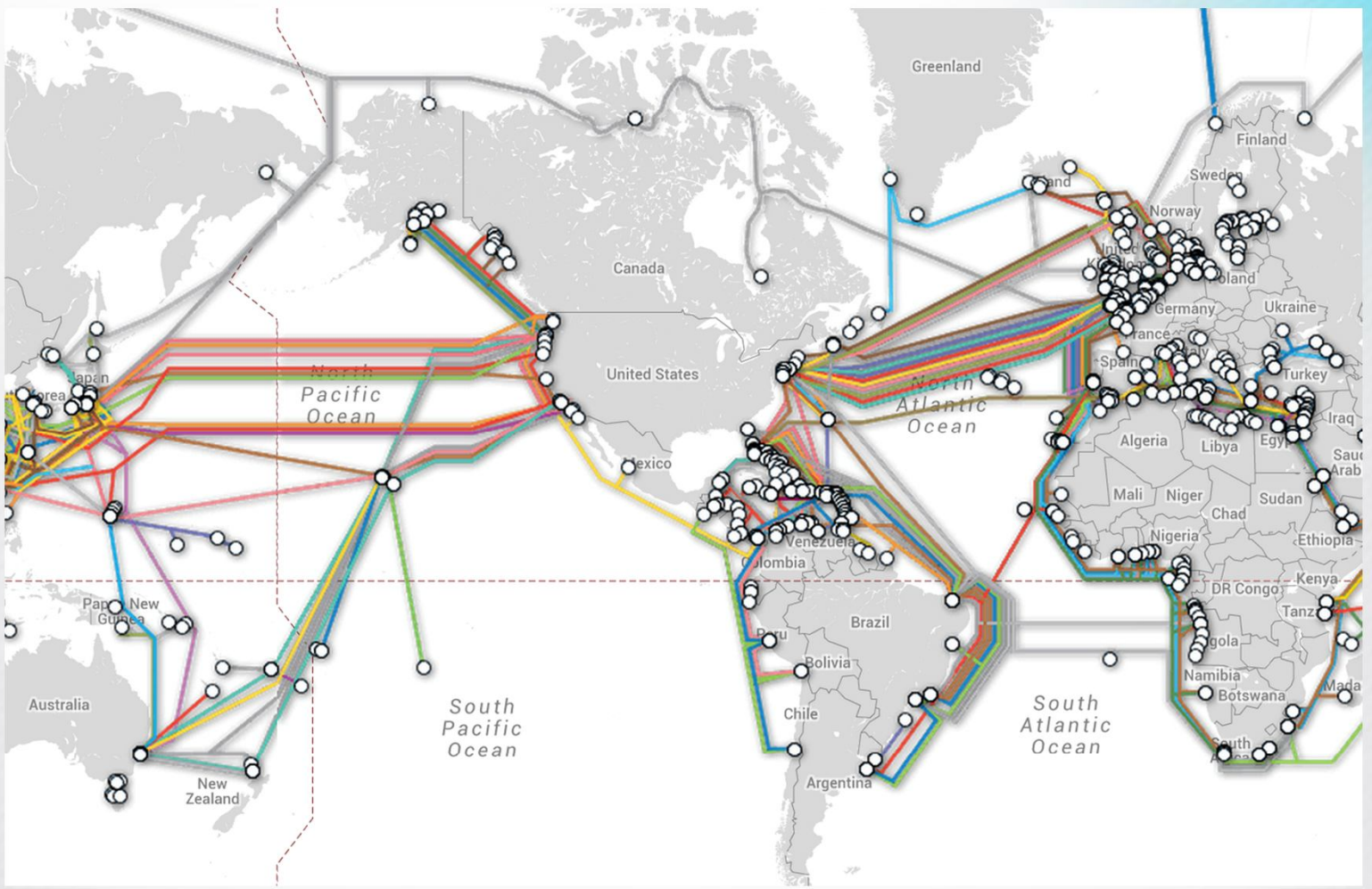
Enjoy life's opportunities

DiPLO
www.diplomacy.edu

End users: addiction + poor hygiene

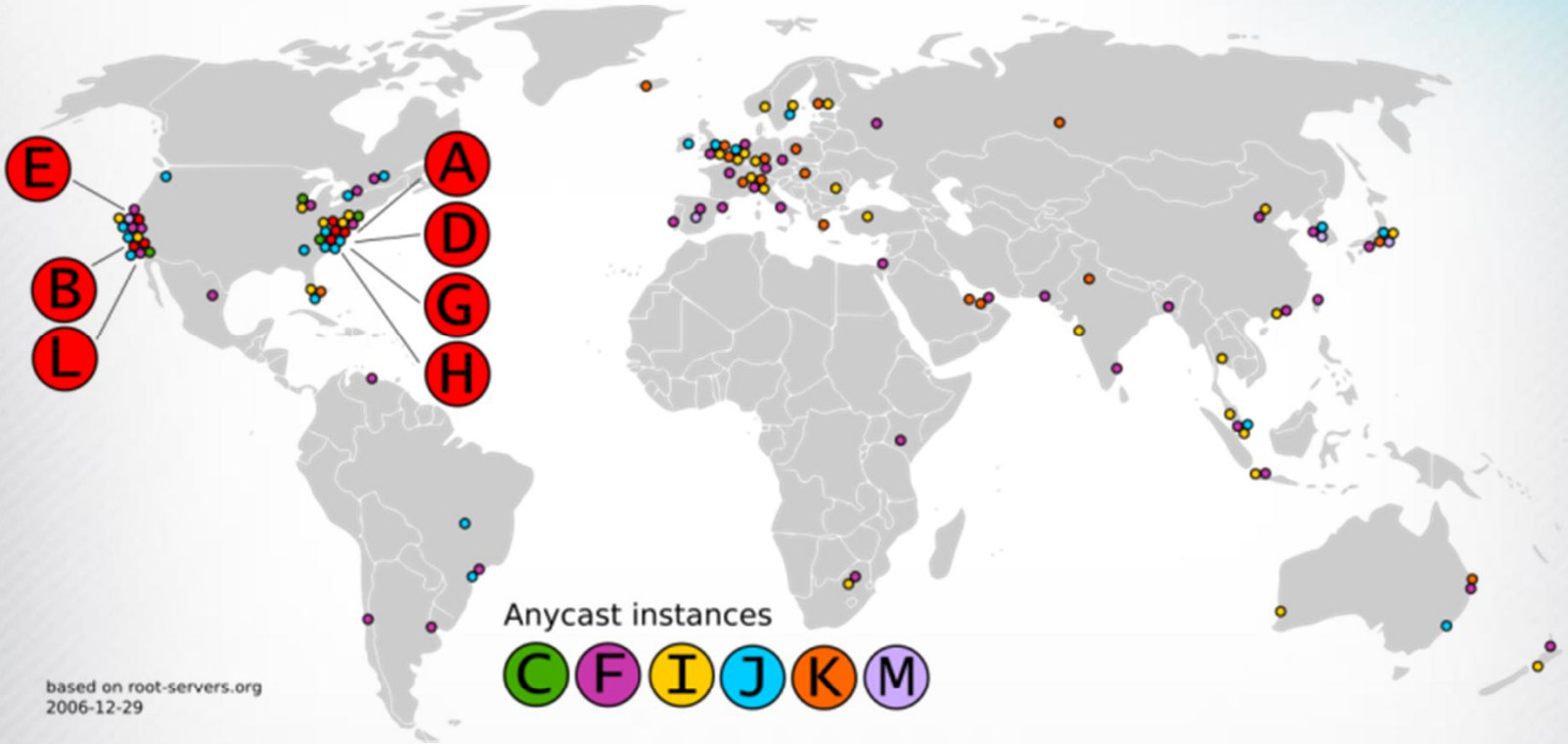
Mapping the field

- Critical information infrastructure protection (CIP)
- Cybercrime
- Cyberconflicts



DiPLO
www.diplomacy.edu

Critical Internet Resources



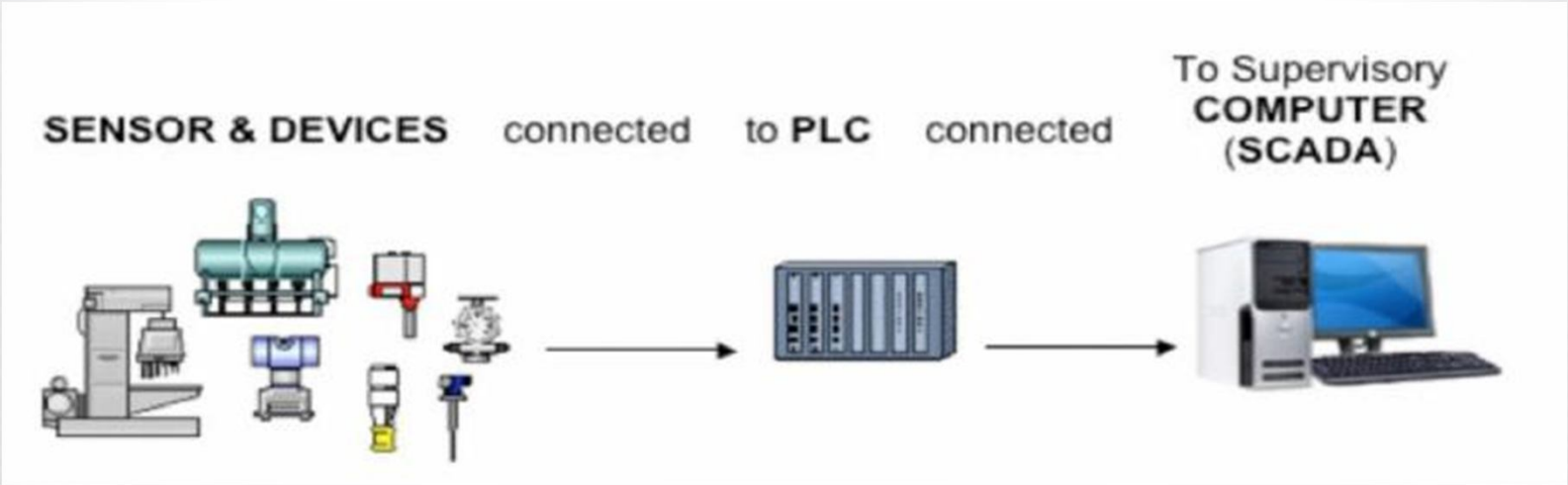
DiPLO
www.diplomacy.edu

- Domain name hijacking
- Packet interception
- Name changing or DNS poisoning
- DNS spoofing

Critical infrastructure



Control room: in 60s, 80s and 2000s



Source: http://www.lucasavoldi.it/blog/?p=62

DiPLO
www.diplomacy.edu

Critical infrastructure

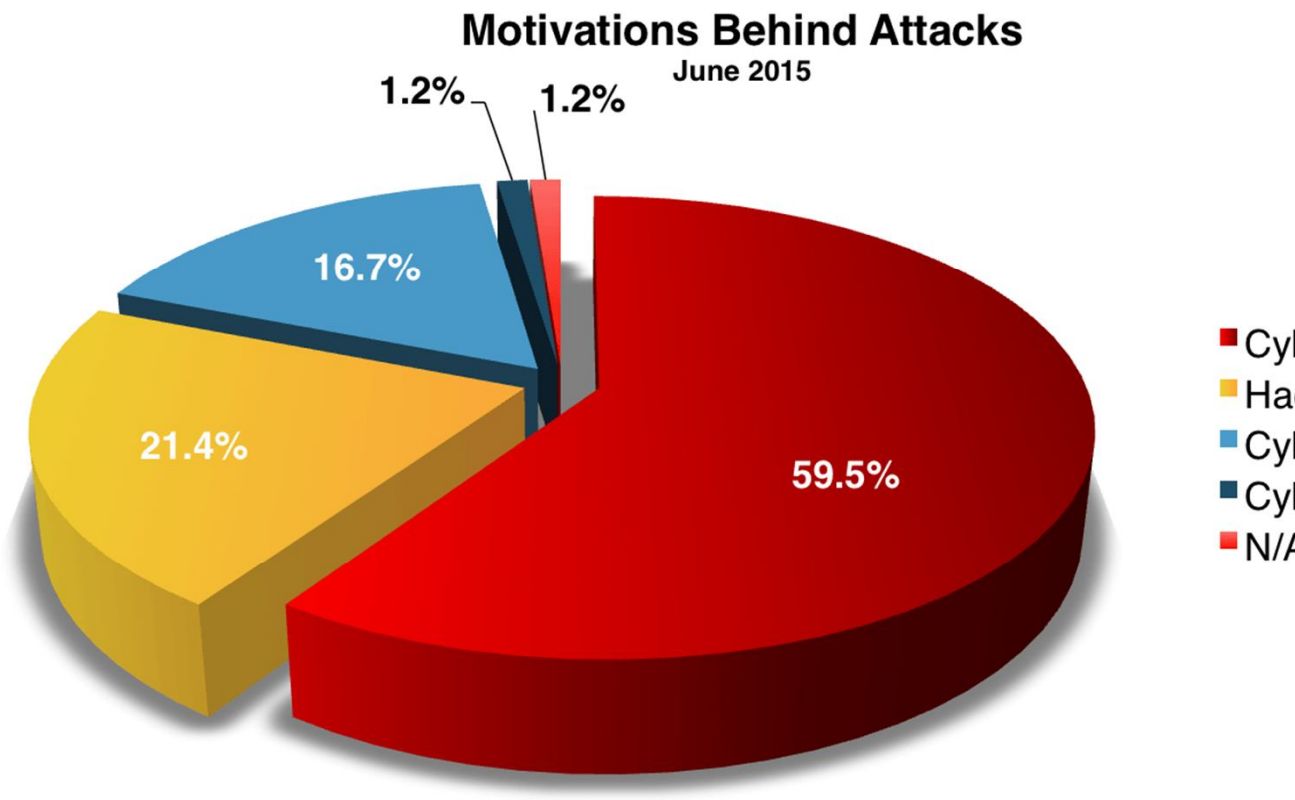
***Source*: http://www.sandia.gov/nisac/overview/**

DiPLO
www.diplomacy.edu

Mapping the field

- Critical information infrastructure protection (CIP)
- Cybercrime
- Cyberconflicts

Attacks



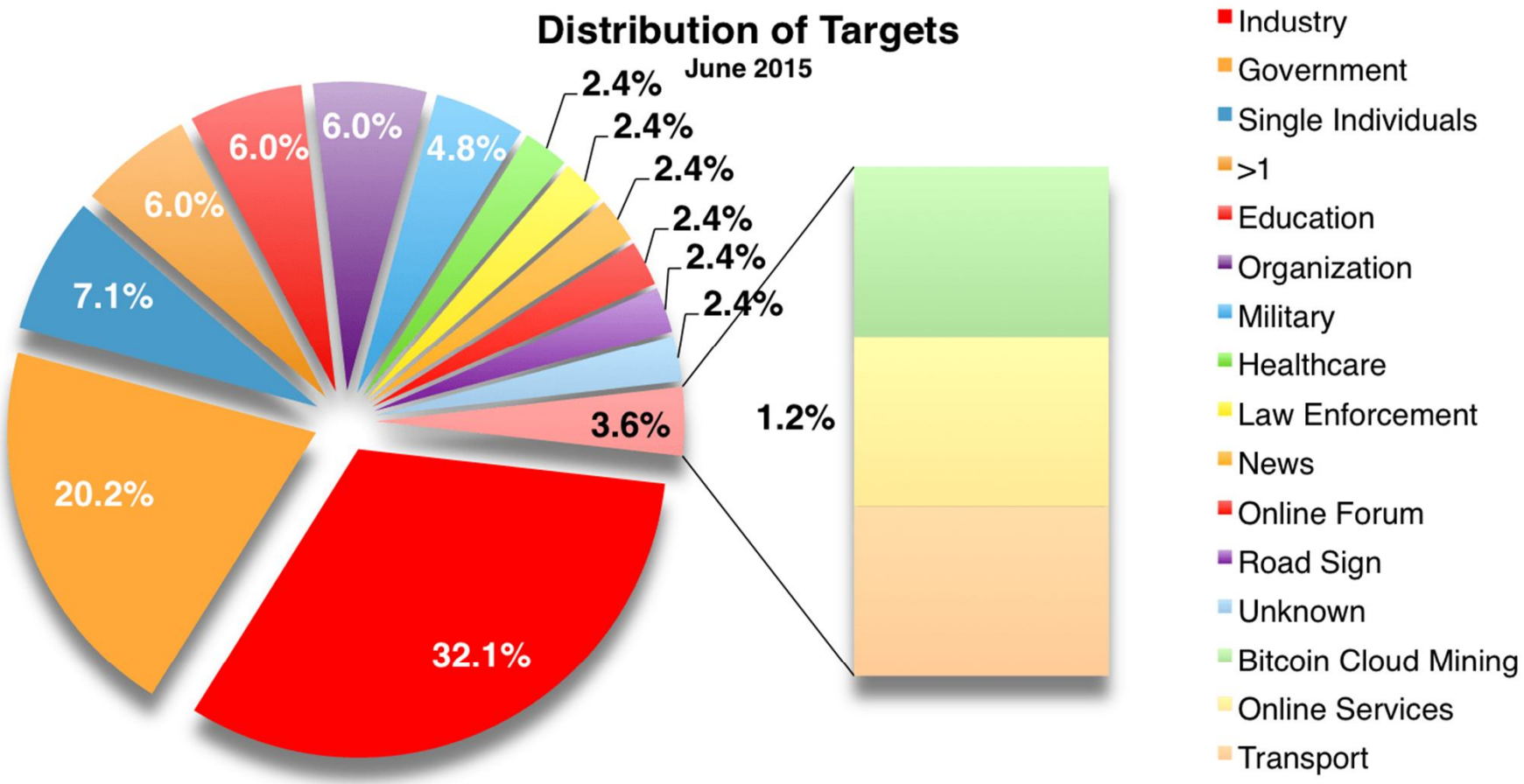
Source: Special prosecutor for high technology crime, Serbia

DiPLO
www.diplomacy.edu

Technology Developments

- 3D printing
- ToR
- Digital currencies
- Internet of Things

Attacks



Source: Special prosecutor for high technology crime, Serbia

DiPLO
www.diplomacy.edu

Cost of cybercrime

Source: Special prosecutor for high technology crime, Serbia

DiPLO
www.diplomacy.edu

Cost of cybercrime

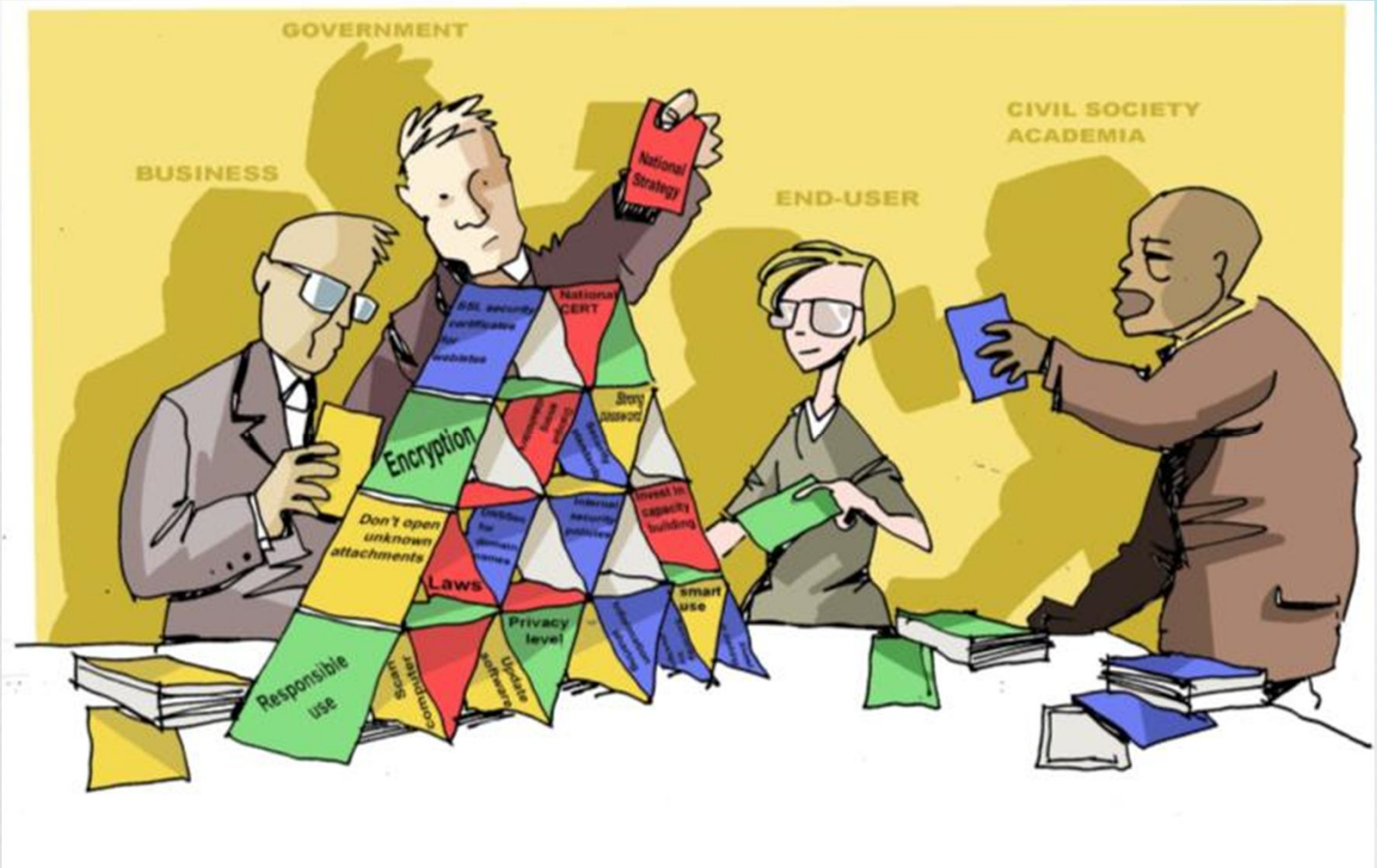
- Internet economy generates between **US$ 2 and US$3 trillion**
- Between **15% to 20%** of the value created by the Internet is extracted by cyber crime

Source: 2014 CSIS/McAfee

Legal Frameworks
CoE's convention on cybercrime

- Offences against the confidentiality, integrity and availability of computer data and systems, such as illegal access or interception or misuse of devices.
- Offences that are computer-related or -facilitated, such as computer-related forgery or fraud.
- Offences that are content-related, particularly those related to child sexual abuse content.
- Offences related to infringements of copyright and related rights.

Collaborative responsibility



DiPLO
www.diplomacy.edu

Actors

- National Governments (Security Ministries, Technology Ministries, Diplomatic Services, Law Enforcement)
- International Organisations (CoE, ITU, UNODC, UN, OSCE)
- Business Sector (Telecomm & Internet Companies, Financial Sector, C(I)IP Operators)
- Academia and technical community (CERTs, TLD and DNS management, hackers, researchers)
- Civil Society (Human Rights, Capacity Building)

International Cooperation

DiPLO
www.diplomacy.edu

International initiatives

- UN: Governmental Group of Experts on “International norms pertaining to state use of ICT” (2011-)
- CoE: Convention on Cybercrime (2001)
- OSCE: Confidence Building Measures re. ICT (2013)
- ITU: Global Cybersecurity Agenda (2008)
- Global Forum on Cyber Expertise (2015)
- OECD: Guidelines on Information Security
- Commonwealth: Cybercrime Initiative and “Model Law” (2011)
- WSIS, IGF, GCCS, ASEAN…

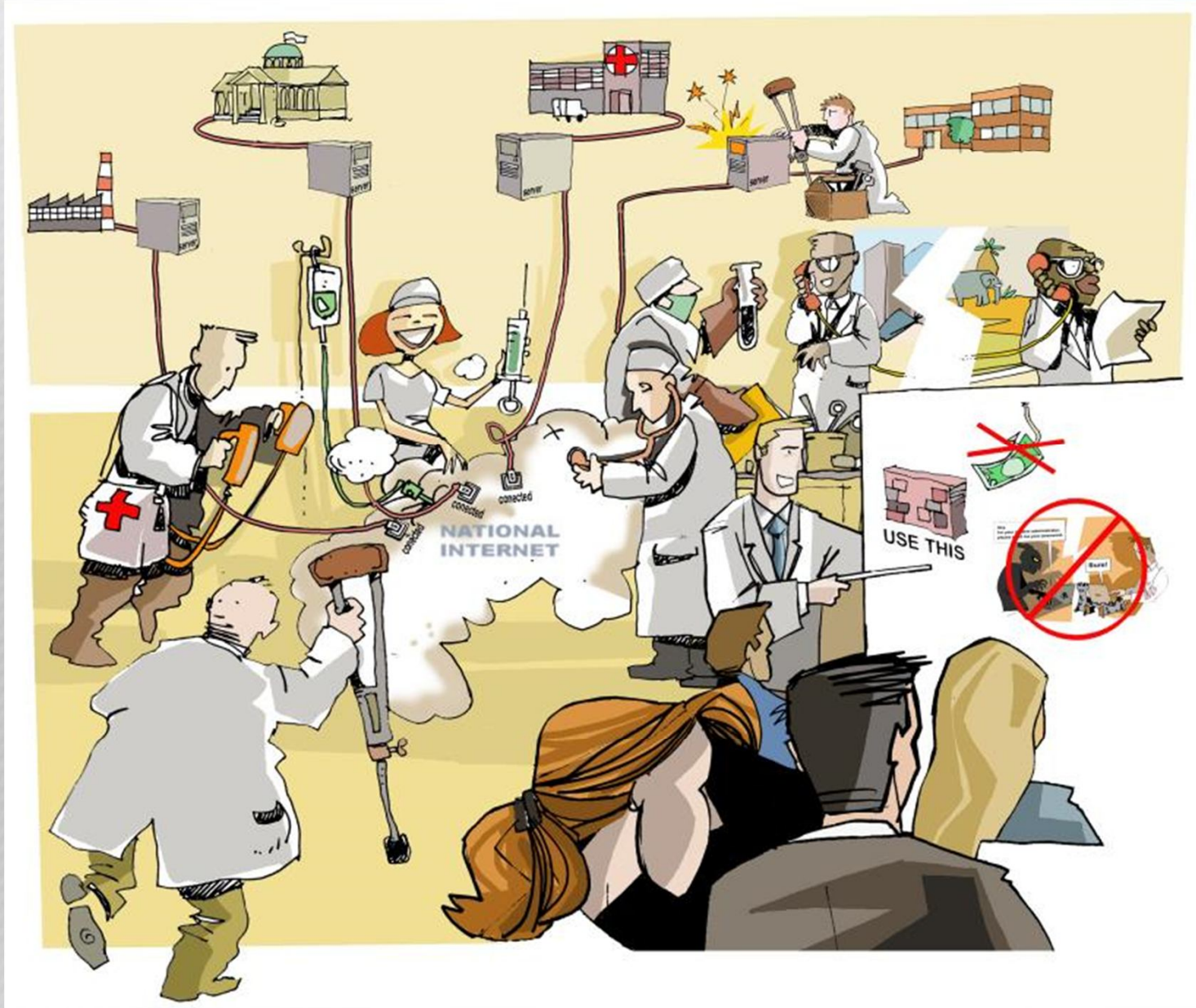
Cooperation

1. Critical Information Infrastructure Protection (CIIP) and network resilience and response
2. Information sharing across sectors on incidents, risks and best practices
3. Legal frameworks and cooperation against cyber-crime
4. Defense and dialogue on IHL applications in cyberspace
5. Role of the corporate sector and Internet communities
6. Awareness building and developing institutional capacities
7. Internet governance and Internet diplomacy

Technical level

CERT/CSIRT

CERT



DiPLO
www.diplomacy.edu

CERT tasks

1. Contact point on a national and international level
2. Incident response
3. Analysis of the system vulnerability and information about the incidents
4. Early warning and alarm
5. National situational awareness in cyber-space
6. Establishing and maintaining a network of partners
7. Awareness raising
8. Advises and assistance with strategic planning

Prevention + Reaction

DiPLO
www.diplomacy.edu

Citizens' level

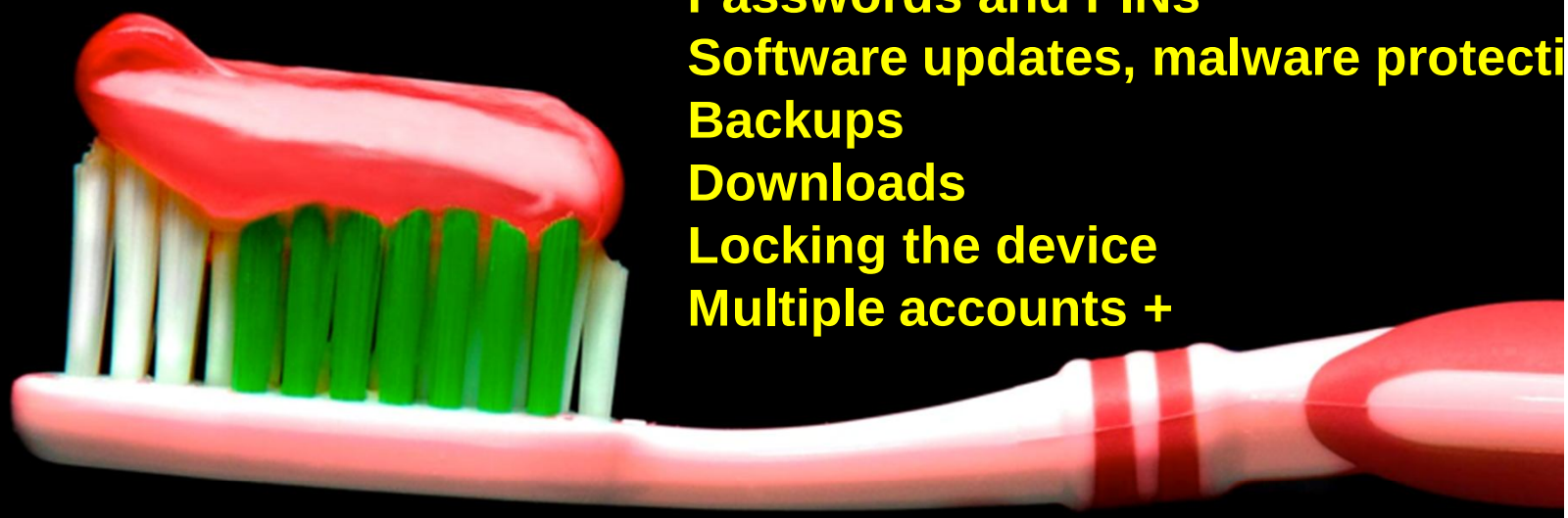
Digital hygiene

DiPLO
www.diplomacy.edu

Promote digital hygiene

The basics

Passwords and PINs
Software updates, malware protecti
Backups
Downloads
Locking the device
Multiple accounts +



Landmines

Disclosures and sharing
Phishing and scams
Attachments
Free unencrypted Wi-Fi

Advanced

Remote wipe
Geolocation
Bluetooth
Home Wi-Fi

Mapping the field

- Critical information infrastructure protection (CIP)
- Cybercrime
- Cyberconflicts

Conflicts

Cyber-warfare

DiPLO
www.diplomacy.edu

Estonia

Sony-N.Korea

Stuxnet

PRISM

„Aurora“

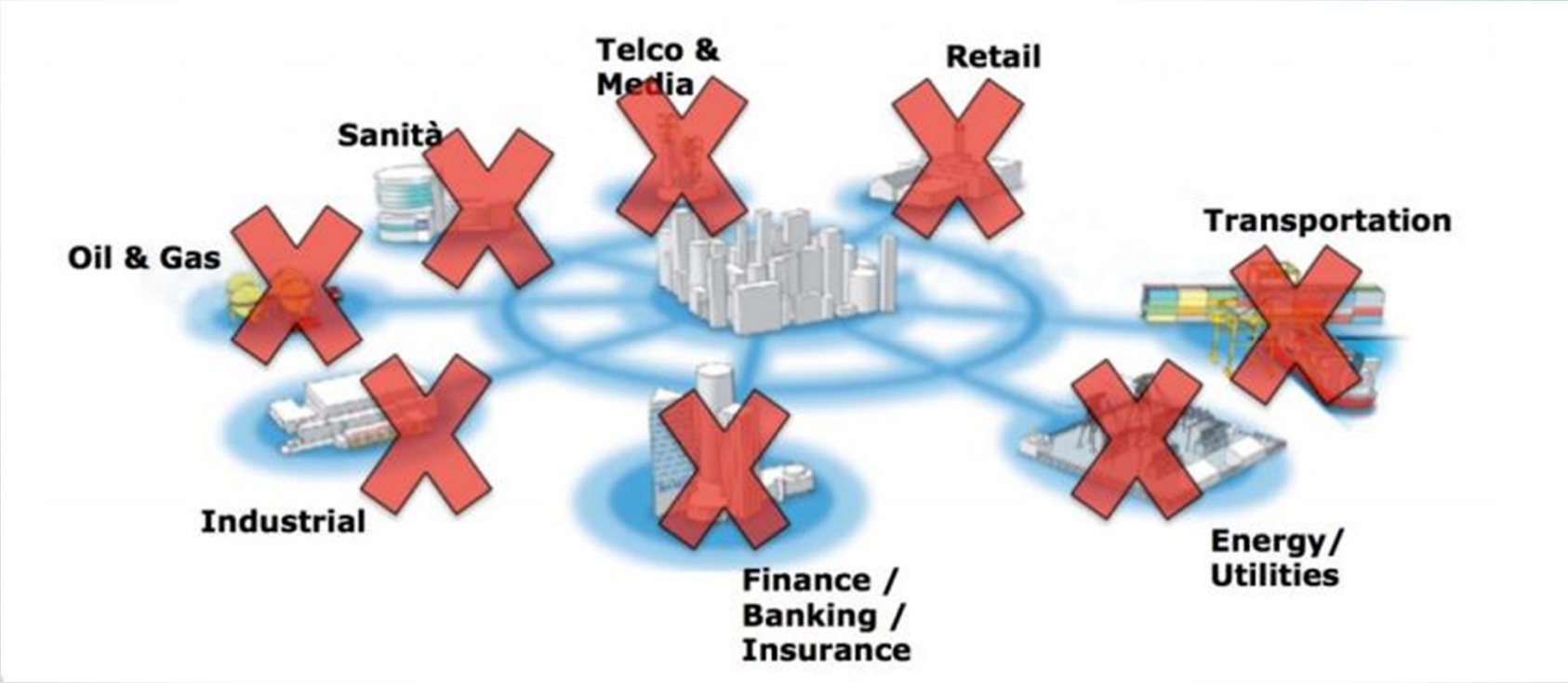
Warfare 2.0

DiPLO
www.diplomacy.edu

Asymmetry


Q:
WHAT WILL THE WARRIOR-GUARDIAN OF THE FUTURE LOOK LIKE?
YO! DUDE... BACK HERE
CYBER SECURITY

Targets



Source: http://www.lucasavoldi.it/blog/?p=62

```
update = '-u' in opts or '--update-taglist' in opts
 if not os.path.isfile("tag_data.json") or update:
   params = urllib.urlencode({
     'username": "config",
     'password": "conf1g",
     "action": "queryresults",
     "query": "select TAGNAME, BITMODE from IND order by ADDR asc",
     "returnType": "array",
     "deflateBoundary": -1
   })
```

Source: CERT-SI. The photo is symbollic. Bonneville Dam (cc) EMSL @ flickr.com

Targets


IBM
Welcome to
TheSmarterCity™
Watch the Documentary
Smarter
Transportation
Airports & Rail
Public Safety
Social Services
Education
Healthcare
Economic
Development
Transportation
Traffic
Energy & Utilities

Militarisation

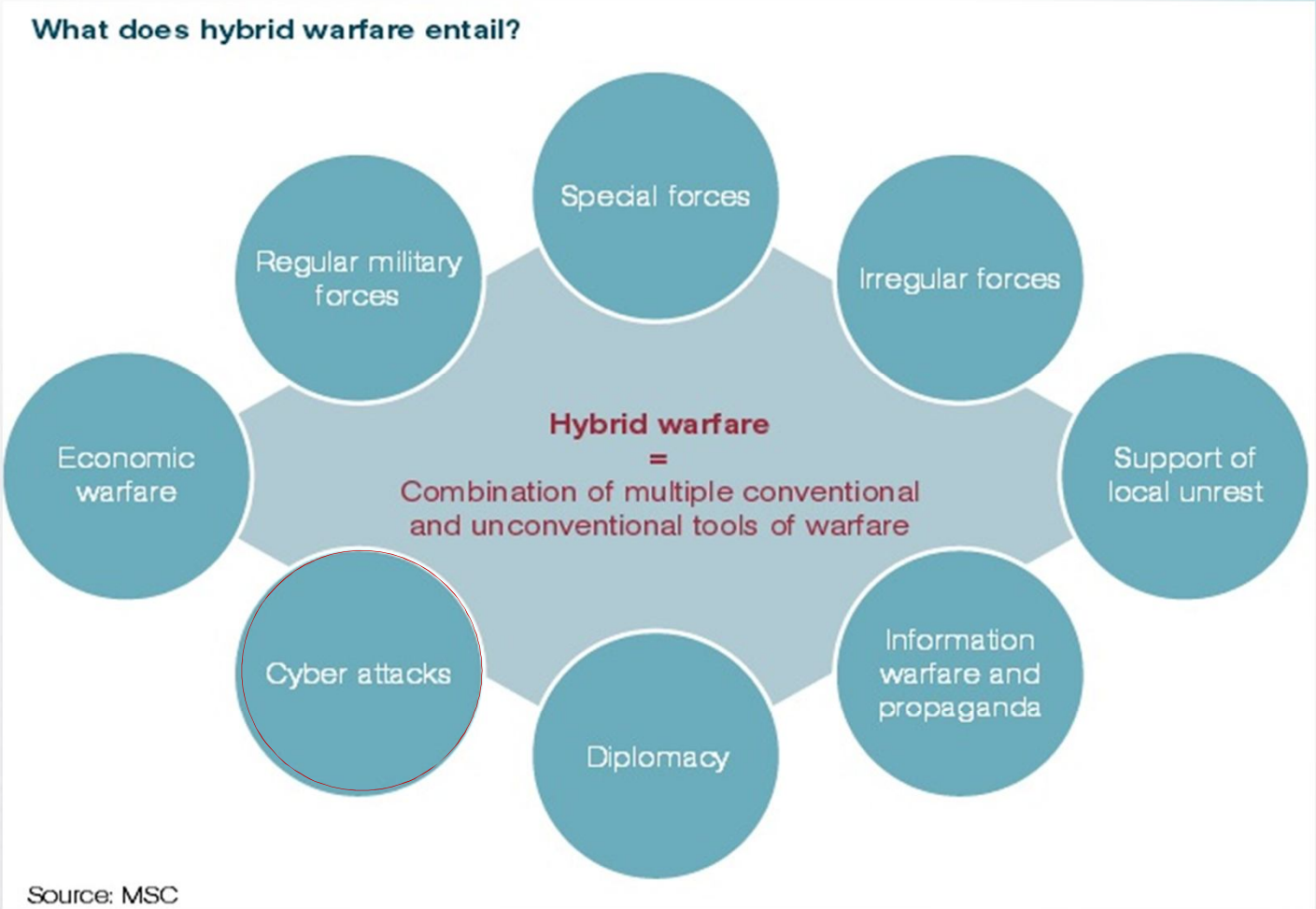
- UN: Expert group on international security in ICT
- US: 4x Cyber-Command with Pentagon
- UK: Cyber Defence Operations Group at the Ministry of Defence
- Russia: FSB (Federal Security Service)
- China: Cyber-warfare unit within PLA
- Iran: High council for cyber-space and cyber-defence command
- NATO: CCDCoE
- EU: European Defence Agency (EDA)

Cyber-war – hype or reality?

- Cyber “armed attack”?
- “Destruction”?
- (Spill-over) Effects?
- Response?

DiPLO
www.diplomacy.edu

Hybrid warfare



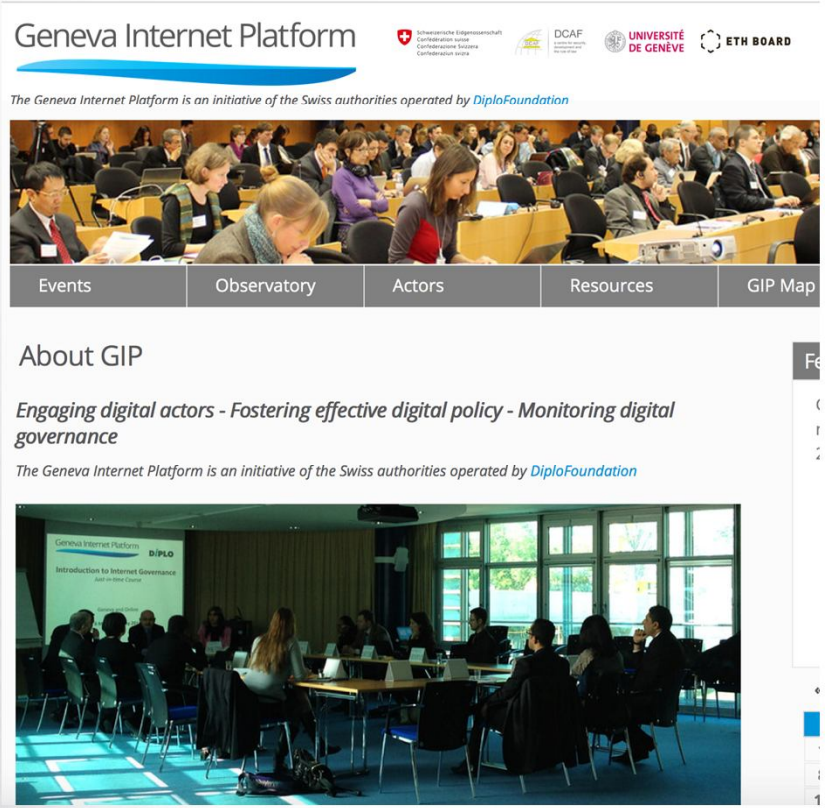
Conflicts Prevention

DiPLO
www.diplomacy.edu

Negotiations

- **Legal frameworks and cooperation against cyber-crime**
- **Confidence building measures (CBM), cooperation on critical infrastructure protection and response to cyber-incidents**
- **Defining cyber-conflicts and application of IHL to cyber-space**
- **Setting the norms of behavior in cyber-space**
- **Control of proliferation of cyber-weapons and dual-use technologies**
- **Cyber-disarmament**
-

Finally, an invitation:



DiPLO
www.diplomacy.edu

Visit:
www.diplomacy.edu
www.diplointernetgovernance.org

Contact:
diplo@diplomacy.edu
mariliam@diplomacy.edu

Twitter:
@igcbp, @DiplomacyEdu
@mariliam

DiPLO
www.diplomacy.edu