JYVÄSKYLÄN YLIOPISTO

AHEAD OF ITS TIME
FOR 150 YEARS

UNIVERSITY OF JYVÄSKYLÄ
JYVÄSKYLÄN YLIOPISTO

Cyber Security threats in the internet world

Dr. Martti Lehto

20.2.2014

High Level Cyber Security Comment

4.2.2014

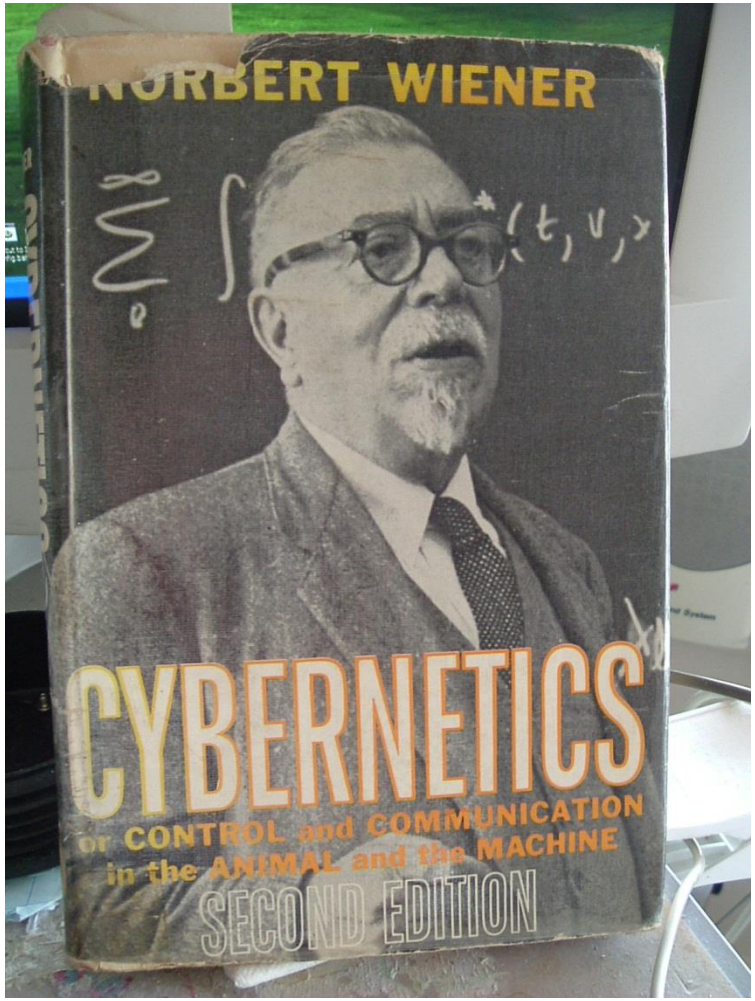
President Sauli Niinistö highlighted cyber security. “Our key functions are more and more dependent on information technology and data networks. Cyber influence forms a part of the picture of future conflicts separately or alongside other ways of applying pressure or using force. While the cyber dimension is not pervasive, it is present. We still have much to do in this respect. We need new legislation. We need to put strategies into practice. All this must be implemented without violating fundamental rights or the protection of privacy,”

CYBER WORLD

Definition of the Cyber World

The word ***cyber*** is generally believed to originate from the Greek verb κυβερεω (kybereo) – to steer, to guide, to control.

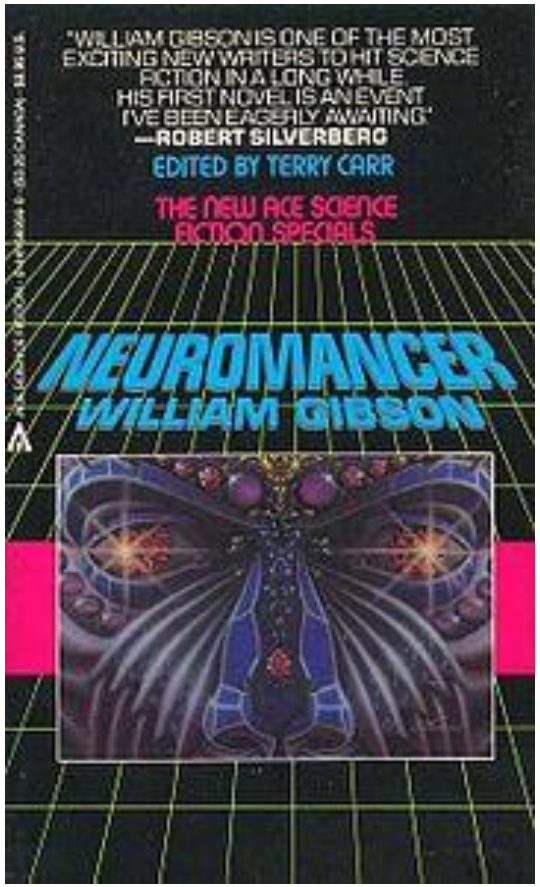
At the end of the 1940s **Norbert Wiener** (1894–1964), an American mathematician, began to use the word ***cybernetics*** to describe computerised control systems.



Definition of the Cyber World

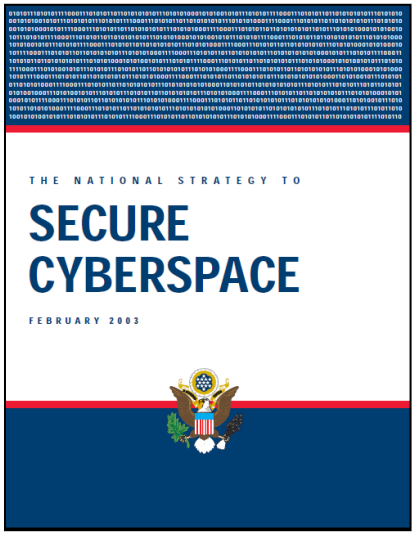
William Gibson, a science-fiction novelist, coined the term ***cyberspace*** in his novel Neuromancer .

Science-fiction literature and movies portray the Gibsonian cyberspace, or matrix, as a global, computerised information network in which the data are coded in a three-dimensional, multi-coloured form.

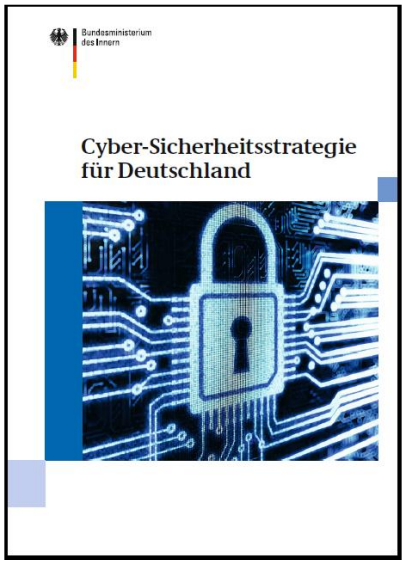


Definition of the Cyber World

US National Strategy to Secure Cyberspace: Cyberspace is **nervous system of our nation's critical infrastructures** - the control system of our country.
Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work."



2003



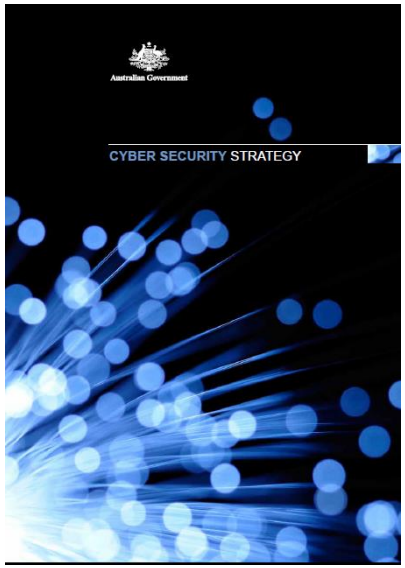
2011

Germany cyber security strategy: "Cyberspace is the **virtual space of all IT systems** linked at data level on a global scale."

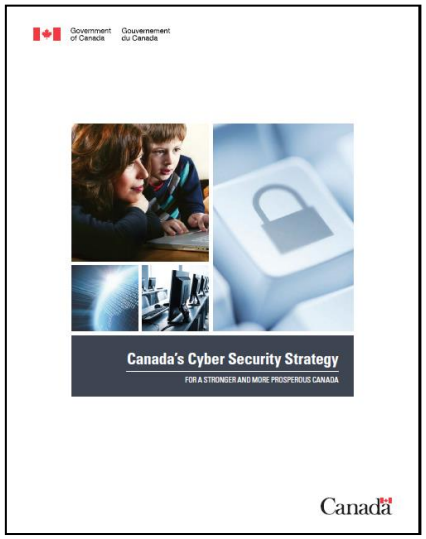
Definition of the Cyber World

Australian Cyber Security Strategy:

"Australia's national security, economic prosperity and social wellbeing are critically dependent upon the availability, integrity and confidentiality of a range of **information and communications technologies (ICT).** This includes desktop computers, the Internet, mobile communications devices and other computer systems and networks."



2009



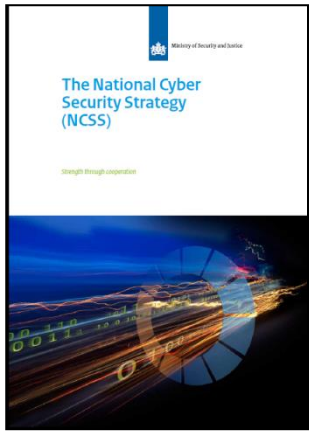
2011

Canada's Cyber Security Strategy:

"**Cyberspace** is the **electronic world** created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship

Definition of the Cyber World

The Netherlands' The National Cyber Security Strategy: "Cyber security is freedom from danger or damage due to the disruption, breakdown, or misuse of **ICT**."



2011

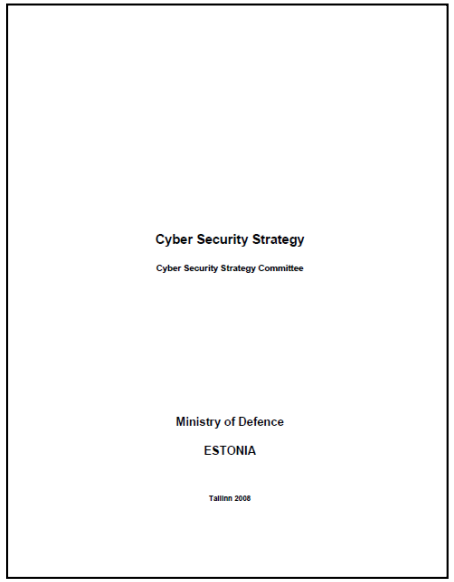
2011

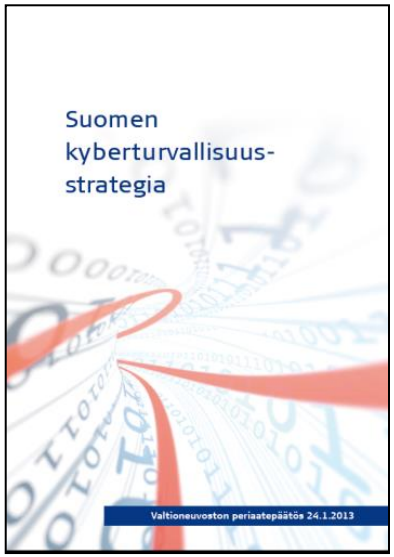
The UK's cyber security strategy: "**Cyberspace** is an **interactive domain** made up of **digital networks** that is used to store, modify and communicate **information.** It includes the Internet, but also the other **information systems** that support our businesses, infrastructure and services."

Definition of the Cyber World

Estonia's cyber security strategy : "The security of **cyberspace** acquires a global dimension and the protection of **critical information systems** must be elevated, in terms of national security, on a par with traditional defence interests."

2008





Finland's cyber security strategy: "An international term for this interdependent, **multipurpose electronic data processing environment** is the **cyber domain**."

2013

Cyber definitions

- **Cyber world:** the presence of human post-modern existence on earth
- **Cyber space:** a dynamic artefactual state formed by bits
- **Cyber domain:** a precisely delineated domain controlled by somebody
- **Cyber ecosystem:** systems of a cyber-community and its environment
- **Cyber environment:** constructed surroundings that provide the setting for human cyber activity and where the people, institutions and physical systems with whom they interact
- **Cyber culture:** the entirety of the mental and physical cyberspace-related achievements of a community or of all of humankind

Definition of the Cyber World

The cyber world can be defined as a global and multidimensional ICT network, into which the user (man or machine) can connect via fixed or mobile data terminals, and virtually move about within it.

In other words, the cyber world is an amalgamation of the Internet, other physical networks, digital services and virtual reality: it is a multi-user virtual environment.

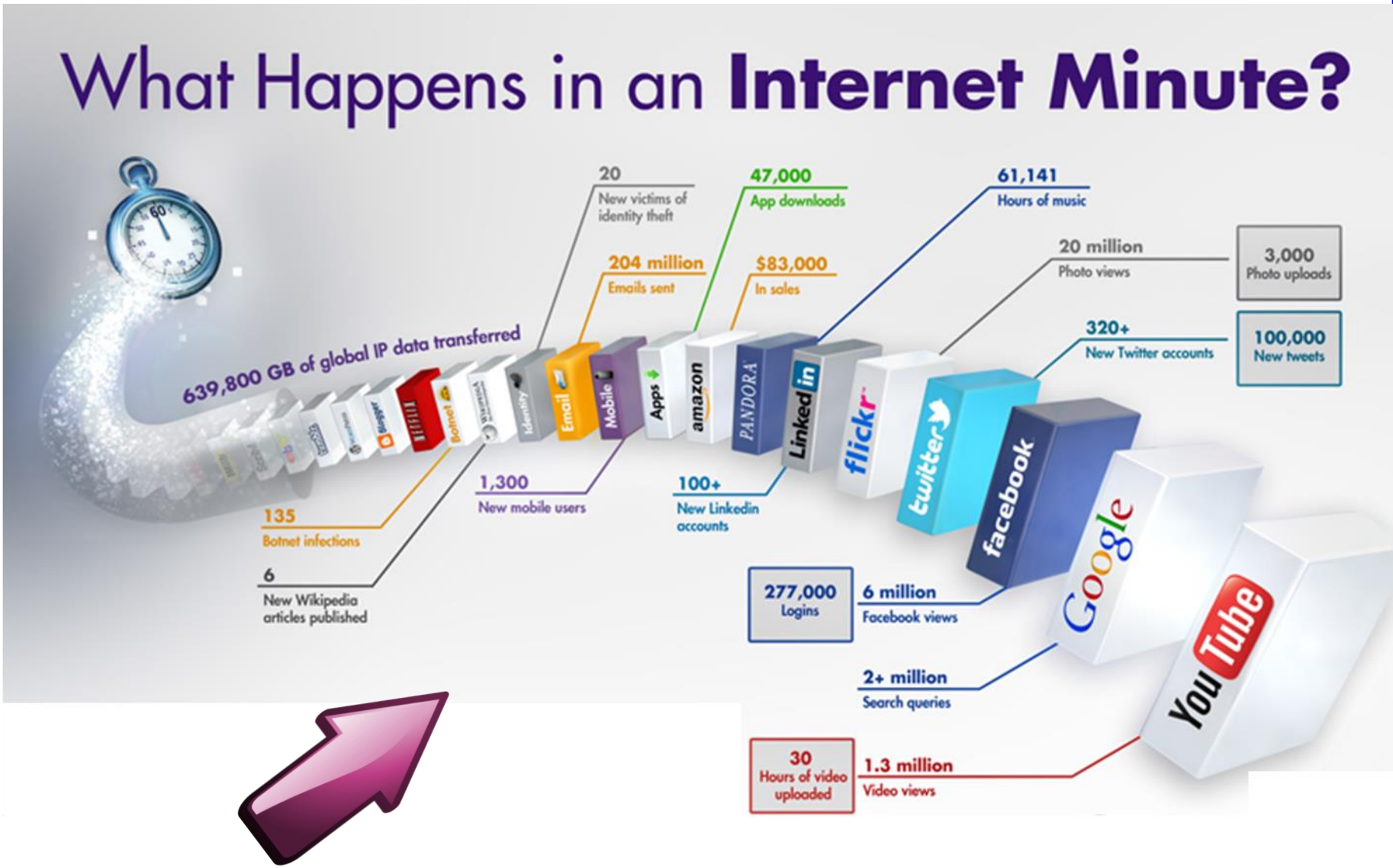
WHAT HAS CHANGED?

Time

Data

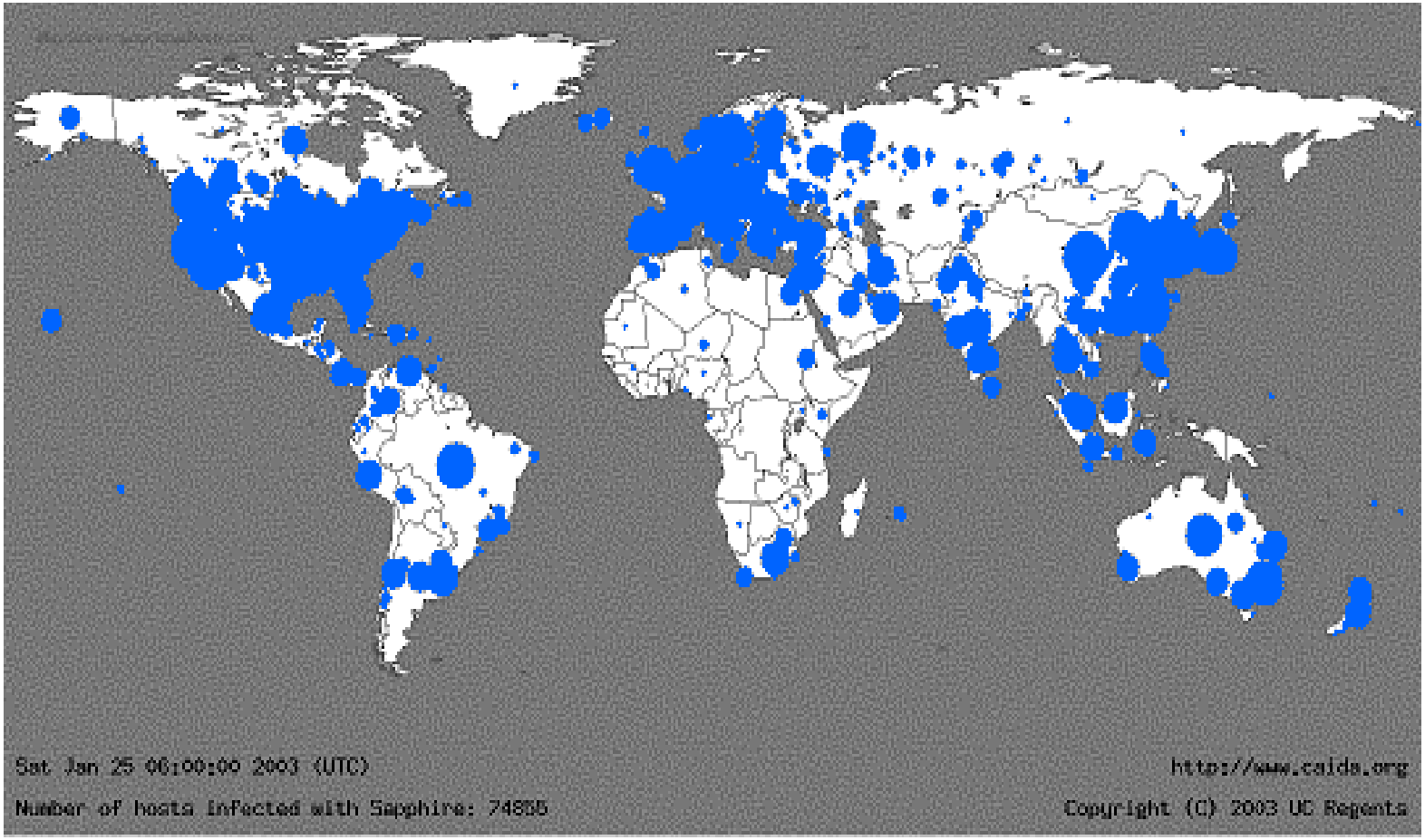
Network

Intelligence



Advanced Cyber Attacks occur up to once every three minutes against the enterprises. (Advanced Persistent Threat, APT)

Slammer-worm infection



Slammer caused a denial of service on some Internet hosts and dramatically slowed down general Internet traffic, starting at 05:30 UTC on January 25, 2003. It is estimated that it reached its full level of global internet infection within ten minutes of release.

Global Data Production

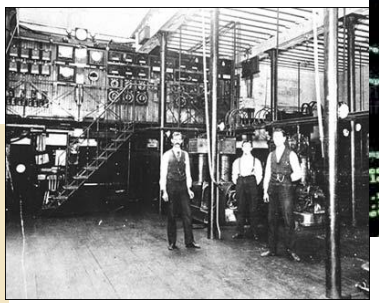
Google CEO Eric Schmidt:
"There was 5 exabytes of information created between the dawn of civilization through 2003, but that much information is now created every 2 days, and the pace is increasing."

October 2010

We produce 2.5 quintillion (2.5×10^{18}) bytes of information every day.

The Large Hadron Collider, at the European Organization for Nuclear Research (CERN), which has 150 million sensors and is creating 22 petabytes of data in 2012.

Network evolution



Internet
1990

Power-distribution network

Edison Illuminating Company 1880

Telephone network

Tivadar Puskás: switchboard 1876

Rail Road

Beginning of the 1800's

Water system

Aqueduct 100 BC

Road network

Via appia antica 400 BC

COMPATIBLE?

Critical Infrastructure

.mil

.gov

Public Networks

DNS

DHCP

DSL

Wireless

Cable

Citizens in the internet

.fi

Core Backbone

Inter-Domain Routers

Distribution

Service Aggregation

Private Enterprise networks

.com

Critical Information Infrastructure

Networked Cyber World

Internet access

Google CFO Patrick Pichette:

Google Fiber 1Gbit: 2012
Google Fiber 10Gbit: 2022 or sooner

Future fiber-to-the-home (FTTH)

“There is an obsessive focus on speed at Google.”

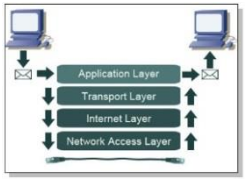
Layers of the information infrastructure

Pragmatic layer

- User's information-awareness environment
- Contextual understanding of information

Semantic layer

- Information and datasets in the user's computer s
- Different user-administered functions, such as printer control



Syntactic layer

- System control and management programs and features
- Network protocols, error correction, handshaking etc.

Physical layer

- Network devices, switches and routers
- Wired and wireless connections

Libicki Martin, Conquest in Cyberspace – National Security and Information Warfare, RAND 2007
Libicki Martin, Cyberdeterrence and Cyberwar, RAND 2009

Intelligent Cyber World

968 million

968 million smart phones were sold in 2013

90%

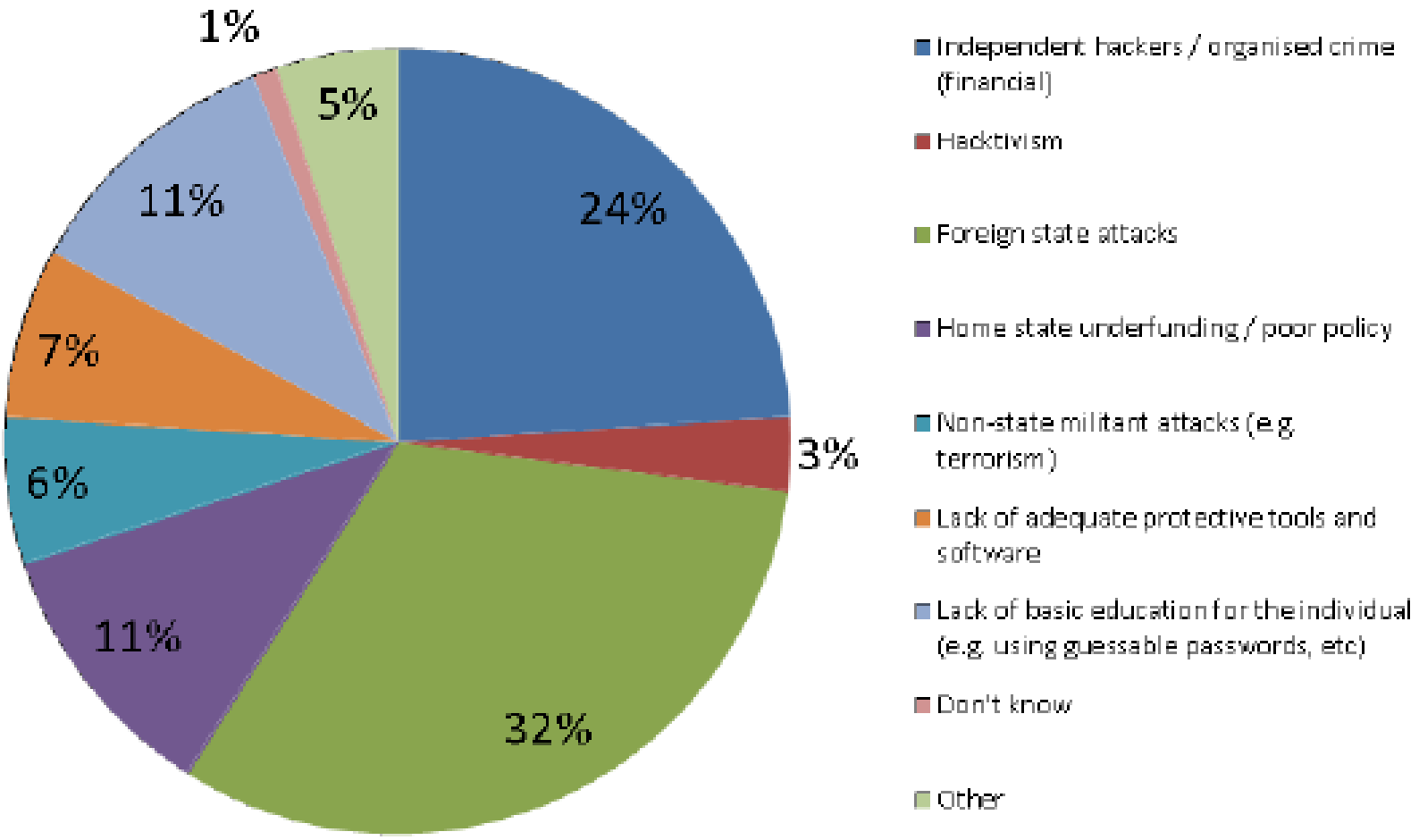
Nearly 90% of innovation in automobiles is related to software and electronics systems.

1 trillion

Soon, there will be 1 trillion connected devices in the world, constituting an “internet of things.”

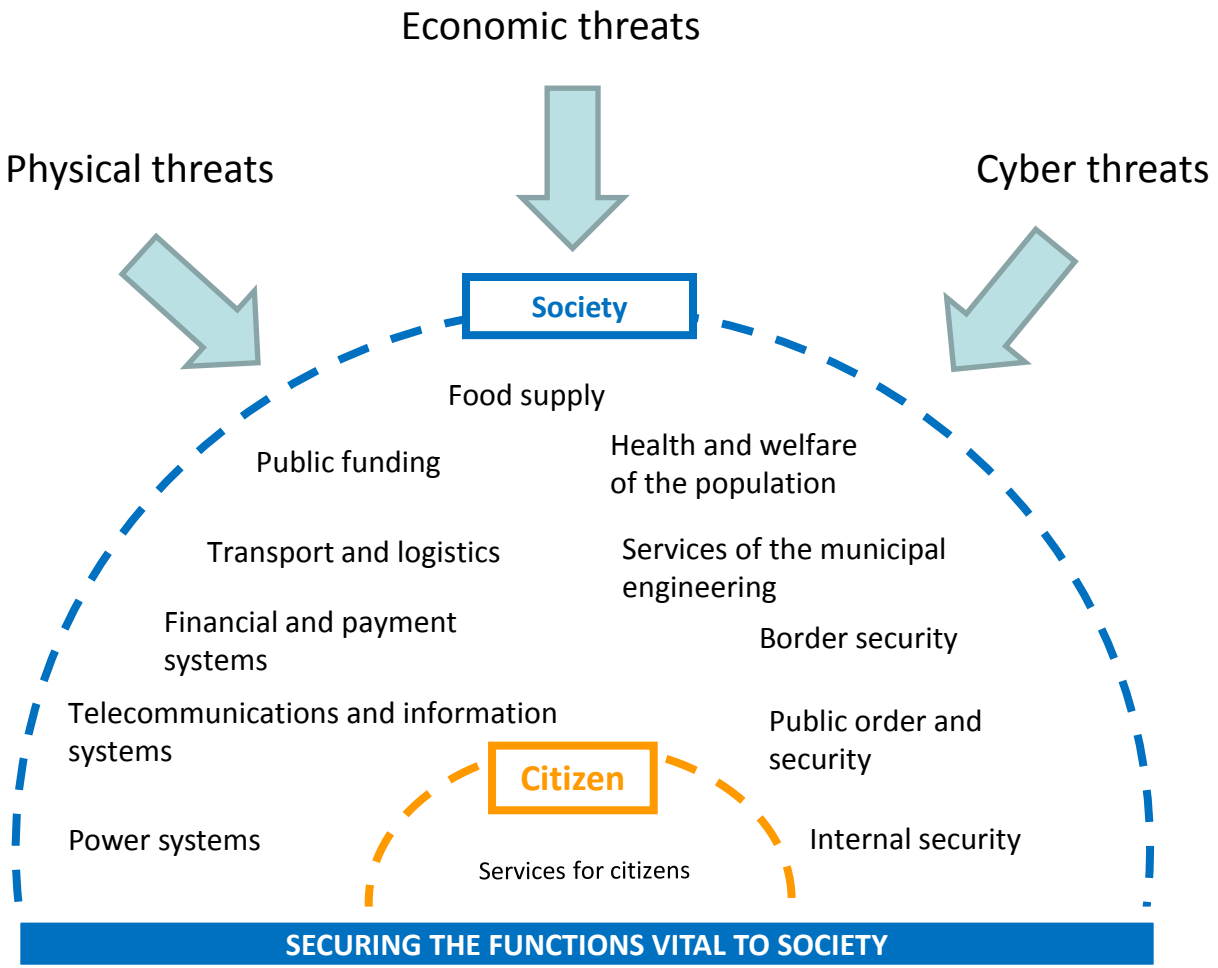
THREATS IN CYBER WORLD

What is the **biggest threat to national cyber security?**



Defence IQ, How Confident Are We In Today's Cyber Defence Measures?, Aug 2012

Threats and the Functions Vital to Society



Physical threats: environmental catastrophes of the nature, traditional war, terrorism, civic disobedience

Economic threats: collapse of the national economy, collapse of the global economy

Cyber Threat Modell

Cyber warfare

Cyber terrorism

Cyber espionage

Cyber-crime

Cyber vandalism

Cyber vandalism: Hactivism

Hactivism stands for the different forms of computer and online activism, mostly on the Internet.

Online activism two main categories: Internet-enhanced and Internet-based. The former concerns activism in which the Internet is mostly used as an extra communications channel or for the purpose of spreading awareness. The latter is only achievable on the Internet.

Cyber vandalism: Cyber swarming

Groups of activists were mobilised over the Internet and led by mobile phones.

- **Britain 2011**
- **Arab spring 2010-**
- **25.1.2011, 15 000 people gathered in the Cairo -> internet/mobile phone blocked**

Cyber Crime

Commission of the European Communities: "criminal acts committed using electronic communications networks and information systems or against such networks and systems".

The cyber-crime is applied to three categories of criminal activities:

1. traditional forms of crime such as fraud or forgery,
2. the publication of illegal content over electronic media (i.a. child sexual abuse material or incitement to racial hatred)
3. crimes unique to electronic networks, i.e. attacks against information systems, denial of service and hacking.

Cyber espionage

Cyber espionage can be defined as action aimed at acquiring secret information (sensitive, proprietary or classified) from private citizens, competitors, groups, governments and adversaries for political, military or financial gain by using illicit methods on the Internet or in networks, programs or computers.

- ECHELON, a signals intelligence (SIGINT) collection and analysis network operated on behalf of the five signatory states to the UKUSA Security Agreement (Australia, Canada, New Zealand, the United Kingdom, and the United States)
- ECHELON was capable of interception and content inspection of telephone calls, fax, e-mail and other data traffic globally through the interception of communication bearers including satellite transmission, public switched telephone networks (which once carried most Internet traffic) and microwave links.

PRISM (US-984XN) is a clandestine mass electronic surveillance data mining program launched in 2007 by the National Security Agency (NSA)

The exact type of data varies by provider: Email, Chat - video, voice, Videos, Stored data, VoIP, Filer transfers, Video Conferencing, Notifications of target activity, logins, etc., Online Social Networking details, Special Requests to ISP's.

Cyber espionage

SORM (System for Operative Investigative Activities) is a technical system for search and surveillance in the internet. Launched 1996 In July 1998 the system was replaced by SORM-2 to allow monitoring of the internet, in addition to telephone communications.

According to some reports, under SORM-2 Russian Internet service providers (ISPs) must install a special device on their servers to allow the FSB to track all credit card transactions, e-mail messages and web use.

SORM-3 is the newest version and is capable collect all type of information

‘Semantic Archive’ is a system, what the Russian security services and Ministry of the Interior (MVD) use to monitor open sources (i.e. the media) and the Internet, including the blogosphere and social networks.

Cyber terrorism

Cyberterrorism uses cyber-attacks against critical IT systems and their control systems. The goal of such attacks is to cause harm and spread fear among people. Cyberterrorism aims to create an impact at the national and international level alike.

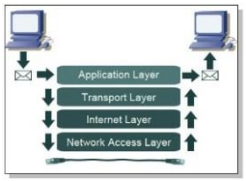
Cyber warfare

War is always widespread and encompasses all forms of warfare. Hence, cyber warfare is but one form of waging war, used alongside kinetic attacks.

Cyber attack methods and techniques

Pragmatic layer
- Cyber attack: Social engineering, Phishing, Rogueware/Scareware, Identity Theft

Semantic layer
- Cyber attack: information theft, destroying or falsifying of the information, compromising confidential information



Syntactic layer
- Cyber attack: SysAdmin assumption, DoS/DDoS attack, Drive-by Exploits, Code Injection Attacks, Search Engine Poisoning

Physical layer
- Kinetic destruction, Physical Theft/Loss/Damage
- Cyber attack: Component Corruption,

CYBER TARGETS

Cyber targets

Military targets:
- Defence industry
- Defence administration
- Armed forces

Political targets:
- Organizations, activities and infrastructure of the nation administration

Society targets:
- Critical infrastructure
- Critical information infrastructure
- SCADA-systems
- Business and industry
- Citizens

Critical infrastructure and SCADA

The Finnish point of view on critical infrastructure can be deduced from the threat scenarios which are defined in the strategy for securing the functions vital to society. They are:

- The energy transmission and distribution network,
- The telecommunications and information systems network,
- The transport logistics system,
- The community technology network,
- The food supply network,
- The financial and payment systems network,
- The health care and welfare system, and
- The safety and security network.

Supervisory control and data acquisition (SCADA) systems of the industry incorporates physical and software components which include sensors and measuring devices, telecommunications networks, drivers, communications equipment, the Human-Machine Interface (HMI) and applications.

The motives of attackers

The motive separates the cyber criminal from a cyber warrior or cyber terrorist.

Where the cyber criminal strives for financial gain, the cyber warrior fights for his military objectives and the cyber terrorist pursues his own agenda.

New threats?

Cloud services

Weather services

Satellite communication

Electricity supply

Satellite positioning

Nuclear power

Air traffic control

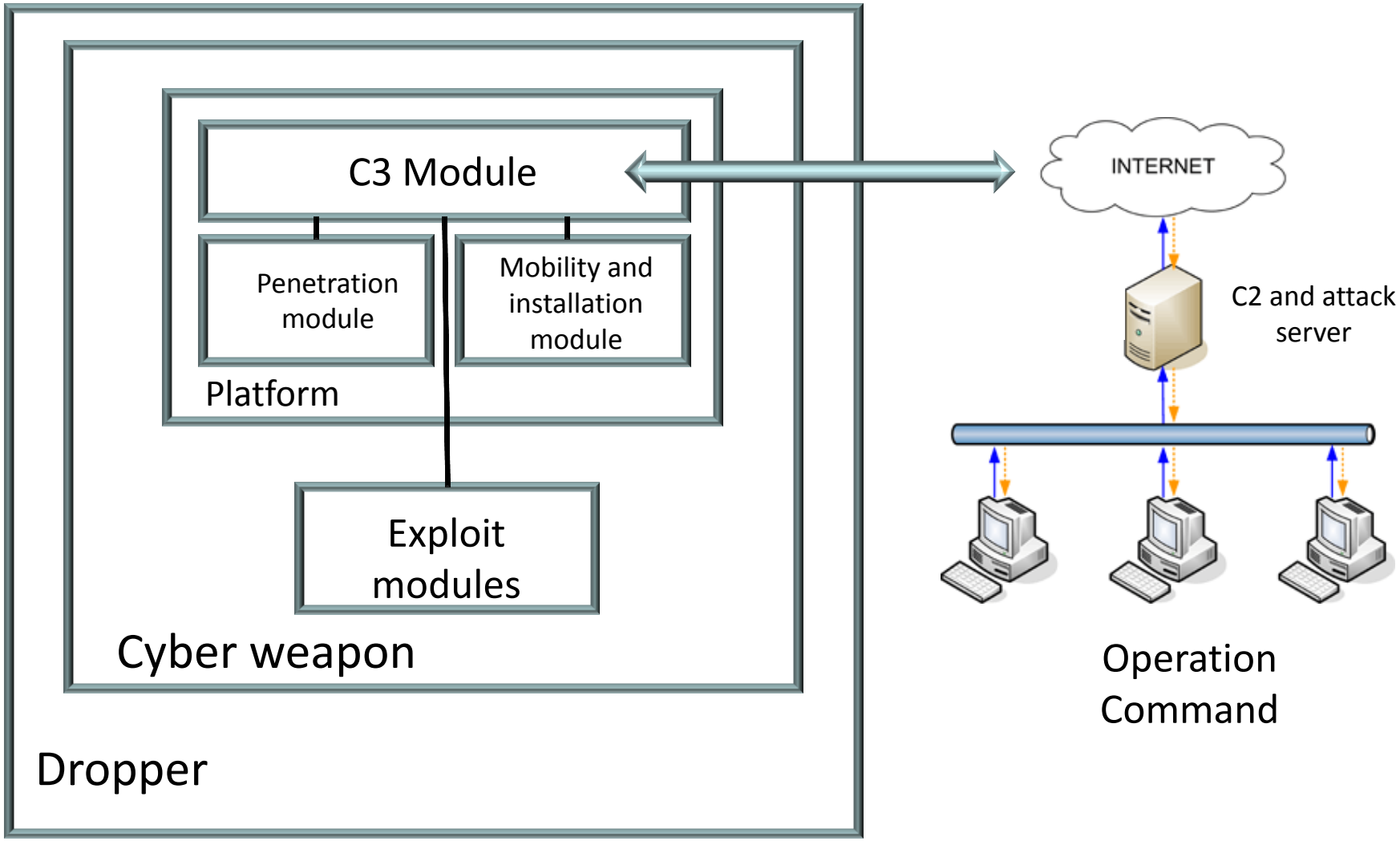
Emergency services

Automobile

Telecommunication

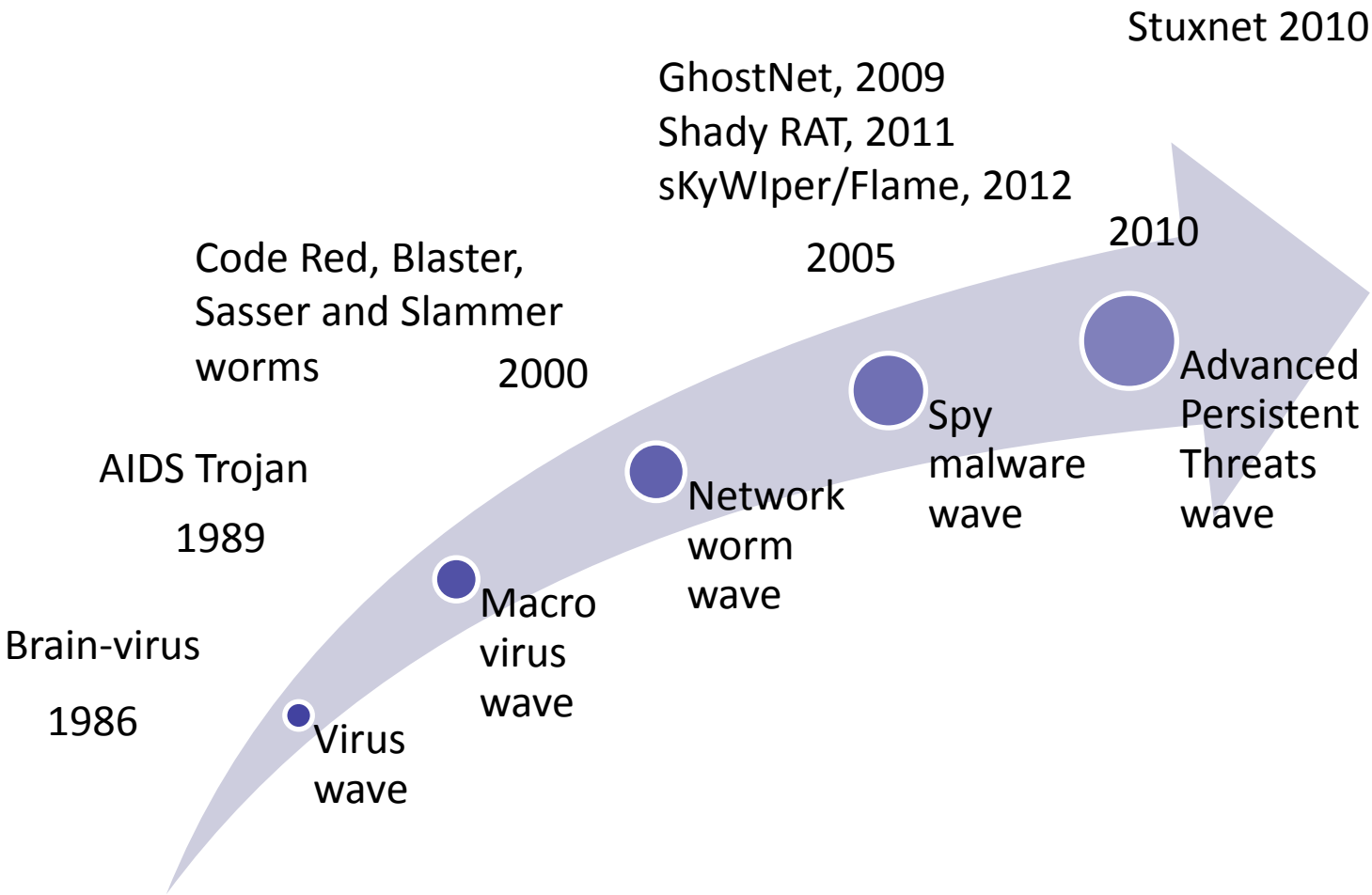
CYBER WEAPONRY

Cyber weapon architecture



Timo Kiravuo & Mikko Särelä, The Care and Maintenance of Cyberweapons in The Fog of Cyber Defence, National Defence University, 2013

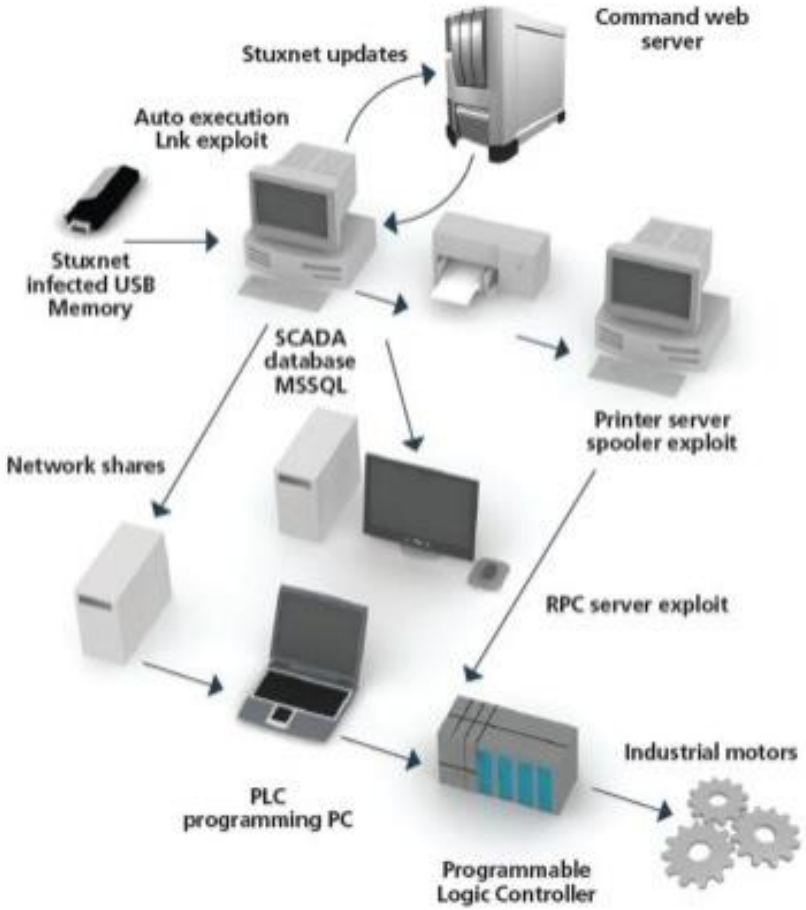
Evolution of the Cyber Weapons



Stuxnet worm

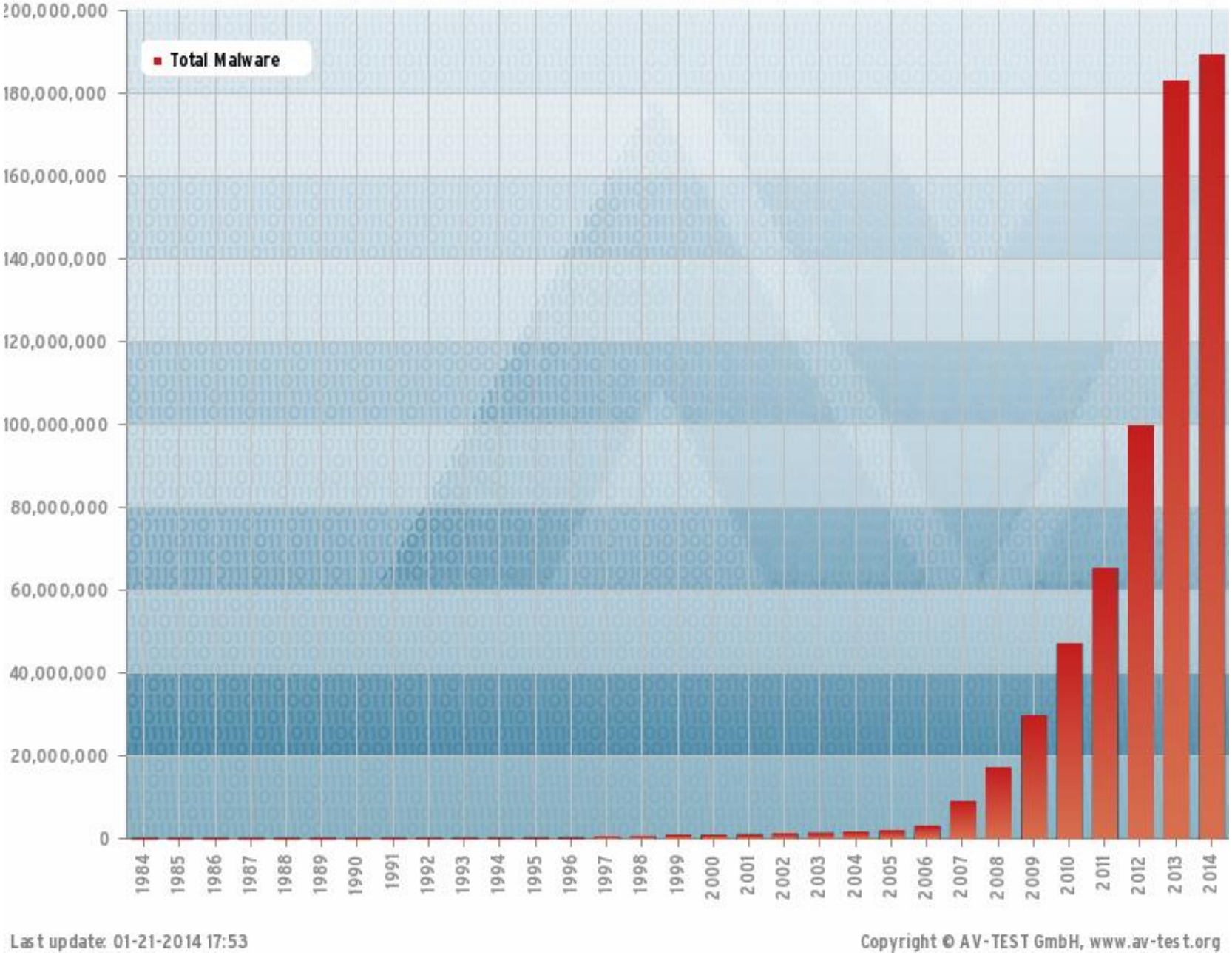
Stuxnet is a computer worm discovered in June 2010 that is created to attack Iran's nuclear facilities.

Stuxnet initially spreads via Microsoft Windows, and targets Siemens industrial control systems. It is the first discovered malware that spies on and subverts industrial systems, and the first to include a programmable logic controller (PLC) rootkit.



Stuxnet almost ruined one-fifth of the Iranian nuclear centrifuge by spinning out of control while simultaneously replaying the recorded system values which shows the normal functioning centrifuge during the attack.

Production of the Malwares



CYBER SECURITY

Cyber Security Risks

Threat + Vulnerability → Value of the risk → Countermeasures

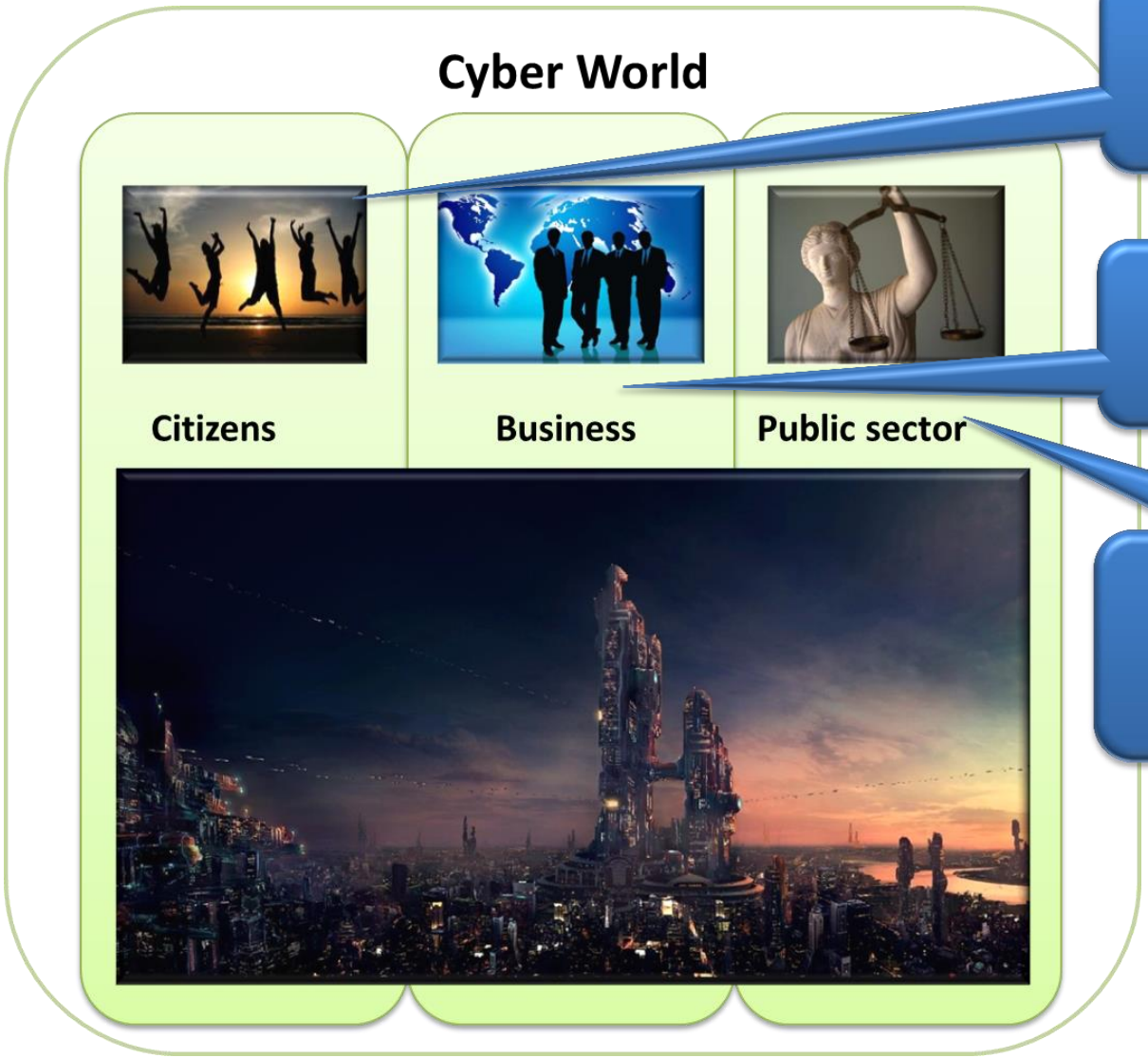
- Cyber vandalism
- Cyber-crime
- Cyber espionage
- Cyber terrorism
- Cyber warfare

- People
- Processes
- Technology

- Value
- Good name

- Regulations
- Operational culture
- Security technology

The Objectives of the Cyber Security



Reliable, open and free digital society

Reliable and secure business environment

Securing the functions vital to society

The Objectives of the Cyber Security

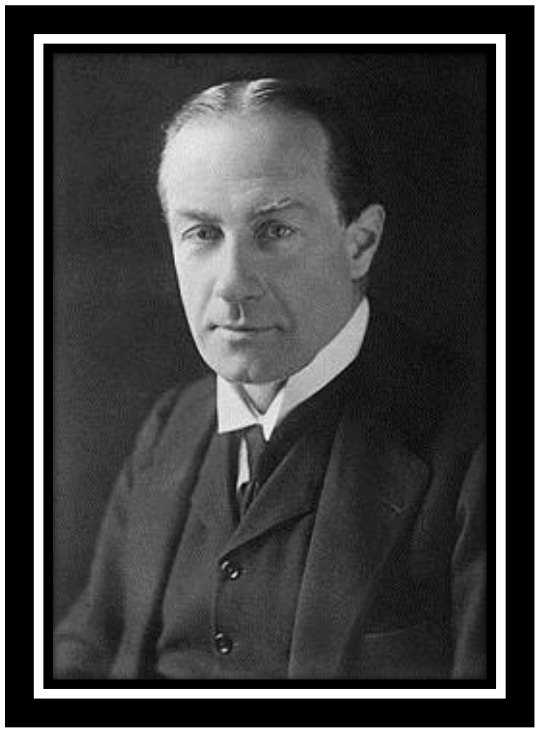
Advanced technology

Knowhow and competencies

Efficient security processes

Tolerance, contingency planning and exercises to be able to operate under cyber-attacks

” The bomber will always get through”



Prime minister **Stanley Baldwin**: "*It is well for the man in the street to realise that there is no power on earth that can protect him from being bombed... **the bomber will always get through***.”

Speech in House of Commons of the Parliament of Great Britain in November 1932.

- ”The cyber-attack will always get through”
- Cyber resilience: capability to operate under cyber-attacks