
CYBER ROAD

DEVELOPMENT OF THE CYBERCRIME AND CYBER-TERRORISM RESEARCH ROADMAP

European Commission
Seventh Framework Programme

# Metrics & Quantification of Cybercrime

## Lies, damn lies & statistics!

**Jart Armin (CyberDefcon)**


## CYBERCRIME METRICS – SHOCK & AWE

WHAT'S HAPPENING RIGHT NOW?
WHAT'S THE COST?

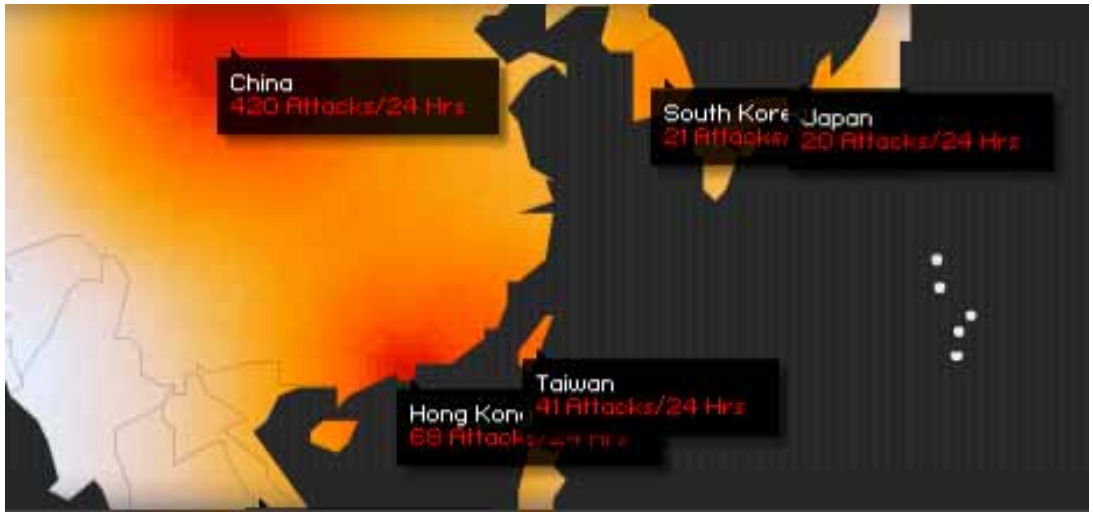
# Global Security Mapping – Today's Attacks - Europe


- # of Networks attacked
- 56% above normal

# Global Security Mapping – Today's Attacks - US


Automated scanning trojans and worms looking to infect new computers scanning randomly generated IP addresses

# Global Security Mapping – Today's Attacks – RU & Asia

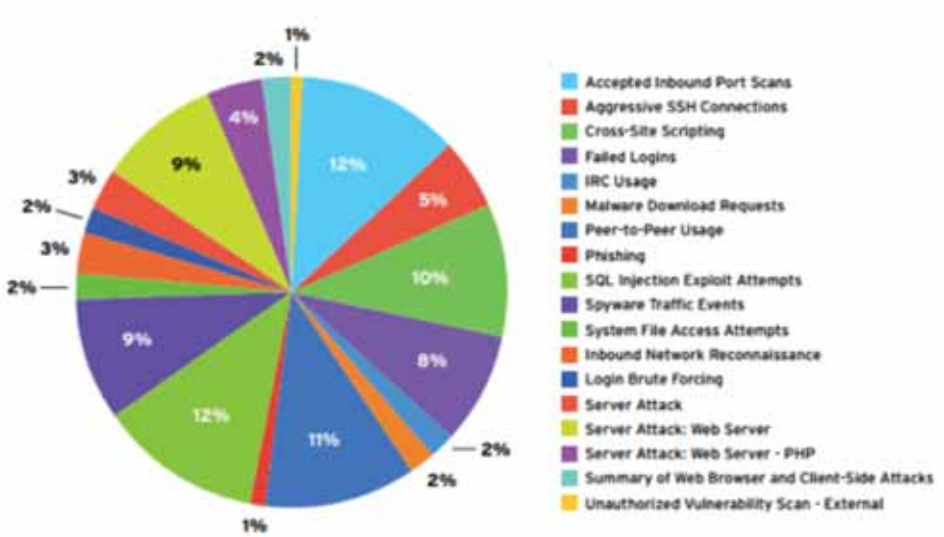



## • Based on Attack Traffic (DDoS, etc.)

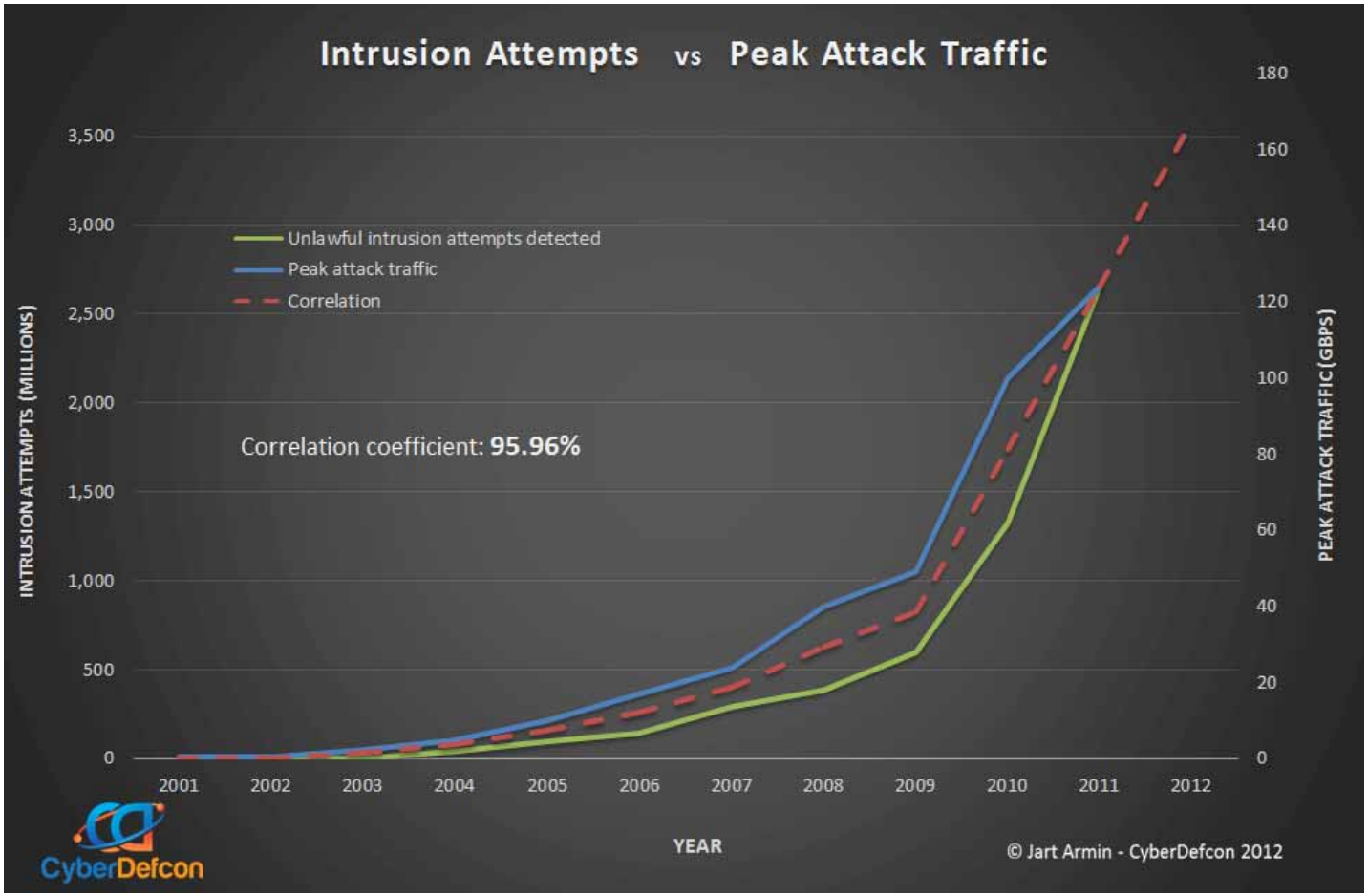
| # ATTACKS / HR | ATTACK ORIGINS | # ATTACKS / HR2 | ATTACK TARGETS |
|---|---|---|---|
| 4,429 | China | 11,032 | United States |
| 4,240 | United States | 1,454 | Hong Kong |
| 1,143 | Mil/Gov | 842 | Thailand |
| 1,084 | Hong Kong | 542 | Canada |
| 930 | Germany | 525 | Portugal |
| 525 | Canada | 306 | Spain |
| 514 | Netherlands | 276 | Australia |
| 502 | Taiwan | 265 | France |
| 386 | Thailand | 265 | Poland |
| 343 | Poland | 235 | Turkey |

| # ATTACKS / HR | ATTACKED SERVICE | PORT |
|---|---|---|
| 1,433 | ssh | 22 |
| 1,246 | domain | 53 |
| 565 | netbios-dgm | 138 |
| 824 | snmp | 161 |
| 620 | microsoft-ds | 445 |
| 951 | ms-sql-s | 1433 |
| 572 | ms-wbt-server | 3389 |
| 617 | efi-lm | 3392 |

## • Network Attacks

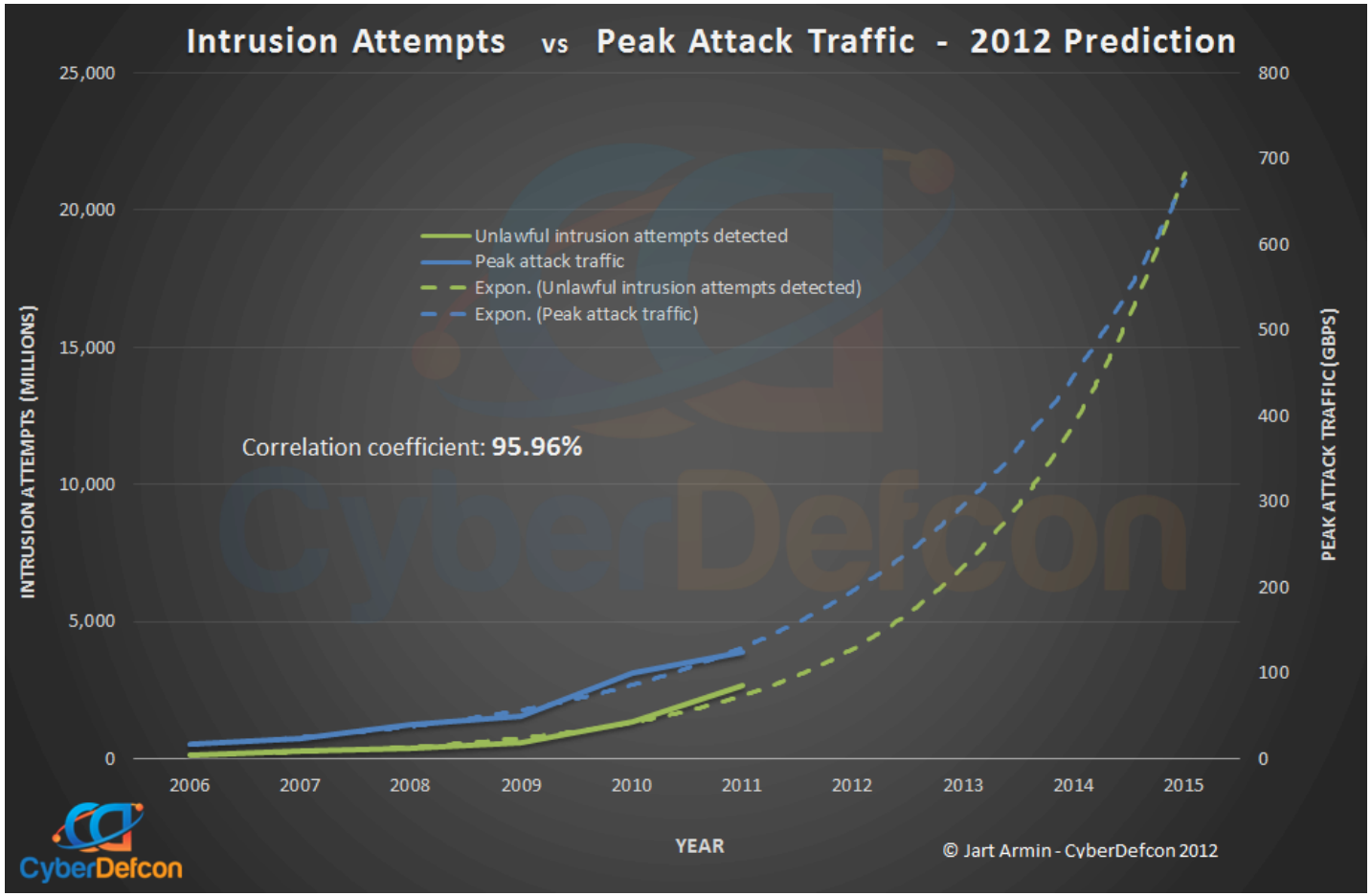



"Attack traffic," meaning countries and regions where port probes, worm, malware, viruses, and reflection attacks originate.



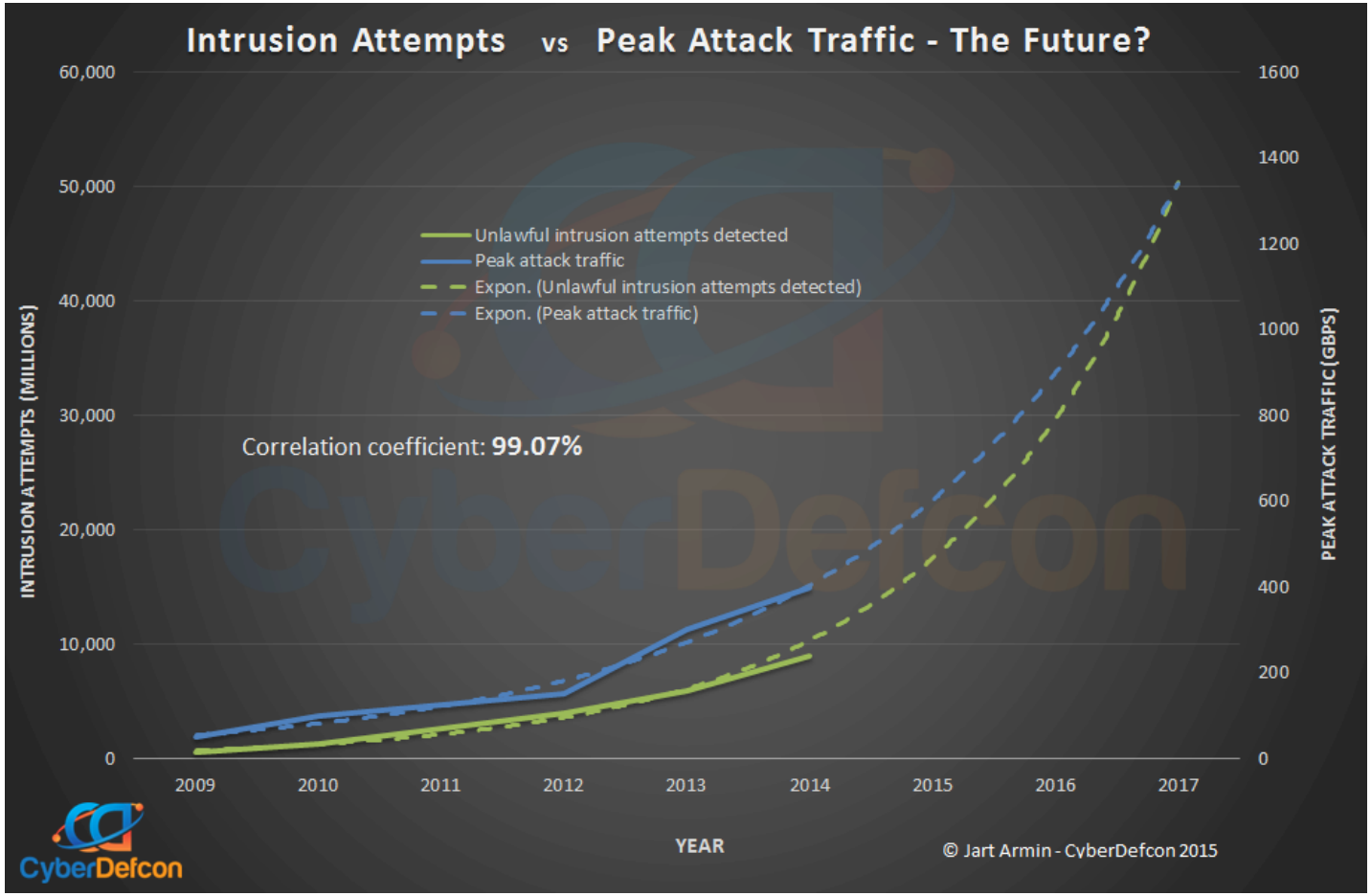

- Peak attack traffic: 2008 - just over 30 GBPs took out Georgia
- Unlawful intrusion attempts detected: - 2011 - 2.6 billion / 2008 – 0.38 billion

## Comparing “Intrusion Attempts” with “Peak Traffic Attacks" The macro effects of cybercrime

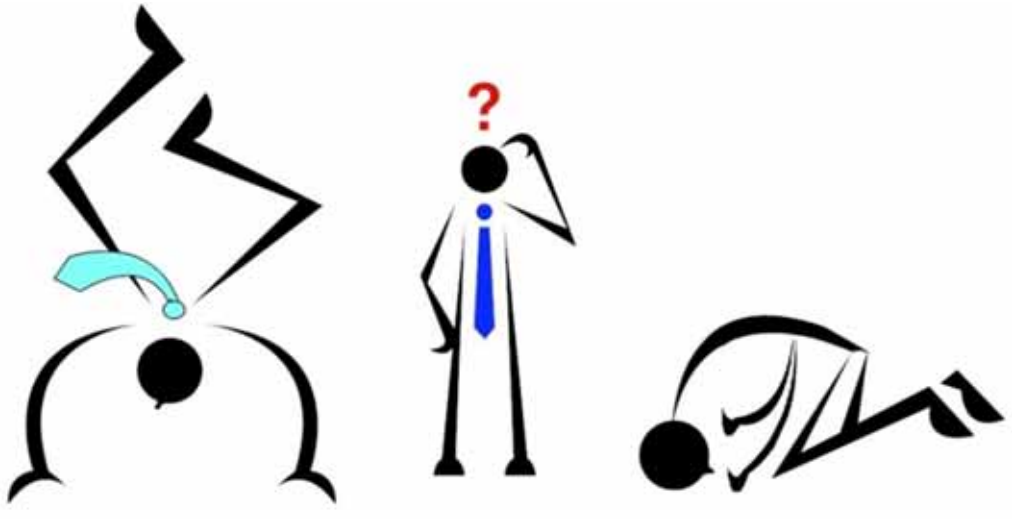



- Intruders & attackers? - probes, botnets, zombies, vulnerability scanners, scrapers, malware & worms…
- In 2009 - 2014 we observed a ***95% correlation*** **-** extrapolated the data to make predictions up until 2016

## The Near Future?



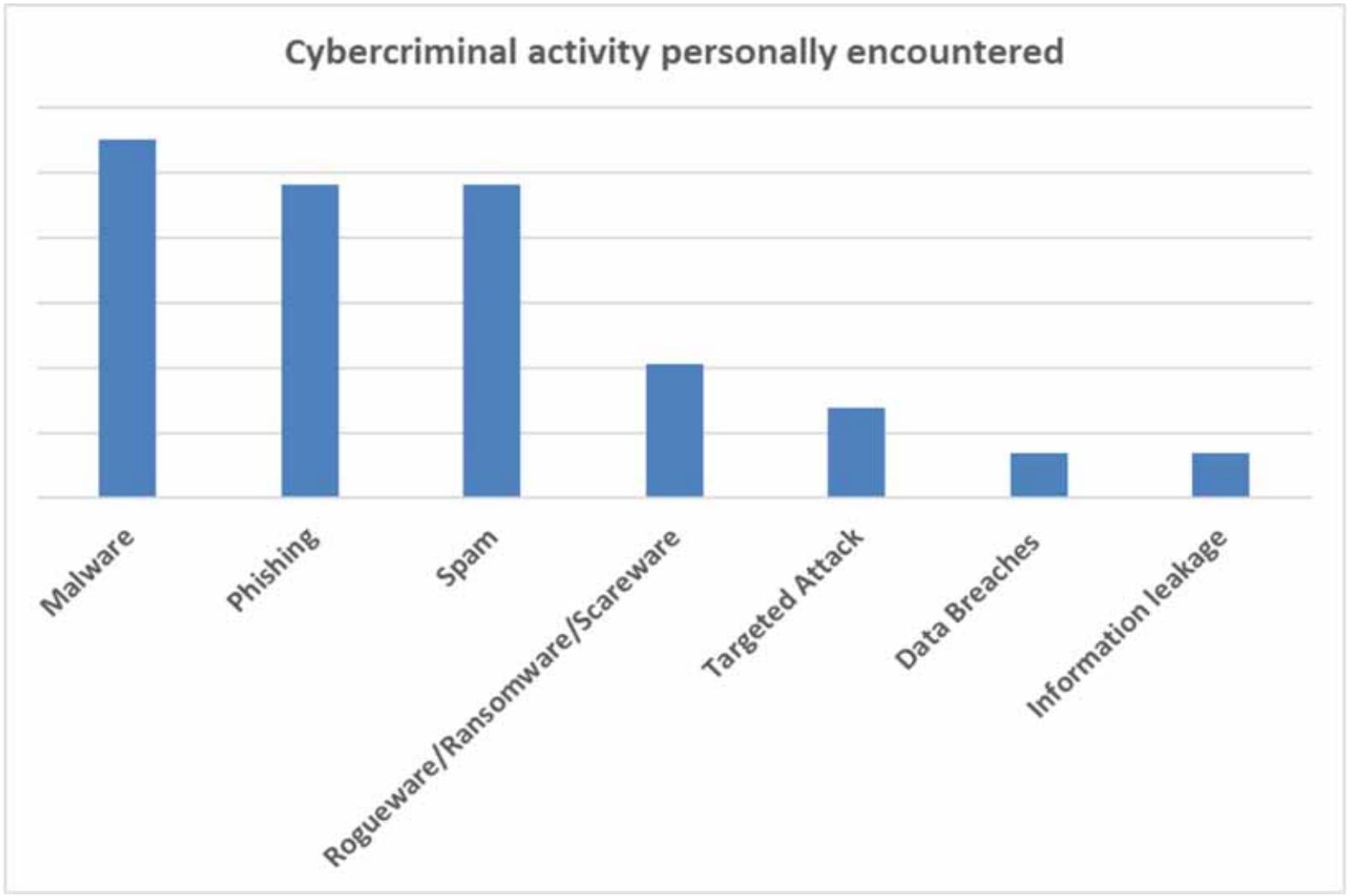

- Renewed predictions show attacks exceeding 1 Tbps by 2017
- In 2015 / 2016 against ‘BBC’ = 600GB/sec

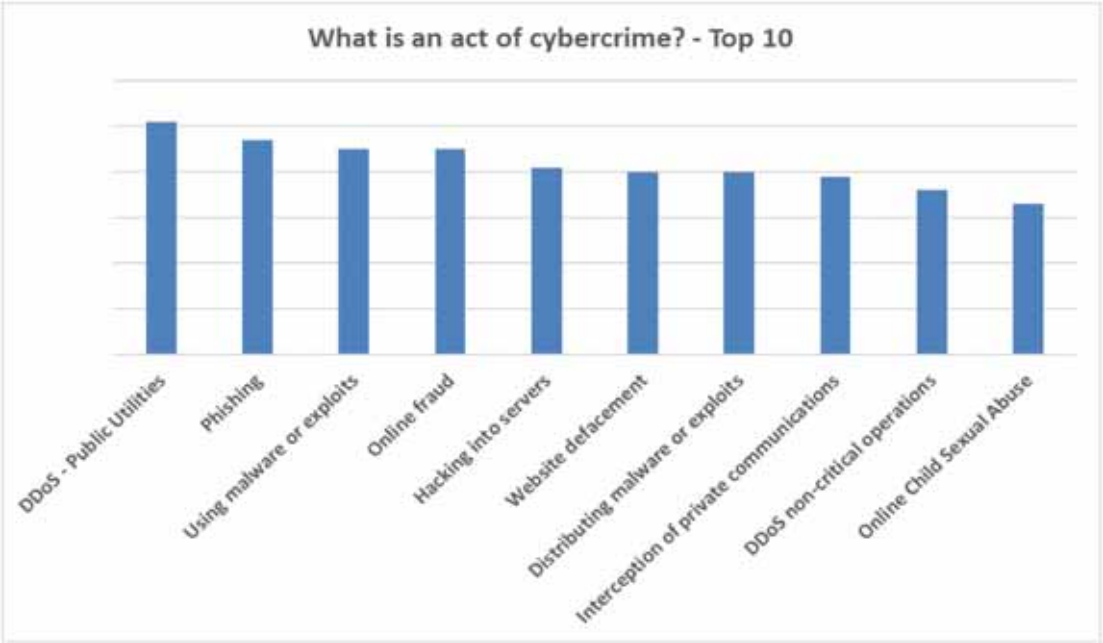


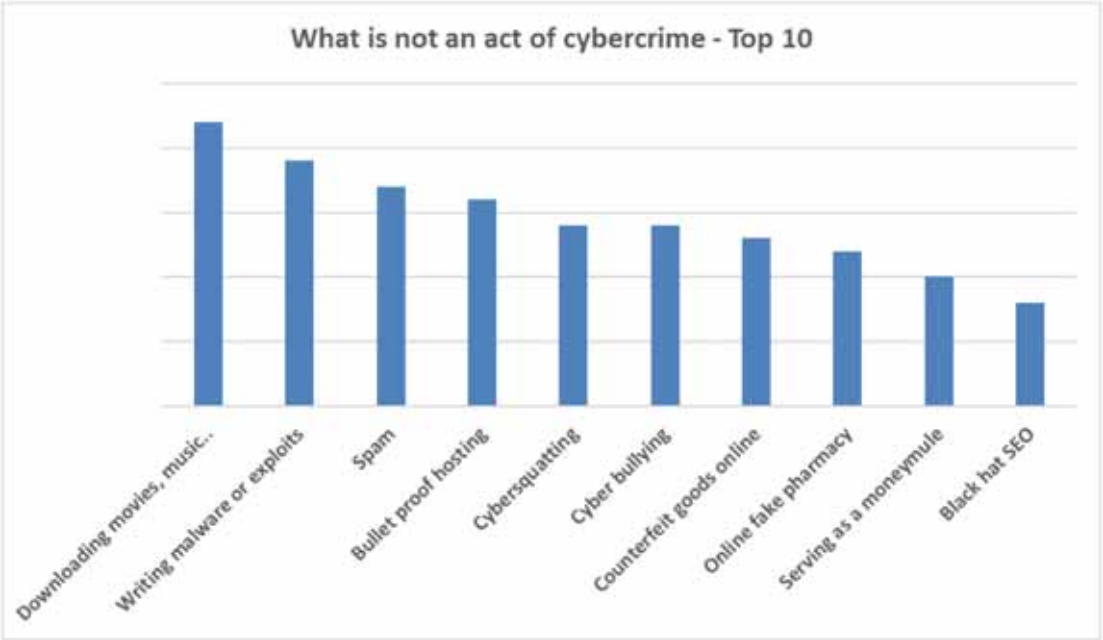
## CYBERCRIME METRICS – What do the e-citizens think?

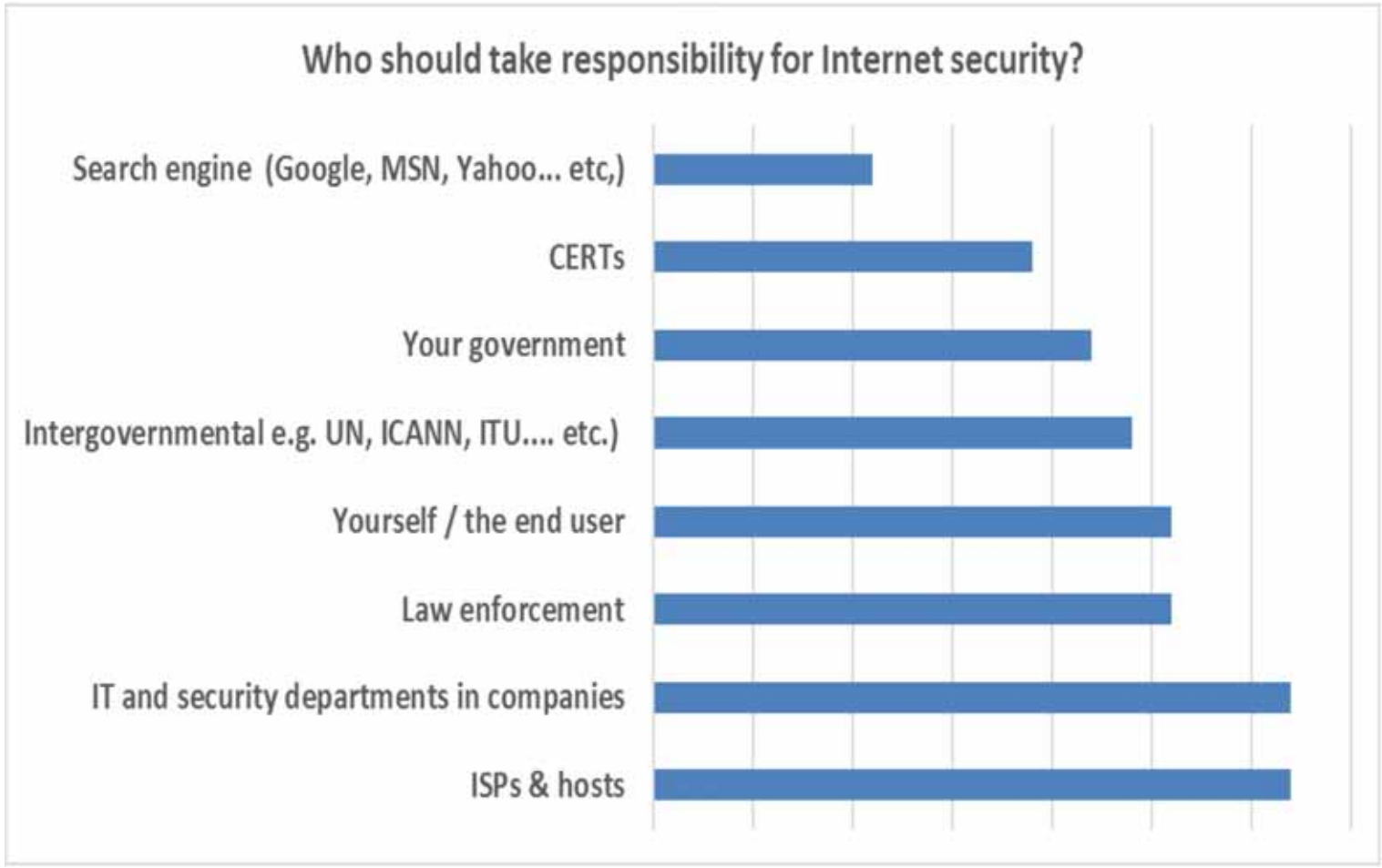
Top ➡ Down

| Population | Worldwide | Poland |
|---|---|---|
| Adults who have experienced cybercrime in their lifetime | 61% | 60% |
| Adults who experienced cybercrime in the past 12 months | 41% | 40% |
| Adults who have been victim of cybercrime and risky behaviours | 50% | 49% |
| Males who have been victim of cybercrime in their lifetime | 64% | 66% |
| People aged 18-32 who have been victim of cybercrime in their lifetime | 66% | 70% |
| Number of victims in the past 12 months (million) | 378 | 6 |

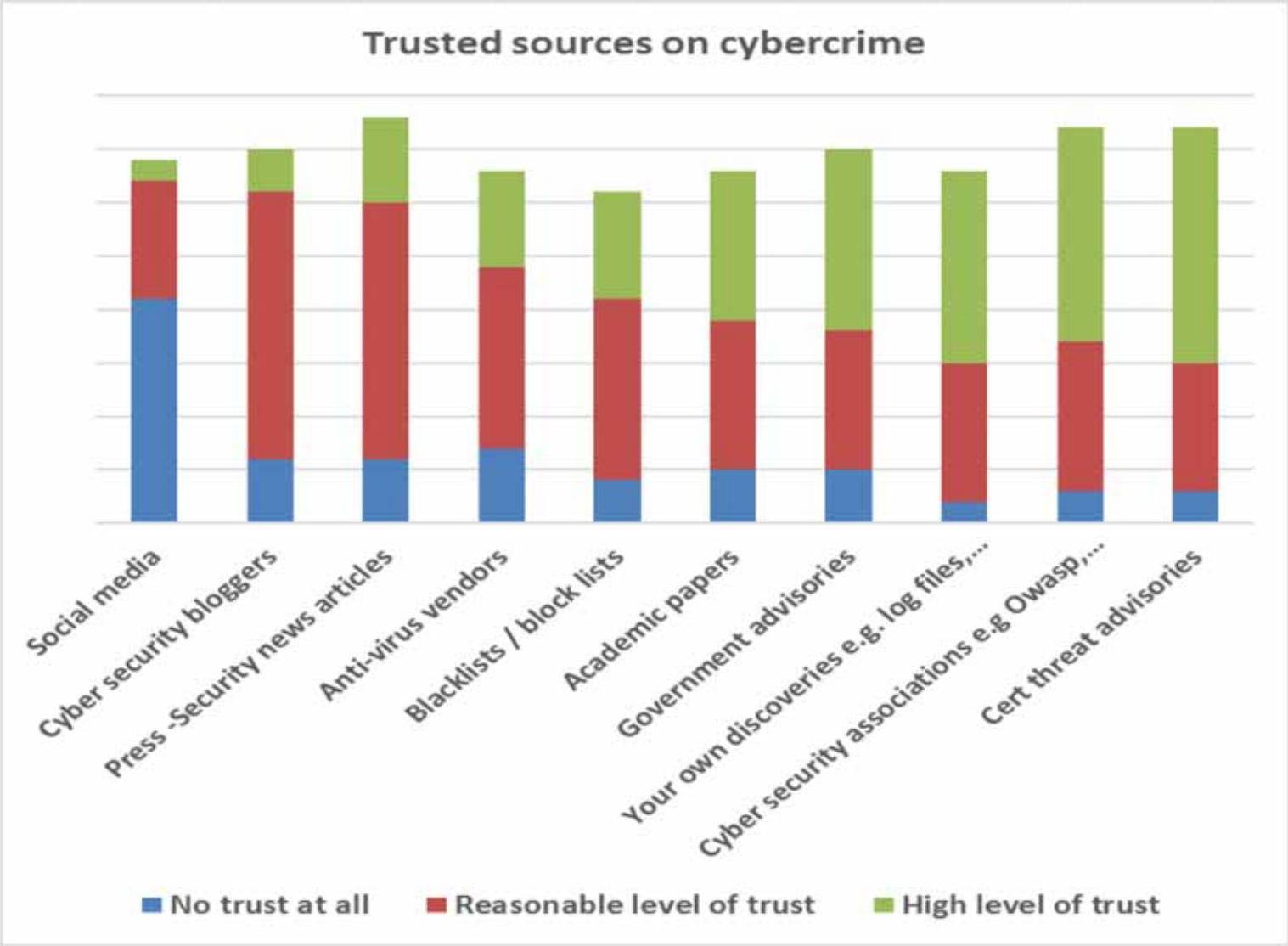

Cybercriminal activity personally encountered
Malware
Phishing
Spam
Rogueware/Ransomware/Scareware
Targeted Attack
Data Breaches
Information leakage

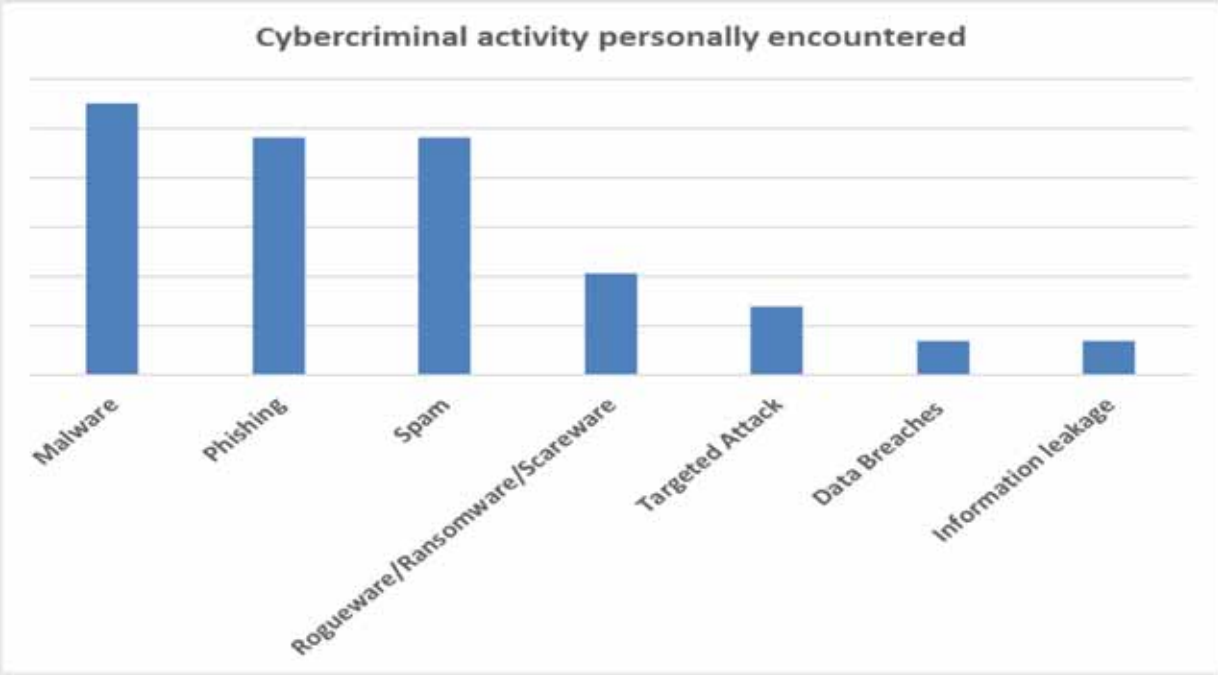

What is an act of cybercrime? - Top 10
DDoS - Public Utilities
Phishing
Using malware or exploits
Online fraud
Hacking into servers
Website defacement
Distributing malware or exploits
Interception of private communications
DDoS non-critical operations
Online Child Sexual Abuse


What is not an act of cybercrime - Top 10
Downloading movies, music..
Writing malware or exploits
Spam
Bullet proof hosting
Cybersquatting
Cyber bullying
Counterfeit goods online
Online fake pharmacy
Serving as a moneymule
Black hat SEO

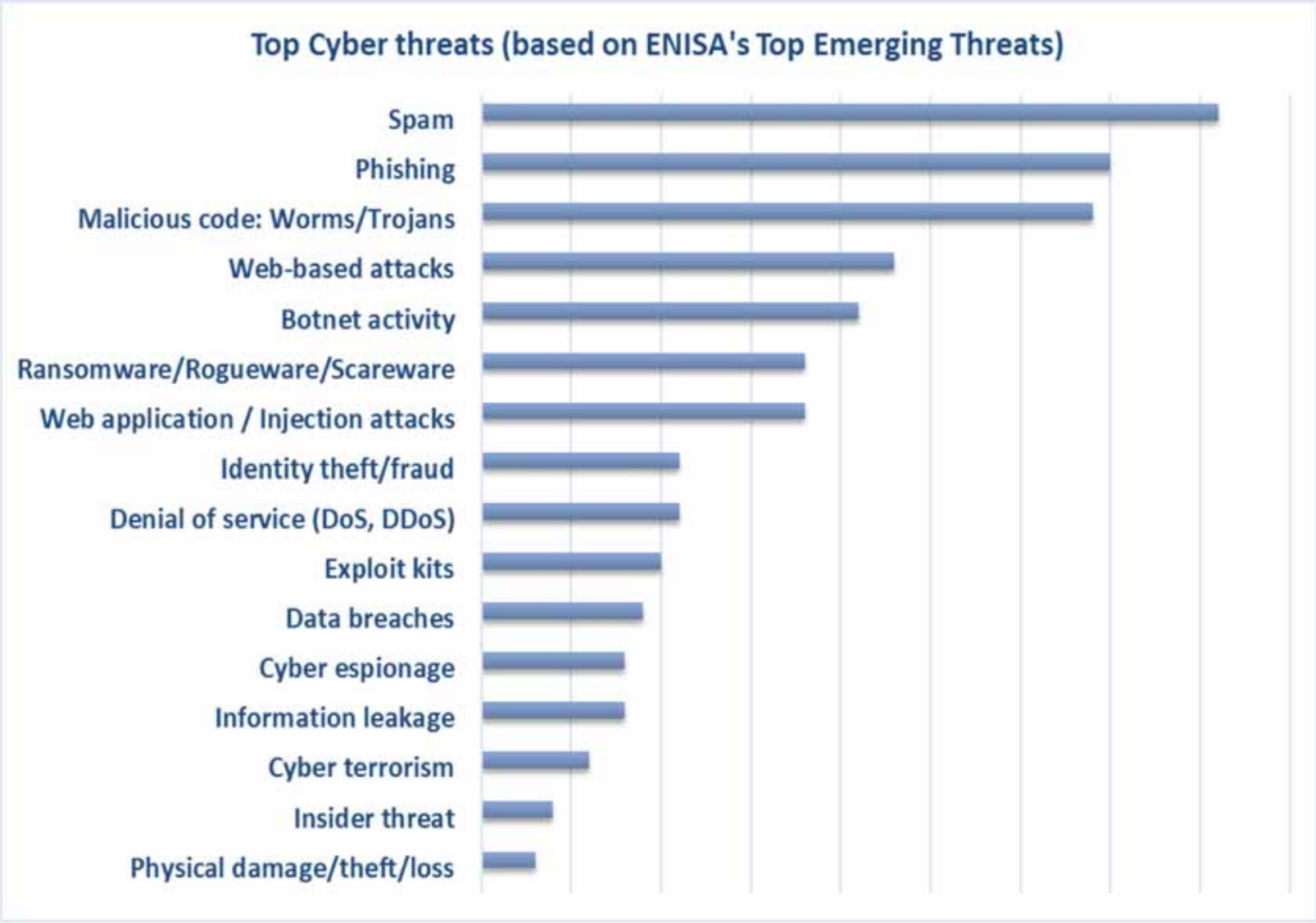

Who should take responsibility for Internet security?
Search engine (Google, MSN, Yahoo... etc,)
CERTs
Your government
Intergovernmental e.g. UN, ICANN, ITU.... etc.)
Yourself / the end user
Law enforcement
IT and security departments in companies
ISPs & hosts

# Where do you get your info from?

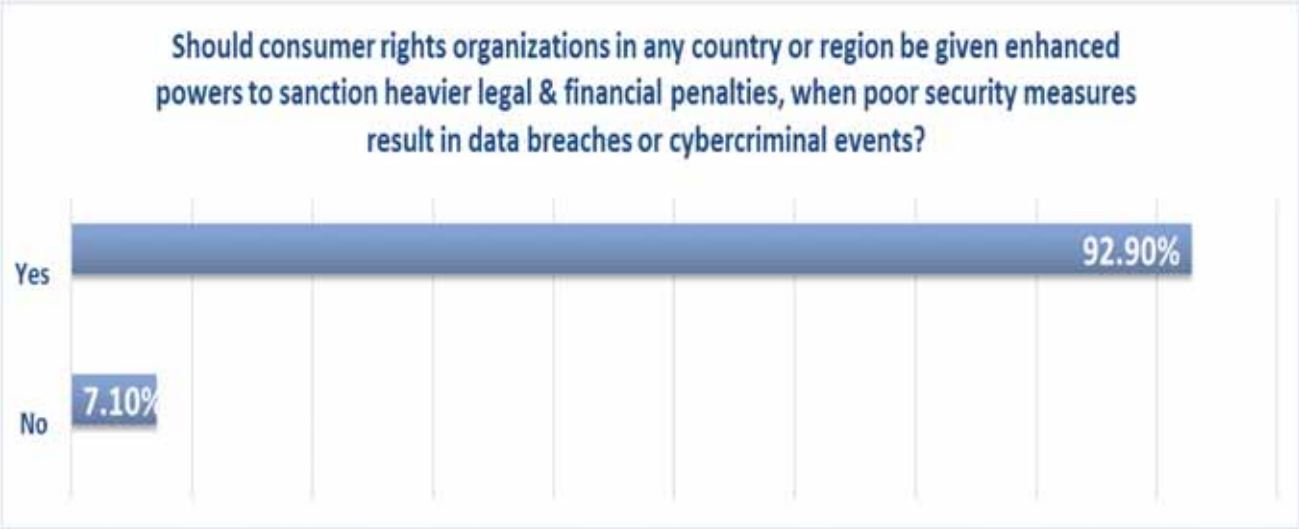



Cybercriminal activity personally encountered
Malware
Phishing
Spam
Rogueware/Ransomware/Scareware
Targeted Attack
Data Breaches
Information leakage


Have you lost control of your personal data online?
Yes
65.50%
It's time to take control back
17.20%
No
10.30%
It's not important if control is lost
6.90%

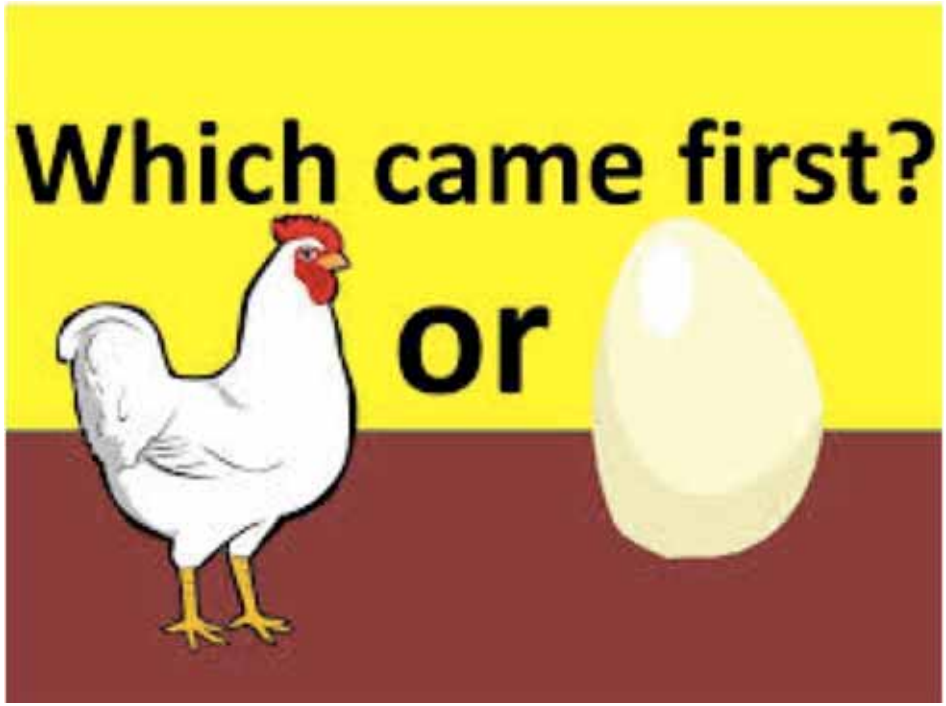

Top Cyber threats (based on ENISA's Top Emerging Threats)
Spam
Phishing
Malicious code: Worms/Trojans
Web-based attacks
Botnet activity
Ransomware/Rogueware/Scareware
Web application / Injection attacks
Identity theft/fraud
Denial of service (DoS, DDoS)
Exploit kits
Data breaches
Cyber espionage
Information leakage
Cyber terrorism
Insider threat
Physical damage/theft/loss


How much time was lost as a victim of cybercrime?
22.7%
36.4%
27.3%
13.6%
< 4 hours
5 - 8 hours
9 - 24 hours
25 hours +


Should consumer rights organizations in any country or region be given enhanced powers to sanction heavier legal & financial penalties, when poor security measures result in data breaches or cybercriminal events?
Yes
92.90%
No
7.10%

# Top 6 From stakeholders

1. Education in cybercrime prevention
2. Cyber security management
3. Laws and policies on cybercrime
4. Risks & effects of cybercrime
5. Economic impact of cybercrime
6. Cybercrime definitions and classifications



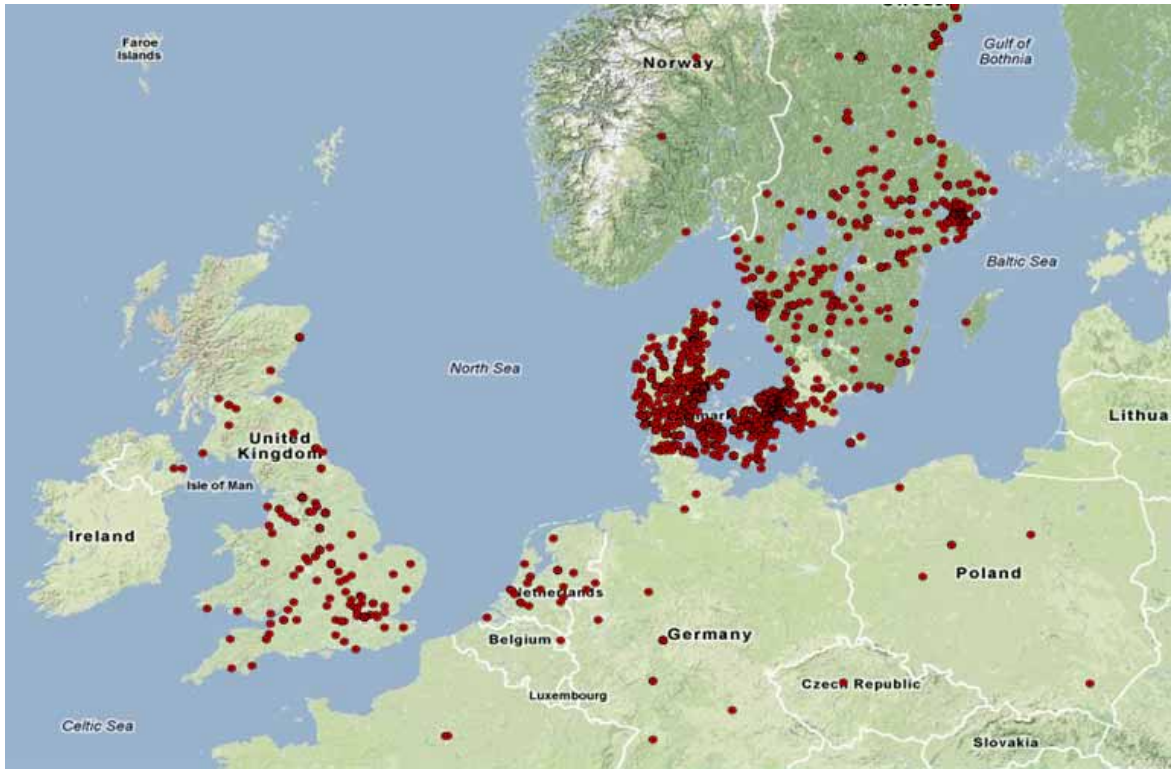

# WE TALK ABOUT RESEARCH TOPICS, BUT WHAT SHOULD BE THE BUDGET?

What should the EU spend on cybersecurity research and why?

## CURRENT ESTIMATES , HOW MUCH R&D?

- The annual cost to the global economy from cybercrime is more than **€300 billion Euros**
  McAfee, Intel, & others
- Cost of cybercrime for the **EU 0.4% of its GDP** = **€13 billion / annum** (2014 IMF)
- Cybercrime market globally itself of **€15 billion / annum**
- Market for security products and services **€50 billion / annum**
- Compare with EU **0.0005% of its GDP = € 150 million / annum** on Cybercrime R&D e.g H2020?
- Should be EU **0.0025% of its GDP = € 750 million / annum** on Cybercrime R&D = ?

- = **A BETTER RETURN ON INVESTMENT (ROI) FOR EU - So end result (5 years) reduce** Cost of cybercrime for the **EU to €7 billion / annum & develop a €5 billion / annum cyber security industry (10% of the world market)**
- **Example 'SISSDEN' project aim to reduce cost of cybercrime in EU by € 100 million / annum & in 5 years develop an EU company earning €25 million / annum**




# CYBERCRIME METRICS & THREAT DATA (THEORY) – EPIDEMIOLOGY

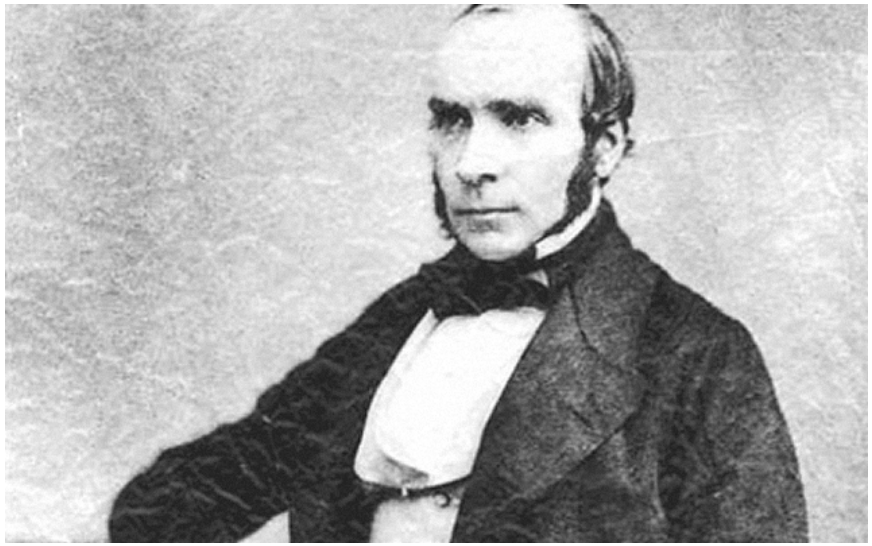
Cholera / Ebola (Disease)

↓

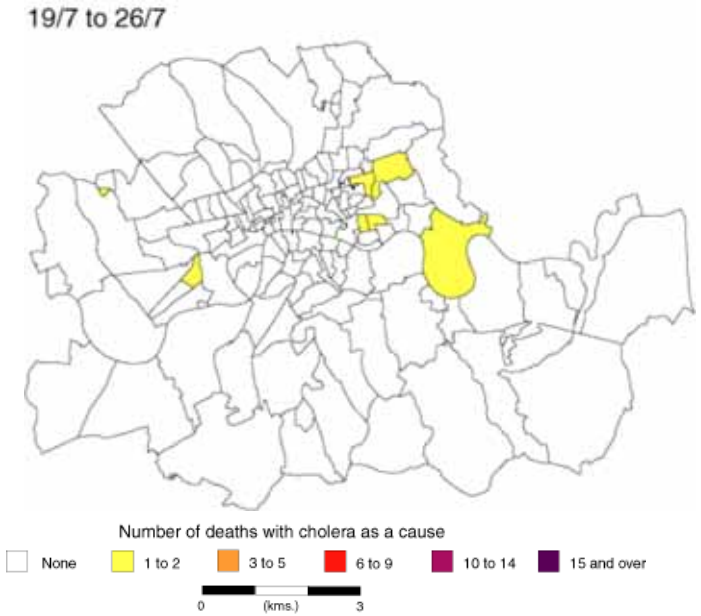
BankTexeasy / Tilon (Banking Malware)

CyberDefcon

## Dr John Snow - Epidemiology



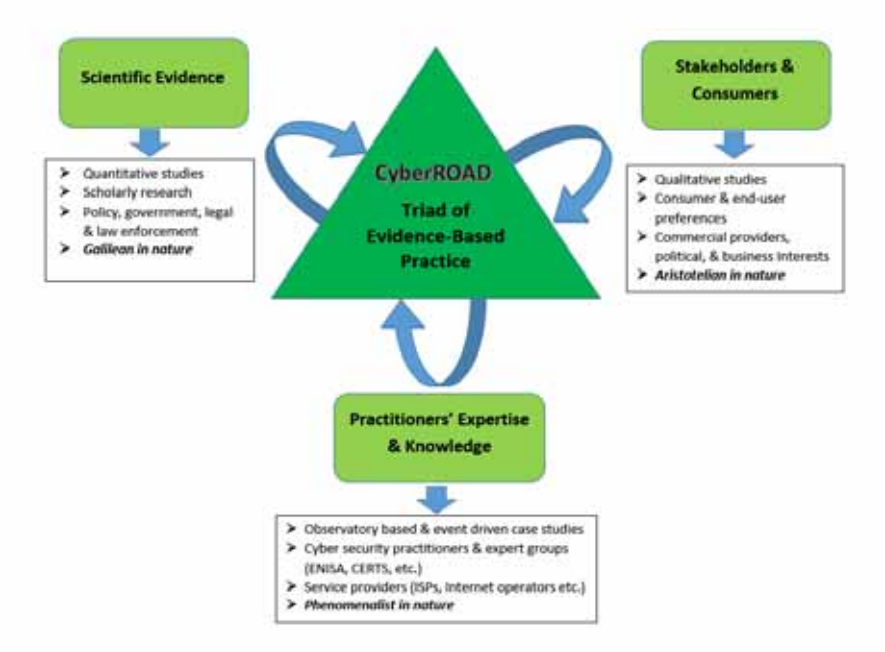
## Cholera epidemic of 1854 London




## Cybercrime & Cyber Threats – Public Health

- **Epidemiology**: the science that studies the patterns, causes, and effects of health and disease in defined populations.
- Cholera, Bubonic Plague, Aids, Ebola!
- Ransomware, Stuxnet, Zeus, Conficker, BlackEnergy…. + DDoS, Spam…
- Cybercrime & Cyber Threats = the public health analogy – an epidemiological approach. – i.e. patterns & causes
- Just to note: The science of: Public health & epidemiology = >150 years – Cybercrime & Threat Data research = < 10 years
- Policy decisions and evidence-based practice by identifying threats and targets for prevention.

## Triad of Evidence-Based Practice for Cybercrime & Threat Data




## A methodological approach

- ***CyberROAD Triad of evidence-based practice***
- to validate all the choices made in cybercrime metrics and threat data

- on the basis of the **available data and interaction of the data** coming from:
  - A. scientific evidence
  - B. practitioners and expertise knowledge (e.g., industry)
  - C. stakeholders and consumers

- This is useful for:
  - D. guaranteeing that the underlying assumptions agree with the available evidence
  - E. defining precise metrics

- Long-term goal of the proposed methodology: making the fight against cybercrime and cyber threats an **empirical science**

# WHAT ABOUT CYBERTERRORISM?


"We are in a 'technology arms race' with terrorists **recruiting** an **army of hackers** to their cause"
– *The Guardian*

"If our **electricity supply**, or our **air traffic control**, or our **hospitals** were successfully **attacked online**, the impact could be measured not just in terms of economic **damage** but of **lives lost**."
– *The Independent*

"[The Paris attacks] have added... **urgency** to **countering** the **extremism** problem. Dealing with material online is the first item on the agenda."
- *EU's counter-terrorism chief*

## Water Utilities Threats

**Status:**

Utilities (such as water, gas and electricity) are managed by automated system.

Industrial control system (ICS) threat landscape has evolved significantly over the recent years.

**Cyberterrorists objectives**:

- aim at disrupting the water delivery service
- prevent people from getting water
- poison the water distribution network (cause disease or death)
- targeting wastewater treatment plants to cause ecological disasters.

## Wearable Devices Threats

**Status:**

Wearable devices (e.g. health implant) rely on remote database servers or computer clouds to store and retrieve information

**Cyberterrorists objectives**:

- theft of sensitive information
- physical harm to human agents (a.k.a. cyber murder), e.g. by tampering with a health sensor used for heartrate monitoring and causing an heart attack.

source: http://sourcebits.com/app-development-services/mobile-app-development/

## Countermeasures & Research Gaps

Improved authentication and anonymization

Improved monitoring of critical materials we all depend on, e.g. water

Advanced malware defence and shielding.

Behavioural-based intrusion detection system.

Crypto-analytical algorithms.

Infrastructures for attack simulation.


## Cleaning up the Garbage in Cyber Space – why?

“The cleaner a nation’s national cyberspace, less attacks on its national infrastructure & lower numbers of cybercrime victims”

**Disease Control? Epidemiology…?**


## Threat Data and Analysis…… Big Data

"Prevention of the disease is better than treatment **or** control"

Thanks for listening

## General Cyber Metrics

| |
|---|
| 2.8 Billion users of the Internet (~39% world population) |
| Over 100 billion emails processed / day |
| 959 million websites — 39 million / month added (4%). |
| IP addresses - IPv4 = 4,294,967,296 ($2^{32}$) - IPv6 = of 2128 |
| 1.4 million browser user agents - bots |

| Measuring malicious events | Source |
|---|---|
| 85% of processed emails are spam | Barracuda |
| 7% of all urls maliscious | Barracuda |
| Public Block List count: 1,018,203,532 IP addresses | Spamhaus |
| 250 million in total identifiable malware | AV-Test Org |
| 200,000 new malicious programs registered | AV-Test Org |
| 1 million+ measurable cyber-attacks every day | Akamai |
| 330 active Real-time Blackhole Lists (RBL & DNSBL) | Hostexploit |
| € 5.9 million is the average annualized cost of data breaches | Ponemon Institute |
| 10.4% net increase cost of data breaches over the past year | Ponemon Institute |
| 250,000 – 500,000 malicious binaries / day | Shadowserver |
| ~280 million malicious binaries collected | Shadowserver |
| 6 / 10 million unique IP's sinkholed / day | Shadowserver |
| 900,000 malicious domains / day | Shadowserver |
| 500 of 52,000 ASNs worldwide (4%) account for 85% of malicious activity | Hostexploit |

## Considerations for Our Digital Future?

What?

- Quantification, what are the metrics? What are we dealing with?

- Cost of cybercrime for the **EU** **0.4% of its GDP** = **€13 billion / annum** (2012 IMF)

- Compare with EU **0.0005% of its GDP** = **€ 150 million / annum** on Cybercrime R&D e.g H2020

- So what proportion of EU research budget should go to reducing this cost, i.e. what should be researched?

The garbage?

- Infrastructure: Misconfigured, outdated, open resolvers - Update the systems a legal responsibility?

- Tools: Viruses, Malware, Botnets & the Zombies

**Cleaning up the garbage, who is responsible?**
**Even more specific who is going to pay for the clean up?**