
Munich Personal RePEc Archive

# Cybersecurity in the perspective of Internet traffic growth

Kox, Henk L.M.

CPB Netherlands Bureau for Economic Policy Analysis

July 2013

Online at https://mpra.ub.uni-muenchen.de/47994/
MPRA Paper No. 47994, posted 05 Jul 2013 04:06 UTC

# Cybersecurity in the perspective of Internet traffic growth

**Henk L.M. Kox** [a)]

**June 2013**

Abstract:
Private and public concern about digital security, cybercrime and data privacy is growing the last few years. If Internet-related markets are flexible enough to cope with security concerns, given time, one would expect that - per unit of Internet traffic - the number and costs of cybersecurity incidents fall over time. This paper is a first attempt to assess empirically whether overall Internet traffic growth has grown faster than the number of cybersecurity incidents. The conclusion is that, overall, the Internet has over time has become a safer place when measured by the number of security incidents per unit of transmitted data. The implication is that the current surge in reported cyberincidents is primarily driven by the growth in scale and pervasiveness of Internet communication exchange. There are a number of caveats that should be taken into account, but for this more consistent and reliable cybersecurity statistics would be required than are available at present.

Keywords: Internet traffic, cybersecurity, timetrend safety Internet

[a)] Contact: Henk L.M. Kox | CPB Netherlands Bureau for Economic Policy Analysis | email: h.l.m.kox@cpb.nl.
Only the author is responsible for the contents of this paper; the contents are not necessarily supported by CPB Netherlands Bureau for Economic Policy Analysis.

# 1. INTRODUCTION

Almost daily now, we get newspaper reports about data leaks, spreading of computer malware, botnets, DDoS attacks on banks and other firms, stealing of digital identities, hacking of databases, and other cybercrime incidents. Private and public concern about digital security, cybercrime and data privacy is clearly growing the last few years. Cybersecurity is defined here as the perceived level of digital data protection and data integrity related to the Internet communication channel. In 2012, the European Commission commissioned a large survey among EU citizens to assess their experiences with and perceptions of cybersecurity issues. Across the EU countries, 8 per cent of Internet users say they have at least once been a victim of digital identity theft.[1] For the EU as a whole, 38 per cent of Internet users have recently received fraudulent emails asking for money or personal details (including banking or payment information). Between 70 and 90 per cent of Internet users were convinced that the risk of becoming a victim of cybercrime has increased during the preceding year (EC, 2012: 50).

The public debate on cybersecurity lacks analytic clarity because all sorts of problems in which computers or the Internet play some role, tend to be lumped together. Moreover, the debate tends to forget that the number of security incidents simply rises in proportion with the growth of Internet traffic.

Intuitively, many people would expect that Internet-related markets will be flexible enough to cope with current security concerns, given time. If this is true, then the number and costs of cybersecurity incidents per unit of Internet traffic should fall over time. Looking backwards, this raises the question what happened with the number of cybersecurity incidents per unit of Internet traffic of ver the past period. To my astonishment I could not find any serious empirical attempt to measure this. The availability, consistency and reliability of current cybersecurity statistics is, undoubtedly a serious explanatory factor for this hiatus. The present paper is a modest first attempt to assess quantitatively whether cybercriminality and other Internet-related security incidents have grown faster than overall Internet traffic growth using the best possible statistical data that I could obtain.

The structure of the paper is as follows. Section 2 provides stylised facts on several dimensions of Internet growth. Section 3 distinguishes four categories of Internet-related security incidents. Section 4 offers the statistical analysis of the central question based on the seven time series of security incident indicators. Forced by lack of data this analysis is entirely based on indicators of the number of incidents. The now available data do not allow to quantify the costs per type of security incident. Section 5 concludes on the basis of the available evidence.

# 2. INTERNET GROWTH: STYLISED FACTS

This section offers a taxonomy of security incidents, and it reviews stylised facts their about cybersecurity in relation to the growth of the Internet as a communication medium. The section deals with security threats that can be attributed to private households, firms and cybercriminals, and that are driven by mainly economic motives. This includes industrial cyber espionage, but it excludes the

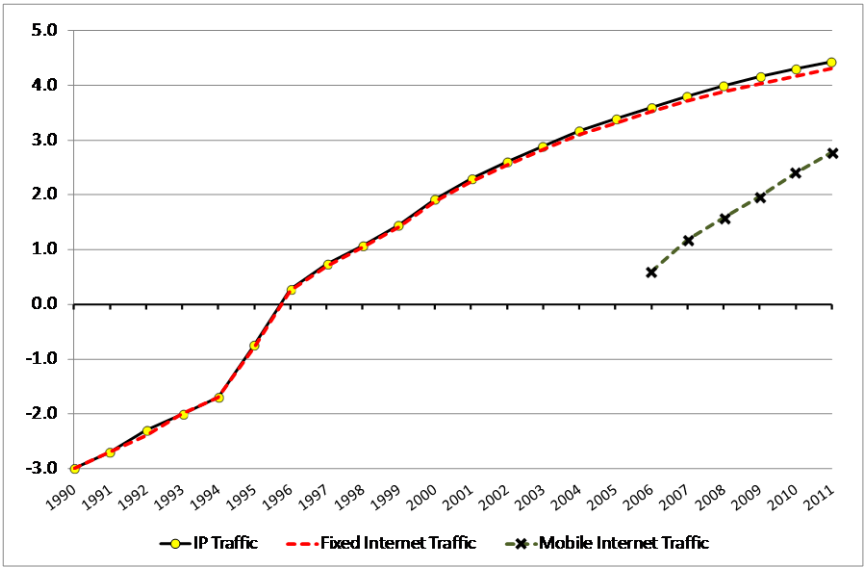
[1] The national differences around this average are substantial. For comparison: in the Netherlands it is 7%, in Germany 6%, and in Denmark 4%, but in Belgium and the UK it is, respectively 10% and 12% (EC, 2012: 48).

use of Internet for cyber-warfare purposes by states and secret services.

The Internet as we know it today has developed from a US defence research project in the 1960s that aimed to design a shock-resilient communication system. It developed further as a project of the US National Science Foundation for research communication between university computers in the USA. In 1990 the Internet was officially opened to commercial ventures. It has since then had an astounding growth by nearly any measure. The total volume of Internet traffic between 1990 and 2011 has grown by about 100 per cent per year, i.e. it doubled each year, although since 2003 the growth rate is gradually falling. This can be seen in Figure 1. Most of the traffic growth came from traffic through fixed lines, but since 2006 traffic through mobile access devices is rapidly increasing its share as can be seen in the Figure 1.

**FIGURE 1 GROWTH OF INTERNET TRAFFIC VOLUME IS SLOWING, 1990-2011**

*(petabytes per month. log scale)*




Note: The traffic volume is measured in petabytes ($10^{15}$, one million gigabytes) per month.
Source: constructed from CAIDA data, cf. CAIDA (2011)

At the descriptive level, the growth of Internet traffic could probably be decomposed into the following growth elements, even though such studies are not yet available:[2]

(a) the number of people that have access to Internet;
(b) the number of devices through which people have access to Internet;
(c) the average time per day that these devices are used;
(d) the average number of computer applications (per access device and per user) that require Internet access;
(e) the average data-exchange intensity per computer application (applications using real-time data or streaming video images generate more traffic volume than simple applications like email).

[2] Cf. Odlyzko (2004). A companion paper (Kox, 2013) presents a formal gravity model for analysing the determinants of Internet traffic growth. Empirical studies of Internet growth and its determinants are still in their infancy, mostly because of the absence of consistent and reliable data series.

At the analytic level the growth of Internet traffic per region can probably be explained in terms of several factors, like GDP growth, population size, GDP composition, network quality, income per capita, stability of political and economic institutions, and cybersecurity.

The number of Internet users increased from roughly 361 million in 2000 to 2.4 billion users in June 2012 (Table 1). Asia accounted for about half of the absolute growth in Internet users between 2000 and 2012. Asia now accounts for 44% of all Internet users, Europe has a 21% share,[3] and the USA and Latin America each have a 11% share. Internet users in OECD countries nowadays therefore represent a minority.

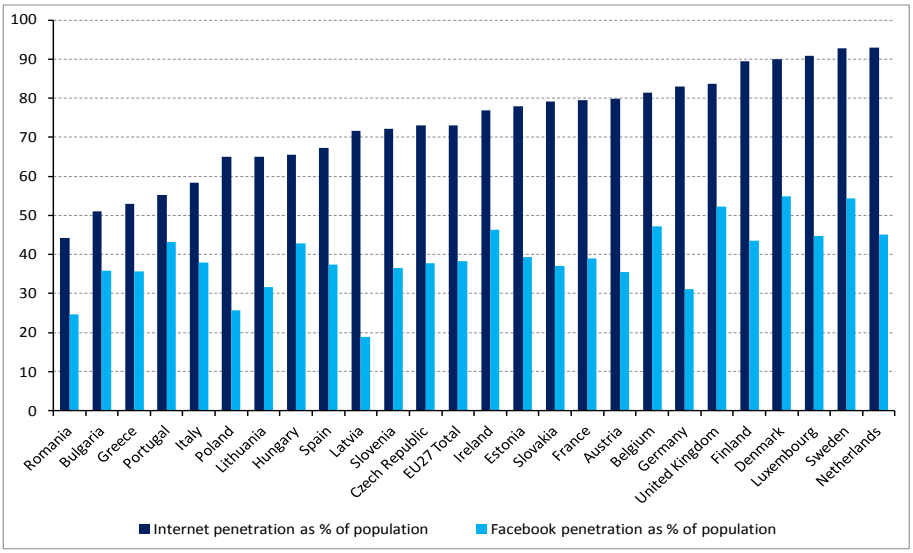
**TABLE 1 GROWTH IN NUMBER OF INTERNET USERS AND INTERNET PENETRATION, 2000-2012**

| World Regions | Number of Internet users (mln.) 2000 | 2012 [a)] | % of 2012 total | Growth of Internet users 2000-2012 | Population (mln. estim.) 2012 [a)] | Internet penetration (% popul. 2012) |
|---|---|---|---|---|---|---|
| Africa | 4,5 | 167,3 | 7.0 % | 3607 % | 1073,4 | 15.6 % |
| Asia | 114,3 | 1076,7 | 44.8 % | 842 % | 3922,1 | 27.5 % |
| Europe | 105,1 | 518,5 | 21.5 % | 393 % | 820,9 | 63.2 % |
| Middle East | 3,3 | 90,0 | 3.7 % | 2640 % | 223,6 | 40.2 % |
| North America | 108,1 | 273,8 | 11.4 % | 153 % | 348,3 | 78.6 % |
| Lat. America & Car. | 18,1 | 254,9 | 10.6 % | 1311 % | 593,7 | 42.9 % |
| Oceania / Australia | 7,6 | 24,3 | 1.0 % | 219 % | 35,9 | 67.6 % |
| World total | 361,0 | 2405,5 | 100.0 % | 566 % | 7017,8 | 34.3 % |

Note: a) Internet Usage and World Population Statistics are for June 30, 2012. Source: www.Internetworldstats.com (retrieval 20 February 2013), with population numbers derived from the US Census Bureau and local census agencies. Internet usage based on data published by Nielsen Online, ITU World Telecommunication /ICT Indicators database, GfK, local ICT Regulators, other sources.

Figure 2 shows the degree of Internet penetration in the European Union (EU27). In 2012 on average 73% of the EU population is Internet user. Internet penetration is highest in The Netherlands (93%) and lowest in Romania and Bulgaria. The Facebook penetration in Europe is an illustration of the

**FIGURE 2 MAJORITY OF EU POPULATION CONNECTED TO INTERNET PENETRATION, 2012**
*(% of population)*



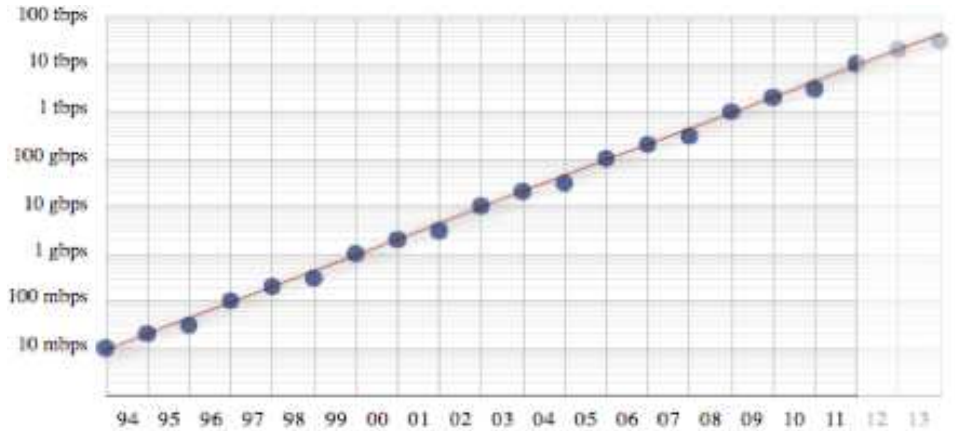

Source: http://www.Internetworldstats.com/ (retrieval 20 February 2013). Participation data are for June 2012.

[3] Europe in this case includes Russia and other non-EU countries.

number of applications for which the Internet is used. On average 38% of the European population participates in Facebook.

A large share of the demand growth for Internet capacity could be facilitated by the increase in information throughput speed, i.e. the speed with which the data packets are sent over the net. Traffic speed went up with 115% per year between 1994 and 2012, as shown in Figure 3. A spurt in Internet and fiberoptics connections took place between 1995 and 2003. The speed-related capacity growth was soon after completion "filled up" with additional data traffic. Most of new investment is nowadays taking place outside Europe and North America (Weller and Woodcock, 2013).

**FIGURE 3 INTERNET TRAFFIC SPEED SHOWS 115% ANNUALIZED GROWTH (1994-2011)**




Source: Packet Clearing House, Weller And Woodcock (2013).

Table 2 depicts that the geographical gravity centre of Internet traffic-volume is shifting from developed OECD countries to emerging markets in Asia and Latin America. The Internet volume growth in Europe and North America is still high, but levelling off. Indicative for the changing geographic pattern in Internet use are the traffic-volume growth rates of the Amsterdam Internet Exchange (AMS-IX). This Internet data exchange point is still one of the largest in the world, but the growth of its traffic volume is gradually diminishing. Its traffic in 2005 increased by 138%, in 2006 79%, in 2007 68%, in 2008 54%, in 2009 50%, in 2010 45%, in 2011 32%, and in 2012 44%.[4]

**TABLE 2 EMERGING TRENDS IN INTERNET TRAFFIC 2005-2015**

| | 2005 | | 2015 | |
|---|---|---|---|---|
| Internet users (millions) in G-20 countries [a)] | 746 | | 2062 | |
| * developed countries | | *238* | | *672* |
| * emerging countries | | *508* | | *1390* |
| Consumer broadband connections (millions) | 167 | | 2707 | |
| * fixed connections | | *167* | | *573* |
| * mobile connections | | .. | | *2134* |
| Global IP-traffic (exabytes per year) [b)] | 30 | | 966 | |

Notes: a) Figures for Internet users and broadband connections refer to sovereign members of the G-20. b) One exabyte is $10^{18}$ bytes, equal to one billion gigabytes. Source: Boston Consulting Group (Dean *et al.*, 2012), based on data of Economist Intelligence, Ovum, Cisco.

[4] Measured in terabytes per second. The 2011 annual report of AMS-IX mentions that the falling growth rate is representative for traffic volume growth for the Internet as a whole.

This shrinking growth rate is consistent with Figure 1, certainly if the continental shift in numbers of Internet users is taken into account (Table 1). Both Figure 1 and Table 2 indicate that Internet access is shifting from fixed to mobile connections, with again most of the growth taking place in Asia and Latin America.[5] Apart from the geographical shift, the following factors are likely to affect future growth patterns of the Internet as a communication medium:

- cloud computing leads to concentration of users and data on less physical locations than in the past, and thus leads to additional transfer demand;
- applications like cloud computing, electronic commerce, online banking, news and video messaging will cause an increase in real-time, high-priority traffic;
- more shift from fixed-line to mobile Internet use through smartphones, tablets and future generations of mobiles.

## 3. CYBERSECURITY INCIDENTS

Internet is increasingly used for personal and professional networking, for economic transactions, and for transfer of personal data. Trust in the Internet has therefore turned into an important precondition for the functioning of society at large, the productivity of firms, and the efficiency of governments. Security incidents may lower the general level of trust in the Internet.

I use a broad and general definition of cybersecurity as the *perceived level of digital data protection and data integrity related to the Internet communication channel*. Cybersecurity has several dimensions: delivery certainty (can we rely on the availability of Internet connectivity); data integrity (can we rely that Internet-linked devices and Internet communication are not tampered with); data privacy (can we trust that electronic data is not used by parties whom we did not give a permission to view and use these data); and protection against cybercriminality (how to protect against malicious digital intrusion, identity theft, destruction, and other attacks). These dimensions show that the sources for a lack of cybersecurity can be very different. To accommodate this I propose an analytic distinction of four types of cybersecurity incidents, based on the backgrounds of the security infringements:[6]

1. *Cyberexploits* aim at stealing and exploiting private digital information from the computer system of Internet users without necessarily causing harm to the infected computer or the assets of its owner;
2. *Cyberattacks* explicitly aim at disrupting or destroying computer systems, data integrity, or at stealing real assets (bank accounts, strategic information) of other Internet users.
3. *Safety neglect incidents* occur where safety negligence of one Internet user causes a higher risk of security incidents for his Internet contacts, or for third parties (firms individuals) that have entrusted their private data to this Internet user.
4. *Technical failure*, other than neglected maintenance that results in loss of functionality and service delivery in Internet-based communication.

[5] Cisco (2012) estimates that the amount of data traffic generated by mobile telephones will by 2016 reach almost 11 exabytes (one exabyte= $10^{18}$ bytes = 1,000 petabytes). In 2012 the sales of smartphones in Asia and Latin America grew by, respectively, 75% and 62% against 20% in Europe and 17% in the USA (Financial Times, 21 February 2013, based on data of Gartner and Bloomberg).

[6] This paper does not consider the actions by secret services, even though the latter may negatively affect the perceived security of Internet communication. State-sponsored cyber actions tend to be driven by goals of espionage, counter insurgency, destabilising, and destroying targeted infrastructures, economic entities and/or military capacities.

Note that the first two incident groups come closest to what is often called cybercrime. Both cyberexploits and cyberattacks rely on the existence of a software vulnerability to get access to computer systems of other Internet users. The perpetrators of cyberexploits and cyberattacks often insert own malicious software code into the host environment to accomplish their goals. Annex shows a bit more details on the two most common types of botnets.

Combinations between these groups of cyber incidents are possible. The recent history has provided several examples of sophisticated multi-staged malicious intrusions where the perpetrators first use cyberexploits to intrude a group of computers. They gain information that can be used to mask the perpetrator's digital trail, his real identity and his objectives. The infected group of computers is called a 'botnet'. In a next stage the perpetrator may turn the infected 'zombie' computers into distance-steered instruments that can be used for cyberattacks on certain websites, servers or network nodes. The managers of the botnets may be economically motivated criminals, hackers or secret services.

Tables 3−5 offer representative examples of cyber-incidents based on, respectively, cyberexploits, cyberattacks, and safety neglect. The tables are here shown for reference purposes only, but a host of other literature provides more detail on all separate elements.[7]

Table 3 includes the 'trade in exploit kits' that according to the European Network and Information Security Agency are increasingly used in the cybercriminal environment (ENISA, 2013). The exploit kits lower the entry threshold for cyberattacks, because the necessary expertise is now stored in ready-to-buy software packages. The exploit kits make use of multiple vulnerabilities in browsers and browser plug-ins; they are mostly applied in drive-by download attacks that inject malicious code in the compromised websites or computers. It is open for debate whether the unsollicited gathering of metadata on the preferences and Internet behaviour of individuals and firms can be regarded as a form of spying. Media websites and search engines like Google secretly gather terabytes of metadata on the information-search behaviour of individual households and firms. On this basis they gather very large quantities of simple behavioural data at a very disaggregated level on individual Internet users and IP addresses. Once they make use of these websites, the user whose Internet actions are meticulously spyed on, have no formal right of consent as regards the use that is made of these data.[8] Search engines have efficient algorithms and structured databases that allow to parse datasets so quickly that the outcomes can be used in real-time for commercial aims (e.g. Cukier and Mayer-Schoenberger, 2013). But not only for commercial purposes. Internet services firms like Microsoft, Apple, Yahoo, Google, Facebook, Skype and YouTube appeared to have been co-operating with the so-called PRISM spying program of the NSA.[9] Within days Google, Facebook and Microsoft raced to publish

[7] E.g. Anderson, Böhme *et al.*(2008); Clark and Landau (2010); Frei (2009); Frei et al. (2010); GOVCERT.NL (2011); NCSC (2012); OECD (2008); OECD (2012); Moore and Anderson (2011); Moore *et al.* (2009); Rao and Reily (2012); Van Eeten and Bauer (2008); Prince (2013).

[8] Formally, the individuals or their firm's software installer may have perhaps have once pushed the "I agree" buttton under the legal terms and conditions of the search engines or social media that 9 out of 10 people never read (cf. Chee et al., 2012, Berthold et al. , 2009). Experimental research by Böhme and Köpsell (2010) found that "*On the bottom line, we have new evidence supporting the hypothesis that ubiquitous EULAs* (end-user license agreements, HK) *have trained even privacy-concerned users to click on "accept" whenever they face an interception that reminds them of a EULA. This behaviour thwarts the very intention of informed consent*". We may therefore take as a fact that many users of these services are fully unaware that social media and search engine providers implant identification cookies on their computer and secretly gather metadata on their behaviour.

[9] In June 2013 *The Guardian* published a series of reports based on information by whistleblower Edward Snowden and other well-informed insiders on the massive spying on the email and Internet traffic of their own citizens by the British and US secret services (NSA's Prism program, GCHQ's Tempora program). These reports hint at disrespect for the constitutional rights to communication privacy of citizens, but at the least they show that the metadata gathered by Internet services firms are not only used for commercial purposes (e.g. Ash, 2013).

details about the frequency and the forced character of the NSA data requests on their websites in an effort to prevent a massive breakdown of consumer trust in their information services. Moreover, the network-platform firms and search engine providers sell these datasets to undisclosed commercial buyers. Individual Internet users have no formal guarantee whatever that these firms would exclude cybercriminals from buying these datasets.

**TABLE 3 TYPES OF CYBEREXPLOITS**

| Type | Brief description |
|---|---|
| **Trade in exploit kits** | Production and trade in ready-to-use software packages that "automate" cybercrime. An important characteristic of exploit kits is their ease of use (usually through a web interface) allowing people without technical knowledge to purchase and use them. |
| **Phishing** | The combined use of fraudulent e-mails and legitimate-looking websites in order to deceitfully gain user credentials. Phishers use various social engineering techniques to lure their victims into providing information such as passwords and credit card numbers. A novelty in phishing is luring authors into paying submission fees for non-existing scientific journals. |
| **Rogueware** | Threat consists of any kind of fake software that cybercriminals distribute (e.g. via social engineering techniques) in order to lure users to their malicious websites. A more specific kind of rogueware is scareware: rogue security software, which tries to infect computers by providing fake security alerts. |
| **Spam** | Abusive use of e-mail technology to flood user mailboxes with unsolicited messages. Removing spam is time consuming for recipients and costly in terms of resources (network and storage) for the service providers. |
| **Cyberespionage** | Industrial and state-driven intrusion in online accessible data systems for stealing private-owned information assets. |
| **Identity theft** | An adversary steals user credentials and uses these for malicious goals, mostly related to financial fraud. The identity of a user is the unique piece of information that makes this specific user distinguishable, e.g. a pair of credentials (username/password) plus Social Security Number (SSN) or credit card number. |
| **Search Engine Poisoning** | Perpetrators deliver bait content for searches to various topics. In this way, users searching for such items are being diverted to malicious content. |
| **Spyware and gathering metadata** | Using unsolicited cookies or even secretly inserted code to spy on the Internet search behaviour of firms and individuals. In a mild form this form of spying is oriented at gathering metadata on individuals or firms that reveal part of their preferences, and that therefore can be commercially sold to third parties (advertisers, sellers of products and services). In a more malicious form these data are gathered to assess vulnerabilities that can be used for criminal purposes. |
| **Information leakage** | Revealing of stolen information by hackers or others, making it available to unauthorized parties. This information can be further processed and abused, e.g. to start an attack or gain access to additional information sources. |
| **Rogue certificates** | Perpetrators steal, produce and circulate rogue certificates which break the Internet chain of trust, giving them the capability of engaging in attacks that are undetectable for end users. By using rogue certificates, attackers may become able to run man-in-the-middle attacks. Moreover, rogue certificates can be used to sign malware that will appear as legitimate and can evade detection mechanisms by other Internet users. |
| **Source: survey constructed from ENISA (2013); Rogers and Ruppersberger (2012).** | |

Table 4 summarises the most conventional types of cyber attacks that –going beyond spying and intrusion– aim at destroying computer systems, disrupting data integrity, or at stealing real assets of other Internet users.

**TABLE 4 TYPES OF CYBERATTACKS**

| Type | Brief description |
|---|---|
| **Drive by exploits** | Refers to the injection of malicious code in HTML code of websites that exploits vulnerabilities in user web browsers. Also known as drive-by download attacks, these attacks target software residing in Internet user computers (web browser, browser plug-ins and operating system) and infects them automatically when visiting a drive-by download website, without any user interaction. |
| **Worms, spyware, viruses** | Malicious programs that have the ability to replicate and re-distribute themselves by exploiting vulnerabilities of their target systems. On the other hand, trojans are malicious programs that are stealthily injected in users systems and can have backdoor capabilities (to get into the operating system), collect and or steal user data and credentials. |
| **Code-injecting attacks** | The adversaries placing such attacks try to extract data, steal credentials, take control of the targeted web server or promote their malicious activities by exploiting vulnerabilities of web applications. |

| | |
|---|---|
| **Using exploit kits** | Use of ready-to-use software packages, mostly in drive-by download attacks, whereby malicious code is injected in compromised websites after exploiting multiple vulnerabilities in browsers and browser plug-ins. The exploit kits may use a plethora of channels to deliver malware and infect unsuspected web users. |
| **Botnets** | Creating a network of 'zombie' computers infected by a piece of malicious software designed to enslave them to a master computer, the so-called botnet herder. These compromised systems ('zombies') communicate with the botnet herder who can direct them to do what he wishes, e.g. spamming, phishing mails, identity theft, infecting other systems, and distributing malware. Annex shows two typical variants of botnets. |
| **Denial-of-service attack (DoS) [a])** | Attempt to make a resource unavailable to its users. The perpetrators of DoS attacks usually either target high profile websites/services or use these attacks as part of bigger ones in order achieve their malicious goals. For a recent spectacular case, see Prince (2013). Despite the fact that these kinds of attacks do not target directly the confidentiality or integrity of the information resources of a target, they can result in significant financial and reputation loss. The confusion caused by a DoS attack can further be used to gain a better response to phishing mails ("reset your account"). |
| **Targeted attack** | Occurs when attackers target a specific entity/organization over a long time span. Often the objective of targeted attacks is either data exfiltration or gaining persistent access and control of the target system. This kind of attack consists of an information gathering phase and the use of advanced techniques to fulfil the attacker's goals. The first phase can possibly involve specially crafted e-mails (spearphishing), infected media and social engineering techniques, whereas the second phase involves advanced and sophisticated exploitation techniques. |

**Note a) A distributed denial-of-service attack (DDoS) occurs when multiple computers launch simultaneous DoS attacks against a single target. In DDoS attacks, attackers use as much firepower as possible (usually through compromised computer systems/botnets) in order to make the attack difficult to defend. Source: survey constructed from ENISA (2013); OECD (2008); Prince (2013).**

Table 5 gives the most prominent incidents in the category *safety neglects*. Data-breach events in which private information leaks away through Internet mostly occurs with databases of firms (client data, credit card numbers), health centres (patient data), public utilities, and parts of government that hold private data about third persons. The information disclosure may result from internal safety procedure or under-investment in safe software and hardware systems, but it may also result from irresponsible behaviour (or even sabotage) by employees or other internally operating agents.[10] The data breaches are often real incidents with a precise time dimension, although also more sneaking data breach incidents occur with a less precise time dimension.

**TABLE 5 TYPES OF SAFETY NEGLECT INCIDENTS THAT ENDANGER CYBERSECURITY**

| Type | Brief description |
|---|---|
| **Compromising of confidential information** | Refers to unintential data breaches of private information about third persons (clients, patients, citizens) after neglecting safety procedures and 'good husbandry' standards for firms, health centres, and public utilities that hold confidential information about third persons. The unintentional information disclosure may result from internal safety procedure or under-investment in safe software and hardware systems, but it may also result from irresponsible behaviour (or even sabotage) by employees or other internally operating agents. |
| **Reported neglects of data and network security** | Neglect of computer safety procedures (password policies, single sign-on procedures to all internal data resources), under-investment in software (no safety updates, out-of-date virus scanners and firewall) and hardware (no back-up systems). On unsafe passwords, see Heninger et al. (2012). This may be caused by sheer neglect or deliberate cost-cutting choices. Such under-investment renders computer systems vulnerable for botnet intrusion with negative knock-on effects for Internet users elsewhere. |
| **Vulnerabilities in management of critical infrastructure** | Delivery certainty of critical infrastructure services (airports, harbours, air control, electricity and telecommunication grids, water protection installations, emergency communication systems) becomes vulnerable if the vital installations for these services are distance-controlled only through Internet connections. In a number of cases it was shown that external cyber intruders had found access to these (so-called SCADA) control systems.[a)] This may create dangerous situations with potential large-scale damage. |

**a) SCADA (Supervisory control and data acquisition) is the collection, transmission, processing and visualisation for monitoring and control of large industrial and infrastructure systems, often multi-site, and sometimes over large distances.**
**Source: survey constructed from ENISA (2013); Security.nl (2012);**

[10] Data breaches are considered as a real risk in Internet use. The 2012 EU survey found that between 60 and 80 percent of the Internet users are concerned that online personal information is not kept secure by websites (EC, 2012: 43). OECD (2011) describes country differences in the legal framework regarding confidential data about third parties.

Under-investment in security by one Internet user may endanger security for other network users with whom the first user is in contact via Internet information exchange. Security under-investment is particularly harmful if it occurs in data systems used for vital infrastructure installations. A failure to ensure physical backup systems for vital Internet and other communication infrastructures forms a critical under-investment incident. In 2011, a fire in a Vodafone connection centre in Rotterdam caused a days-long breakdown of important government communication channels around Rotterdam and The Hague; there appeared to be no physical backup system. Substantial parts of a country's critical infrastructure (energy and telecom grids, water management systems, traffic control) are nowadays at least partly managed via Internet communication, or depend on the latter. Multiple negative physical feedbacks loops arise by a growing reliance on remote Internet-based control of vital infrastructure. Critical vulnerabilities may arise if the local Internet provision depends on the local electricity grid, while the latter is coordinated through Internet. It creates a double sensitivity to low-probability-strong-impact risks like natural disasters or fires. The hurricane Sandy on the US east coast caused days of disrupted electricity grid and vital Internet connection points in 2012.

A last type of security incidents is related to *technical failure* (other than neglected maintenance). Such security incidents cause a loss of functionality and service delivery in Internet-based communication. Often, this type of security incidents occur in the 'last mile' of Internet connections.[11] They can mostly be traced back to a lack of redundancy in Internet connection systems (switches, cables, servers), giving rise to single points of failure. A fire or flooding in a vital switching point, or the breaking of a fiberoptics cable by a bulldozer may create severe disruption of Internet communication.

The four types of cybersecurity incidents form a stylised framework for further analysis, but it should be clear that in practice there can be several overlaps between the four categories. For instance, a relation exists between *safety neglect* incidents and the *cyberexploit* incidents that precede cyberattacks. Several empirical reports on security incidents establish that vulnerability to cyberexplots is mostly preceded by safety neglect. Two examples:

- A large US Internet services provider reports: "*Unfortunately, breaching organizations still doesn't typically require highly sophisticated attacks. Most victims are a target of opportunity rather than choice. The majority of data is stolen from servers, victims usually don't know about their breach until a third party notifies them, and almost all breaches are avoidable (at least in hindsight) without difficult or expensive corrective action*" (Verizon, 2011: 3).
- Careless providing of personal data to semi-closed social media creates vulnerability to use of these data by cybercriminals. Krishnamurthy *et al*. (2011) assess that it is easy to obtain private information from social-media websites, booking sites and medical sites that are supposed to guard these personal data of their clients. Kosinki *et al.* (2013) find that public Facebook 'likes' reveal a person's private traits 'with spooky accuracy'.[12] It is just a matter of time before cybercriminals learn to do these tricks. It creates new vectors for sophistically targeted cyberexploits and cyberattacks.

[11] Technical failure incidents may sparsely occur in the core of the Internet connection system, e.g. when a sub-marine trunk fiberoptics cable is broken by a ship's anchor or by fishing activities. However, the impact of this can mostly be remediated quite soon by other connections; the core system of the Internet has much flexibility due to sufficient redundancy in connection possibilities.

[12] Kosinski *et al.* (2013) collected consenting Facebook users' personal traits from a questionnaire app called My Personality. Pairing that data with the users' publicly available Facebook "likes," Kosinski's team developed an algorithm that figured out which "likes" corresponded to which personality traits, such as race, religion, sexual orientation, political affiliation, smoking, use of alcohol and drugs.

It is difficult to attach an average 'importance weight' to the four categories of security incidents that were distinguished in this section. The occurrence intensity of the different types of security incidents differs over time, by country and by type of victim (cf. Panagiotis, 2010). By way of 'importance weight' Table 6 reproduces the expected relevance ranking for 2013 by main type of security incident, according to the European Network and Information Security Agency ENISA.

**TABLE 6 ENISA CLASSIFICATION OF MAIN 2013 CYBERSECURITY THREATS IN EUROPEAN UNION**

| ENISA Rank a) | Top threats | General trend b) | Relevance for specific cybersecurity areas b) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Mobile Internet | Social media | Critical infrastruct. | Cloud computing | Big data |
| | **Cyberattacks** | | | | | | |
| 1 | Drive-by-exploits | + | + | + | + | + | + |
| 2 | Worms/Trojans | + | + | + | + | = | + |
| 3 | Code injection | + | = | | + | + | |
| 4 | Using exploit kits | + | + | = | + | | + |
| 5 | Botnets | + | + | | = | = | |
| 6 | Denial of Service | = | | | = | | |
| 11 | Targeted attacks | + | | + | + | + | = |
| | | | | | | | |
| | **Cyberexploits** | | | | | | |
| 7 | Phishing | = | + | + | = | | = |
| 9 | Rogueware | = | | = | | | |
| 10 | Spam | ? | | = | | | = |
| 11 | Identity theft | + | + | + | | + | + |
| 15 | Search engine poisoning | = | | | | | |
| | | | | | | | |
| | **Safety neglect incidents** | | | | | | |
| 8 | Breach confident. informat. | + | + | | + | + | + |

a) ENISA threat ranking for 2013. b) Codes: + expected to increase; = stabilising; − expected to decrease. Source: ENISA (2013).

## 4. CYBERSECURITY IN THE PERSPECTIVE OF INTERNET TRAFFIC GROWTH

This section investigates empirically whether the number of cyberincidents has been growing faster than overall Internet traffic.

Press reports suggest a dramatic increase of the number of cybersecurity incidents. In 2012, the European Commission commissioned a large survey among EU citizens to assess their experiences with and perceptions of cybersecurity issues.[13] The survey found that between 70 and 90 per cent of Internet users were convinced that the risk of becoming a victim of cybercrime has increased during the preceding year. The increased awareness of cybercrime might just reflect the grown importance of the Internet.[14] More people use Internet communication, in more countries, with more physical devices, for more private and commercial activities, during more time of the day, and they confide more information about themselves and about their businesses to their digital contacts or to 'the world at large'. Also the number of security incidents increases: a larger Internet traffic opens more 'entries' and opportunities for digital criminality and for individual safety leaks.

[13] In total 26,593 interviews were held, on average 1000 interviews per EU member state. The survey examined the frequency and type of Internet use that EU citizens have, their confidence about Internet transactions, their awareness and experience of/with cybercrimes, and the level of concern they feel about this type of crime.

[14] However, the Commission's definition (*any crimes which are committed via the Internet* (EC, 2012) may not be helpful for getting an unbiased measurement. It misses analytic clarity. Many standards forms of criminality (like tax and social security fraud and illegal copying) are nowadays wrapped in 'digital jacket', simply because the Internet has become a more important communication medium. But here is nothing news under sun apart from this new jacket.

A proper discussion of the question *whether the Internet is becoming more insecure over time* requires that the number of incidents is corrected for the growth of Internet traffic. In this way we obtain a time pattern of the number incidents per amount of data sent over Internet. The following procedure is used for measuring this. To cope with the multiple dimensions of cybersecurity I use a set of seven more or less time-consistent data series: [15]

- the total number of newly discovered and documented software vulnerabilities per period;
- the number of documented vulnerabilities in Internet browser software;
- the number of threats to confidential information in the top-50 malicious code reports;
- the number of botnet-infected computers, observed per day (average);
- the number of unique phishing messages (thousands);
- the number of domain names known to be engaged in phishing activities; and
- the number of distinct phishing attacks.

The growth percentage of these indicators is diminished with the growth percentage of Internet traffic over the same period.[16] Table 7 gives the results. Each of the seven panels depicts the relative increase in security incidents per period. Our overall finding is that *the number of cyberincidents per unit of transferred data tends to fall*, both over the full data period and for the last four data years (last column of Table 7). The average normalised growth of cyberincidents in the last four data years has fallen in all cases except for the number of phishing attacks.

**TABLE 7 RELATIVE INCREASE IN INCIDENTS PER UNIT OF DATA SENT OVER THE INTERNET, 2001-2011 (% INCREASE)**

| Indicator | Data coverage period | Avg. nominal growth (full period) | Growth % normalised for Internet traffic growth b) | |
|---|---|---|---|---|
| | | | full period | 2008-2011 |
| Internet traffic volume (IP-based) | 2001-2011 | 28.9 | | |
| Total vulnerabilities detected by Symantec | 2001-2011 | 8.1 | -20.8 | **-16.3** |
| Documented browser vulnerabilities a) | 2003-2011 | 28.6 | 3.1 | **-11.6** |
| Threats to confidential information in top-50 malicious code reports | 2001-2011 | 5.3 | -23.5 | **-18.0** |
| Daily observed no. of botnet-infected computers | 2006-2009 | -0.4 | -24.4 | **-26.6** |
| No. of unique phishing messages (000) | 2005-2007 | 23.3 | -4.6 | **..** |
| No. of observed phishing domain names | 2009-2011 | 15.5 | -3.0 | **-3.0** |
| No. of phishing attacks | 2009-2011 | 24.4 | 5.8 | **5.8** |

**Notes: a) This includes documented vulnerabilities in MS Internet Explorer, Apple Safari, Mozilla Firefox, Opera, and Google Chrome. b) semi–annualised growth after correction for Internet traffic growth. Source: calculated from semi-annual reports by Symantec (e.g. Symantec, 2007); reports by the Anti-phishing Working Group of the Internet Policy Committee (e.g. APWG, 2008-2012); Internet traffic volume data is obtained from annual reports of the Cooperative Association for Internet Data Analysis (e.g. CAIDA, 2011).**

Contrary to public beliefs and press reports, this empirical evidence provides no support for the view that Internet has become intrinsically more unsafe than it used to be. Rather, it suggests that the Internet per unit of data traffic has become safer over time, and that the current public unease about

[15] The first five indicators reported by Symantec, a leading producer of anti-virus software and firewalls in semi-annual reports (e.g. Symantec, 2001-2012); the last two items are reported by the Anti-phishing Working Group of the Internet Policy Committee (e.g. APWG, 2008-2012).

[16] The data on Internet traffic growth are provided by the annual reports of CAIDA (e.g. CAIDA, 2011), with the traffic volume measured in petabytes (one million gigabytes) per month during the time interval.

cybersecurity is driven mainly by the growth in scale and pervasiveness of Internet communication exchange.

However, a few caveats should be taken into account. The Internet has grown faster than the count-based indicators of cyber-incidents. No reliable and consistent data series were from which the average harm per incident can be derived. Part of the data on cyberincidents stem from Symantec, a firm that sells Internet security software and services. If anything, this firm has an incentive to exaggerate the cyber threats. Hence, the normalised growth of cyberincidents as reported in Table 7 tends even to be upwardly biased. Secondly, Table 7 only uses items for which data series longer than a few years could be constructed; these are not necessarily the best indicators for cyber-incidents. A further caveat is that the data should be refined for regional differences, because the growth of Internet traffic and the growth of cyberincidents are now averaged for the world as a whole. Better data quality, more time consistence and statistical independence is required for future cybersecurity policy-making.

Suppose part of Internet traffic growth is driven by the improved video quality of images that are sent over the Internet, rather than by a larger volume of data requests or by a larger number of data content items. In that case, the Internet traffic indicator used in Table 7 to normalise the growth of cybersecurity incidents should be image-quality corrected. Such a correction should also take on board the possibility that the demand for better video properties may come at the cost of new cyber vulnerabilities, e.g. due to software that opens more of the user's computer ports at the same time. A methodological study is required to develop measurements standards for both types of corrections.

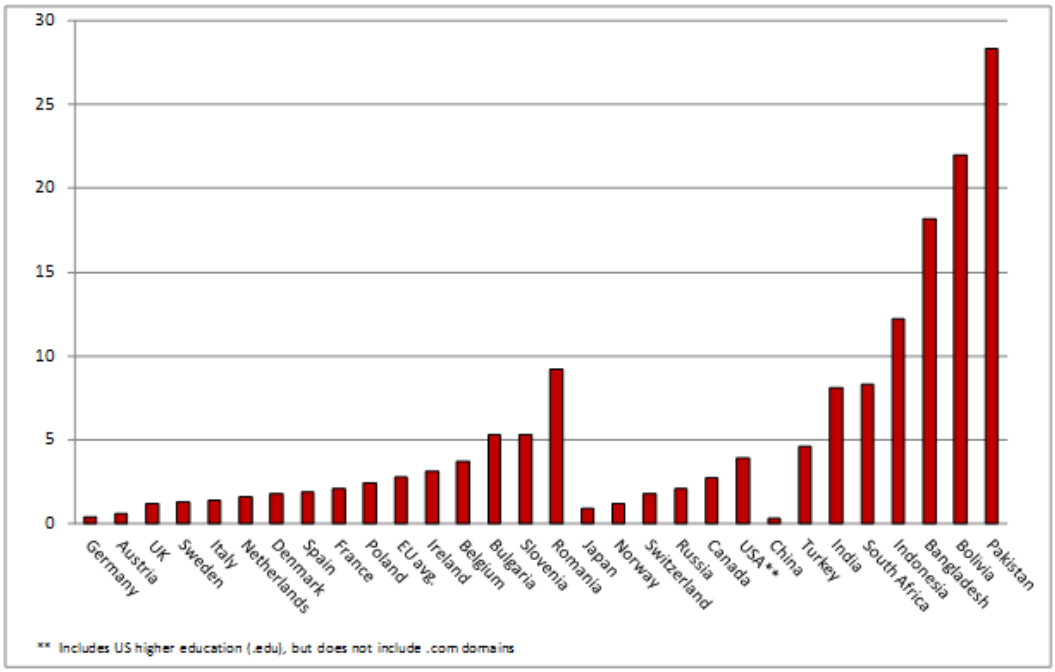
The finding that, the Internet - in relative terms - has become safer per unit of transferred data does not make security concerns futile. The fact remains that private persons, firms and government are being confronted with more cyberincidents. From the 2012 EU survey on cybersecurity it emerges that, on average across the EU, 8 per cent of Internet users report to have at least once been a victim of digital identity theft, but in Romania and Hungary this is, respectively, 16 and 12 per cent.[17] Some forms of cybercriminality seem to be targeted at high-income countries. For the EU as a whole, 38 per cent of Internet users have received fraudulent emails asking for money or personal details (including banking or payment information), but in the Netherlands and Denmark this percentage was 54 percent, against only 18 and 19 per cent in, respectively, Bulgaria and Poland (EC, 2012: 50). Both actual experience with cybercriminality and perceived risks of Internet use −even if this would be caused by hyped media messages− have impacts on actual behavioural choices of firms and private households.

In absolute numbers, most of current Internet growth occurs outside Europe and the USA. This also has consequences for cybersecurity. The massive entry of new Internet users in Asia and Latin America creates new cohorts of potential victims. Though their average incomes are generally lower, their numbers still make them attractive targets. Uninformed new Internet users will more easily become victims of cybercriminality. For instance the incidence of phishing activities tends to be higher in developing countries than in developed countries as Figure 4 shows; phishing sites are found most in less-developed countries.[18]

[17] For comparison: in the Netherlands it is 7%, in Germany 6%, and in Denmark 4%, but in Belgium and the UK it is, respectively 10% and 12% (EC, 2012: 48).

[18] Most phishing attacks target at banks and other financial services firms, and more recently on the ISP sector (10 percent of reported phishing attacks). ISP accounts can be valuable to phishers because they may contain email accounts, Web-space, and other authentication credentials (e.g. Symantec, 2012).

**FIGURE 4 PHISHING ACTIVITY STRONGER IN DEVELOPING COUNTRIES, 2012**




Note: graph depicts number of phishing domains per 10,000 web domains. Data: Rasmussen and Aaron (2012).

## 6. CONCLUSIONS

Internet traffic volume has about doubled each year between 1990 and 2011. In the OECD countries the growth rate has been smaller, and it is gradually levelling-off. Most growth came from Asia and Latin America, and medium-term forecast project that this continue until 2015. This leads to important shifts in Internet traffic. In 2015 only one in three Internet users will live in one of the OECD countries. Fixed wires still carry by far the largest part of Internet traffic, but the traffic share generated by smartphones, tablets and other mobile devices is increasing fast. From a contents perspective, an increasing share of Internet traffic will be driven by network-platforms, cloud computing, streaming video and other real-time traffic. Cybersecurity will be one of the key environmental parameters that determine a further growth of ecommerce, online banking and other economic transactions that depend on the exchange of confidential data items.

This paper uses a broad definition of cybersecurity, namely the perceived level of digital data protection and data integrity related to the Internet communication. Based on behavioural backgrounds, cybersecurity incidents are split into four groups. *Cyberexploits* aim at stealing and exploiting private digital information of Internet users without necessarily causing harm to the infected computer. *Cyberattacks* through Internet explicitly aim at disrupting or destroying the computer systems of the victim, and/or stealing real assets like bank accounts. *Safety neglect incidents* are incidents whereby reprehensible negligence of one party causes data breaches, malware infection or violation of data integrity for other Internet users. *Technical failure* refers to contingent incidents resulting in loss of functionality and service delivery in Internet-based communication.

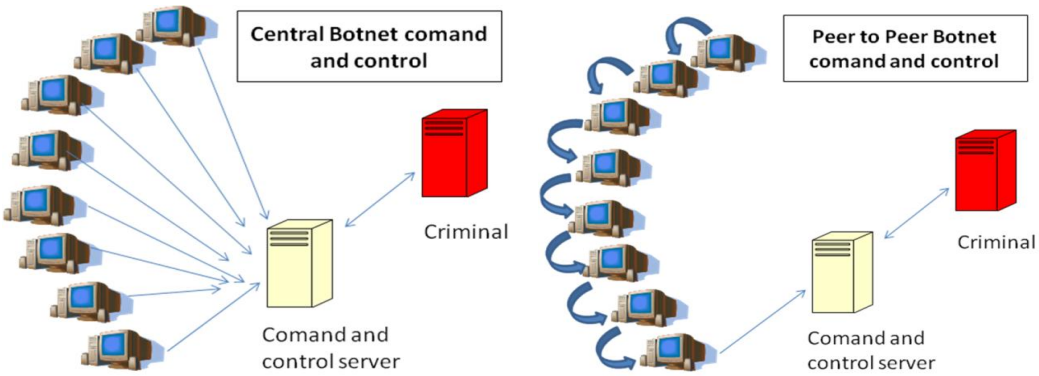
Using seven security indicators the paper finds that between 2001 and 2011 Internet traffic volume has grown faster than the number of most cyberincidents. This was also the case in the recent years (between 2008 and 2011). This suggests that in relative terms the Internet is becoming a safer place over time, and that most growth of cyberincidents is driven by the Internet traffic volume. The recent surge in the number of reported cyberincidents is then driven by the growth in scale and pervasiveness

of Internet communication exchange. This result must be interpreted with due care, because adequate, unbiased and time-consistent statistics on cyberincidents are still very scarce. A regional desaggregation of the security and traffic statistics is required, and it would also be desirable to correct Internet traffic-volume data with a time index for the average amount of traffic per Internet data-exchange application.

The finding that, the Internet - in relative terms - has become safer per unit of transferred data does not make security concerns futile. The fact remains that private persons, firms and government are being confronted with more cyberincidents, and that the associated insecurity hampers the development of online economic activity.

## ANNEX THE OPERATION OF BOTNETS

**FIGURE A1 SETTING UP A BOTNET (TWO TYPES)**




Source: OECD (2008).

# REFERENCES


Anderson, R., R. Böhme, R. Clayton and T. Moore, 2008, *Security economics and the Internal Market*, report commissioned by European Network and Information Security Agency (ENISA), Heraklion.

APWG, 2008-2012, *Global Phishing Survey - Trends and Domain Name Use* (twice per year), APWG, Internet Policy Committee, Lexington MA.

Ash, T.G., 2013, If Big Brother came back he'd be a public-private partnership, *The Guardian*, 27 June 2013.

Berthold, S., R. Böhme, and S. Köpsell, 2009, Data retention and anonymity services, In: V. Matyas et al. (eds.), *The Future of Identity in the Information Society*, Springer, Boston, 92–106.

Black, P., K. Scarfone and M. Souppaya, 2008, Cybersecurity metrics and measures, in J. Voeller (ed.), *Handbook of Science and Technology for Homeland Security*, John Wiley and Sons, London.

Böhme, R. and R. Köpsell, 2010, Trained to Accept? A Field Experiment on Consent Dialogs, paper presented at CHI 2010 (April 10-15, 2010, Atlanta, Georgia, USA), (http://dmrussell.net/CHI2010/docs/p2403.pdf).

CAIDA, 2011, *Annual report for 2011*, Cooperative Association for Internet Data Analysis, University of California, Supercomputer Centre (http://www.caida.org/home/about/annualreports/2011/#topology).

Chee, F., N. Taylor and S. de Castell, 2012, Re-Mediating Research Ethics: End-User License Agreements in Online Games, *Bulletin of Science Technology Society*, 32 (6), 497-506.

Cisco, 2012, *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2011–2016*, White Paper, www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.pdf.

Cukier, K. and V. Mayer-Schoenberger, 2013, The Rise of Big Data -How It's Changing the Way We Think About the World, *Foreign Affairs*, 92(4), May June,

Dean, D., S. DiGrande, D. Field, A. Lundmark, J. O'Day, J. Pineda and P. Zwillenberg, 2012, *The Internet Economy in the G-20: The $4.2 Trillion Growth Opportunity*, Boston Consulting Group.

EC, 2012, *Cybersecurity*, Special Eurobarometer #390, TNS Opinion and Social, at the request of European Commission DG Home Affairs, coordinated by DG COMM, Brussels.

ENISA, 2013, *Threat landscape: responding to the evolving threat environment*, European Network and Information Security Agency, Heraklion.

Frei, S., B. Plattner, and B. Tramell, 2010, *Modelling the Security Ecosystem - The Dynamics of (In)Security*, paper presented at WEIS 2010 conference, ETH Zürich (http://www.techzoom.net/security-ecosystem).

Frei. S., 2009, *Security econometrics: the dynamics of (in)security*, PhD dissertation, ETH, Zürich.

GOVCERT.NL, 2011, Cybersecuritybeeld Nederland 2011, Ministerie van Veiligheid en Justitie, Den Haag.

Graham-Rowe, D., 2007, Mapping the Internet, *MIT Technology Review*, 19 June, (http://www.technologyreview.com/news/408104/mapping-the-Internet/), accessed April 09, 2013..

Heninger, N., Z. Durumeric, E. Wustrow and J. Halderman, 2012, Mining your Ps and Qs: detection of widespread weak keys in network devices, *Proc. 21st USENIX Security Symposium*, Aug. 2012 ()

Kosinski, M., D. Stillwell and T. Graepel, 2013, Private traits and attributes are predictable from digital records of human behavior, *Proceedings of the National Academy of Sciences of the United States of America*, (published online before print, March 11, 2013: doi: 10.1073/pnas.1218772110 ).

Kox, H. (2013), Analysing the effect of cybersecurity with a gravity model of Internet traffic, MPRA Paper, Munich (forthcoming).

Moore, T, and R. Anderson, 2011, *Economics and Internet security: a survey of recent analytical, empirical and behavioural research*, WP TR-03-11, Computer Science Group, Harvard University, Cambridge MA.

Moore, T., R. Clayton and R. Anderson, 2009, The economics of online crime, *Journal of Economic Perspectives*, 23(3), 3-20.

NCSC, 2012, *Cybersecuritybeeld Nederland2012*, Nationaal Cyber Security Centrum, Den Haag.

Odlyzko, A., 2004, *Internet traffic growth: sources and implications*, mimeo, University of Minnesota, Minneapolis, MN.

OECD, 2012, *Proactive policy measures by Internet service providers against botnets*, OECD Digital Economy Papers #199, OECD, Paris.

OECD, 2011, *National strategies and policies for digital identity management in OECD countries*, DSTI/ICCP/REG(2010)3/FINAL, DSTI, Working Party on Information Security and Privacy, Paris.

OECD, 2008, *Malicious software (malware): a security threat to the Internet economy*, DSTI/ICCP/REG (2007)5/Final, OECD, Paris

Panagiotis, T., 2010, *Measurement frameworks and metrics for resilient networks and services: challenges and recommendations*, ENISA European Network and Information Security Agency, Heraklion.

Prince, M., 2013, *The DDoS That Almost Broke the Internet*, CloudFlare blog, March 27, 2013 (http://blog.cloudflare.com/the-ddos-that-almost-broke-the-Internet).

Rasmussen. R and G. Aaron, 2012, *Global Phishing Survey: Trends and Domain Name Use 1H2012*, APWG, Lexington MA.

Rao, J. and D. Reily, 2012, The economics of spam, *Journal of Economic Perspectives*, 26(3), 87-110.

Rogers, M. and D. Ruppersberger, 2012, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, U.S. House of Representatives, 112th Congress, Washington DC.

Security.nl, 2012, *Onderzoeker vindt 23 SCADA-lekken in 4 uur*, October 28, 2012 (https://www.security.nl/artikel/44099/1/Onderzoeker_vindt_23_SCADA-lekken_in_4_uur.html).

Symantec, 2001-2012, *Annual and Quarterly Symantec Internet Security Threat Reports*, Symantec Corp. (e.g. 2007: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_Internet_security_threat_report_xi_03_2007.en-us.pdf)

Van Eeten, M. and J. Bauer, 2008, *Economics of malware: security decisions, incentives and externalities*, STI Working Paper DSTI/DOC(2008)1, OECD, Paris.

Verizon, 2008-2012, *Annual Data Breach Investigations Report (DBIR): study conducted by the Verizon RISK Team with cooperation from the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting and Information Security Service, Police Central e-Crime Unit, and United States Secret Service*, (2012: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf?__ct_return=1).

Weller, D. and B. Woodcock, 2013, *Internet traffic exchange: market developments and policy challenges,* DSTI/ICCP/CISP(2011)2/Final, OECD, Paris.