Economic aspects of Internet security[1]

Henk Kox[2] and Bas Straathof[3]

CPB Background Document

[1] We would like to thank Giuseppe Abbamonte, Jaap Akkerhuis, Esther van Beurden, Fokko Bos, Maarten Botterman, Alessandra Falcinelli, Eric Hertogh, Peter Hondebrink, Olaf Kolkman, Edgar de Lange, Michel van Leeuwen, Ronald van der Luit, René Nieuwenhuizen, Alex Noort, Mink Spaans, Michiel Stal, Paul Timmers, Michel Verhagen, Jan Westerman, Henry van der Wiel, Erwin Zijleman and others for insights and discussions. All errors and omissions are ours.
[2] h.l.m.kox@cpb.nl
[3] s.m.straathof@cpb.nl

Executive summary

The Internet has become a part of daily life for many people. And if the past decade is of any guidance, the role of the Internet in the economy is going to increase substantially. As a consequence of this rapid development, the security of communication over the Internet will become even more important than it already is today.

The Internet is provided by a broad range of organizations with varying, and sometimes conflicting, objectives. The security of the Internet depends on the behaviour of all users (although in varying degrees) but these users often do not have sufficient incentives to invest in cyber security. Insights from economics help us to understand these incentives and may help to make the Internet a safer place.

This background document surveys cyber security issues related to the Internet from an economic perspective, focusing on the role of markets and incentives. Cyber security covers four areas:

- Availability (can we use the Internet without interruptions?)
- Integrity (can we trust that data we transmit or store are not tampered with?)
- Privacy (can we trust that data is not used by parties whom we did not give permission?)
- Identity (do we know who we communicate with? how to protect against fishing and spam?).

The central question of this study is: Under which conditions will markets provide solutions for cyber security issues, and in case they do not arise, what can governments do? We discuss market failures that may lead to cyber security investment levels that are insufficient from society's perspective and other forms of unsafe behaviour in cyber space. Intervention by national governments and international cooperation may be called for, if the social costs of intervention (including administrative burdens on firms) are smaller than the damage caused by cyber security problems.

Economic theory offers standard solutions for categories of market failures that also apply to cyber security. For example, we discuss standard solutions for asymmetric information problems (how to identify reliable market partners) and for coordination failure (how to get safer Internet standards adopted). However, externalities of investments in cyber security have some peculiar features that, to our knowledge, have not received any attention in the literature.

The security of the Internet depends on the organizations that together provide the infrastructure and on the behaviour among end users. Regarding the infrastructure of the Internet, there are several reasons why markets may fail to deliver a level of cyber security that is optimal for society as a whole:

a) A first problem is information asymmetry between two economic agents. For example, end users may not be able to verify whether an Internet Service Provider (ISP) gives correct information about its security performance. This uncertainty makes end users reluctant to pay for security. For ISPs this means that their investments in cyber security do not give them an advantage over competitors; additional security will only increase costs. ISP's can try to escape this mechanism by investing in a reputation of providing high degree of security. As building a

reputation requires substantial investments, market concentration will increase and competition might be reduced.

Similar problems caused by limited information about security levels apply to other infrastructure-related organizations, including Certificate Authorities. Internet users that want to have certainty about the identity of the people or organizations they connect with, depend on commercial Certificate Authorities (CA). The service quality of CA information cannot be assessed by individual end users, and there have been serious incidents in recent years. Because providers of Internet-related services cannot observe the quality of the CA, they are tempted to use the cheapest CA-services. In situations like this one, where markets fail due to information asymmetry, governments can intervene by enforcing transparency, for example by publishing cyber security incidents or requiring certification, and by setting minimum security standards.

b) A second problem is related to the external effects, or externalities, of investments in security. ISPs may not be able to capture the full benefits of their investments in cyber security, for example because part of the potential benefits is for customers of other ISPs. This market failure is another reason why investment in cyber security might be insufficient from society's perspective. When externalities are strong, governments may promote cyber security by subsidizing the use of secure technology or by setting minimum cyber security standards. Temporary policy measures will suffice for the promotion of the adoption of safer communication protocols.

A similar problem arises for core infrastructure providers (so-called backbone providers) who are responsible for the resilience of the Internet against shocks like natural disasters and massive DDoS attacks. Many end users expect that the Internet is available at all times and this requires sufficient spare capacity in the backbone. However, the organizations responsible for the backbone infrastructure only capture a fraction of the benefits of redundant capacity, and may be inclined to invest less than is socially optimal.

c) Another type of market failure in the network infrastructure relates to indivisibility of investments, which may lead to market power problems. Competitive pressure on large international network providers to improve their security performance may be low as they are "too-big-to-block" by peering partners. Governments might be able to raise the level of security by imposing minimum security standards. International coordination would be required for these standards to be enforceable.

On the Internet, security problems not only arise because of the behaviour of infrastructure providers, but can also be due to the behaviour among end users, which can be households, firms, as well as governments. The market failures that lead to cyber security problems are of a similar nature as those that affect the behaviour of network-infrastructure providers:

a) Firms and households may not have reliable information on the quality of a firm's handling of private customer information. End users may therefore limit their online transactions to a lower level than they would choose otherwise. The information asymmetry also implies that firms cannot compete on the level of security that they provide: firms that under-invest in security drive secure firms out of the market. An independent 'cyber security label' for firms could relief this problem and lead to more efficient market solutions.

b) Second, the behaviour of end users partly determines the security of communication over the Internet. Each firm or household has means to protect its computer and data integrity against malicious intrusion from outside, ranging from spam filters, virus scanners, firewalls, changing passwords, avoiding suspect websites, to dedicated IT departments. These means have in common that they cost money and effort. End users make a private choice about the security level that they want to achieve. Almost no one opts for maximum security because this would be very expensive and would reduce the benefits of participating in the Internet.

Cyber criminals and hackers use end-user security vulnerabilities for their own profits and interests, spreading botnets, viruses, and phishing mails on the Internet. Investment in security by end users not only limits the possibilities for cyber criminals on the end user's own computer system, but it also creates positive externalities for other end users and for some network infrastructure providers. Because end users do not fully take into account the benefits of security to other users, they will tend to invest less than would be socially desirable. These externalities need not lead to market failure per se. Markets can adjust for externalities if the following two conditions are met:

- Awareness: do we know that we have been damaged, or that (future) costs have been created for our computer, data integrity or data privacy?
- Attribution: who is responsible for this damage, and through which action has this damage been caused?

When it comes to externalities stemming from the behaviour among end users, these two conditions often are not fulfilled. Awareness is far from perfect as many end users do not know that their computer, software or data is infected by a botnet or by other malicious software. Such awareness often only arises long after the event has taken place. Attribution is even more difficult, because most end users are unable to reconstruct the technical chain of events that damaged their computer system. And finally, even if awareness and attribution is possible, the negotiation and enforcement of a compensation deal can be troublesome, in particular when end users operate in different countries and jurisdictions. Improving awareness, attribution and enforcement will probably require that Internet service providers and national cyber security agencies play a more prominent role.

An economic perspective on Internet security is useful not only for identifying weak spots, but also for finding solutions to security problems. In time, economics may prove to be indispensable for making the Internet a safer place.

Contents

Executive summary 2
Contents 5
1. Introduction 6
1.1 An economic perspective on cyber security 7
1.2 Is the Internet getting less secure? 8
1.3 Outline 11
2. When do markets fail to provide security? 12
2.1 Public goods, common goods, and club goods 12
2.2 Asymmetric information 13
2.3 Externalities 14
2.4 Market power 17
2.5 Overview 18
3. Market failures related to infrastructure 19
3.1 National networks 19
3.2 International backbone of Internet 21
3.3 Summary 25
4. Market failures related to end users 26
4.1 Households 26
4.2 Firms 28
4.3 Governments 30
4.4 Summary 31
5. Concluding remarks 33
Annexes 34
Annex 1 Internet basics 34
Annex 2 Types of cyber security incidents 37
References 38
Endnotes 46

1. Introduction

After years of increasing enthusiasm about the Internet's capacity to lower the costs of information and communication, people now become more aware that the Internet is also a network that is open to criminal use. Our personal data are nowadays stored in the databases of supermarkets, ecommerce firms, banks, insurance firms, health institutions, and government authorities. Social media like Facebook, LinkedIn and Twitter are widely used.[1]

The downside of almost frictionless communication is that privacy appears to become more elusive. Where a 'vault' or a 'safe' was the place where one used to store private information or entitlements fifty years ago, many of such data are now in electronic databases that can −at least in principle− technologically be accessed via the Internet. Unsurprisingly, large pools of data attract both professional and occasional cyber criminals. Almost on a daily basis, newspapers report about data leaks, spreading of computer malware, attacks on online banking accounts, stealing of digital identities, hacking of databases, and other cyber crime incidents. There is growing evidence that private data entrusted to social media is 'mined' by outsiders.[2] With the spread of the Internet, also concerns about cyber security have become a part of our daily life.

Cyber security is a concept used in many different contexts. In this background report we will limit our discussion to security risks that are inherent to using the Internet. We do not consider ordinary crime that makes use of the Internet to be a cyber security risk. Instead, we distinguish between four types of cyber security risks:

- Availability (can we use the Internet without interruptions?)
- Integrity (can we trust that data we transmit over the Internet or store on connected devices are not tampered with?)
- Privacy (can we trust that data is not used by parties whom we did not give permission to view and use?)
- Identity (do we know who we communicate with? how to protect against fishing and spam?)

Cyber security has acquired a permanent spot on the agenda of policy makers around the world. In the last five years, many national governments in the EU and elsewhere have set up national cyber security centres and 'digital' police task forces to cope with security in cyberspace, and with cyber criminals using the Internet as their domain of operation. In June 2011, the US Secretary of Commerce Locke declared that: "*Today, the Internet is again at a crossroads. Protecting security of consumers, businesses and the Internet infrastructure has never been more difficult. Cyber attacks on Internet commerce, vital business sectors and government agencies have grown exponentially*" (US Dept of Commerce, 2011). In February 2013, the European Union published its *Cyber security strategy of the European Union: an open, safe and secure cyberspace*, the EU's comprehensive vision on how best to prevent and respond to cyber disruptions and attacks (EC, 2013a). The OECD calls for a "*holistic review of prevailing incentive structures […] to identify where and how production of protective countermeasures to systemic threats has been undermined, and policy makers should consider what fiscal and regulatory options are available to address such market failures*" (2011a).

This background document offers an economist's perspective on Internet security. The paper is primarily concerned with the behaviour of standard Internet users and not so much with the

incentives for criminals, nor with the business opportunities for companies that sell cyber security solutions. Rather, we focus on the following question: Under which conditions will markets provide solutions for cyber security issues, and in case they do not arise, what can governments do? We discuss market failures that are most likely to lead to cyber security investment levels that are insufficient from society's perspective as well as other forms of unsafe behaviour in cyberspace.

Intervention by national governments and international cooperation may be desirable, if the costs of intervention (including administrative burdens on firms) are smaller than the damage caused by cyber security problems. Economic theory offers standard solutions for categories of market failures that also apply to cyber security. For example, we discuss solutions for asymmetric information problems (how to identify reliable market partners) and for coordination failure (how to get safer Internet standards adopted). Externalities of investments in cyber security have some distinct features that, to our knowledge, have not received attention in the literature.

1.1 An economic perspective on cyber security

An economic perspective on cyber security emphasizes that individual firms and Internet users may have different security demands and interests. Such a market-based approach also searches for self-disciplining mechanisms (monitoring each other, effective feedback) based on incentives, with minimal government intervention. This view is not (yet) very common in the literature on cyber security. Broadly speaking, three perspectives can be distinguished in the literature:

- The 'engineer's approach' to security is geared towards the best possible security of Internet through more robust software, more encryption, better data integrity checks, and better technical standards. Technical standards and innovations are key elements in this approach, but cost aspects tend to receive less attention.
- The 'homeland security view' on cyber security is oriented at eradicating illegal domestic activities and foreign activities that endanger vital national interests, and that diminish the security of private persons and firms in the country. National borders and state intervention form key elements in this approach.
- The 'market-based approach' aims at creating efficient economic mechanisms that are disciplined by the market parties themselves, by aligning different security interests through prices and other market signals. Costs, benefits and the flexibility of decentralised decision-making are key elements.

The three approaches are different, but they have overlaps, and may well be complementary. For example, the homeland security view might seem less appropriate when international security issues are driven by economic mechanisms that are by nature border-crossing, but it may be indispensable when market-based solutions are not feasible. The 'engineer's approach' (innovations in the security area) sets the stage for both the market-based and 'homeland security' approaches, but 'ideal' technical solutions to security might be too costly or might see little demand because of market failure.

Cyber security is not a free lunch, neither for individual persons or firms, nor for society at large. Moreover, the costs of achieving higher security levels will increase as the technological challenges get more complex. Initially, relatively simple and cheap measures like changing

passwords, making backups and regular updates of security software can be taken, but the closer one gets to what is technologically feasible, the costs of further steps may rise. Beyond some point, additional security benefits will no longer compensate the costs of the additional resources needed to reach a higher security level.

End users like firms and households make independent decisions –explicitly or implicitly– on the level of security they desire. They only look at their own (private) costs and benefits. For society as a whole, the outcome of this decentralized decision process is not necessarily optimal. Economic theory specifies the conditions under which a decentralised market outcome is likely to lead to socially optimal the level of cyber security.

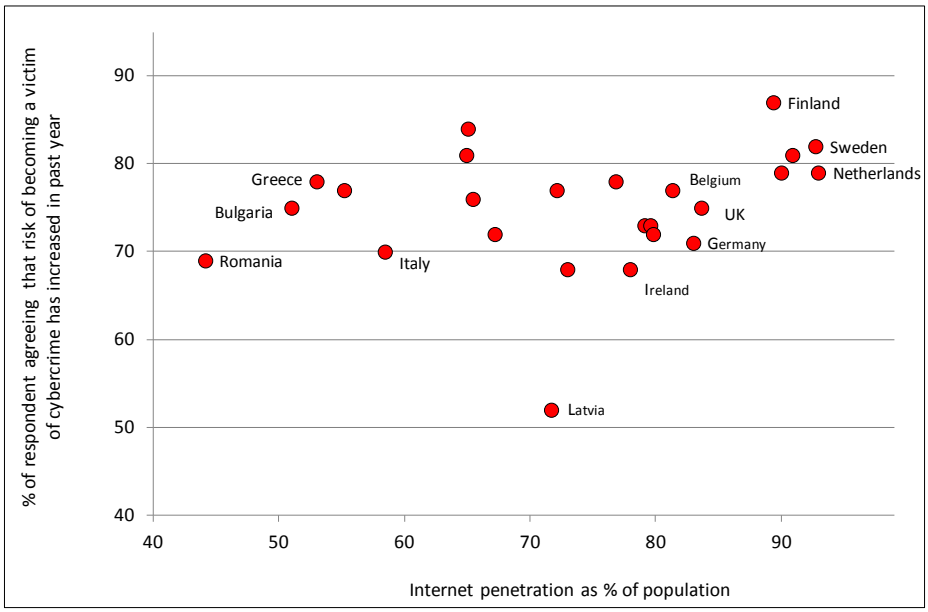
Many papers have been written about cyber security from a technological perspective, but few papers have focused on the market failures that aggravate security problems.[3] Mostly, these studies focus on one or two market-failure aspects in cyber security. Our contribution to the literature is that we perform a more systematic analysis of market failures that affect cyber security. Does the free play of market forces provides an adequate solution to different security aspects, and if this is not the case, what could be the role of governments? In answering these questions we build on the wealth of studies on general market failures in the economics literature.

We suggest various policy instruments that might mitigate market failures due to asymmetric information (how to identify reliable market partners) and coordination failure (how to get safer Internet standards adopted). In addition, we analyze the conditions under which markets can provide solutions for security externalities that Internet users pass on to each other. In most contexts, intervention by national governments will require international cooperation in order to be effective.

1.2 Is the Internet getting less secure?

In 2012, the European Commission commissioned a large survey among EU citizens (including people not using the Internet) to assess their experiences with and perceptions of cyber security.[4] The survey found that between seventy and ninety percent of Internet users were convinced that the risk of becoming a victim of cyber crime has increased during the preceding year. Figure 1 shows the results per country. The figure suggests that the perceived risk hardly depends on Internet penetration.

Figure 1 Perceived risk of becoming a victim of cyber crime increased during 2011−2012, EU



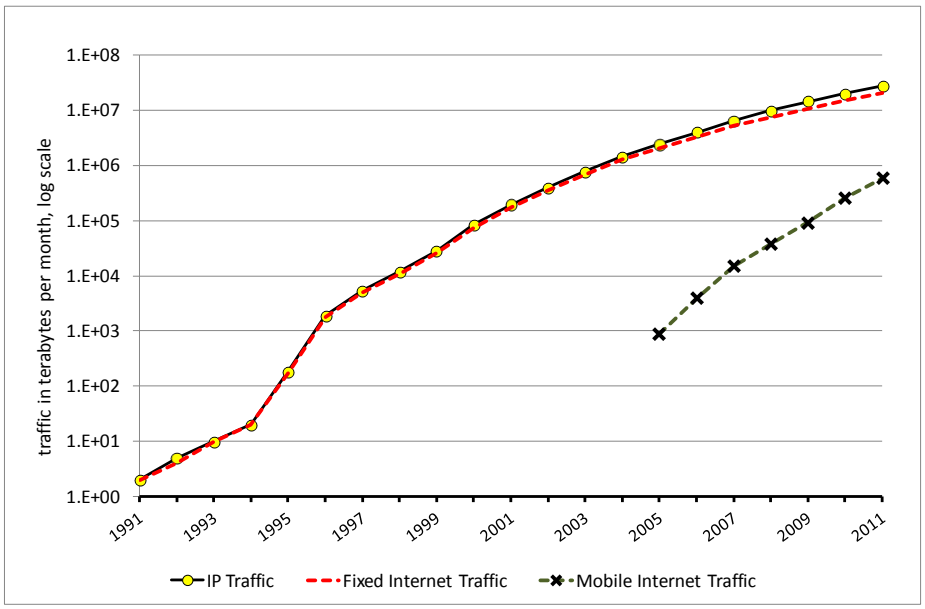
Note: vertical axis gives the percentage of Internet users that agreed with statement "The risk of becoming a victim of cyber crime has increased in the past year", average country scores. Sources: (EC, 2012c); Internet penetration ratios are derived from: http://www.Internetworldstats.com/ (retrieval 20 February 2013).

The increase in perceived risk is rather constant across countries, but behind these perceptions are different experiences. From same survey it emerges that, on average across the EU, eight per cent of Internet users say they have at least once been a victim of digital identity theft, but in Romania and Hungary this is, respectively, 16 and 12 percent. Some forms of cyber crime seem to be targeted at high-income countries. For the EU as a whole, 38 percent 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 percent in, respectively, Bulgaria and Poland (EC, 2012c: 50).

The numbers mentioned above suggest that cyber security is quantitatively important, but a proper discussion of the question whether the Internet is becoming less secure over time requires that the number of incidents is corrected for the growth of Internet. Ideally such a measure reflects the number of "transactions" on the Internet or the time spent on the Internet by its users, but these data are hard to come by. In stead we use normalize using the volume of internet traffic per year.

An optimistic measure of Internet growth simply is the number of bytes transmitted. Figure 2 shows evolution of Internet traffic from 1990 onwards. Various factors contribute to the growth of traffic: more users connect to the Internet at higher speeds, with more devices, and for more hours a day. Although the Internet is still growing rapidly (especially mobile transmissions), growth is less than exponential in recent years.

Figure 2 Growth of Internet traffic volume is slowing, 1991-2011



Source: constructed from CAIDA data, cf. CAIDA (2011).

A second, more conservative indicator of Internet growth is the growth in the number of users. The number of Internet users worldwide increased from roughly 361 million in 2000 to 2.4 billion in June 2012 (Table 1). Asia accounted for about half of the absolute growth in Internet users between 2000 and 2012. Asia now is home to 44 percent of all Internet users, Europe has a 21 percent share,[5] and North America and Latin America each have an 11 percent 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	Internet users				Population (mln 2012)	Internet penetration (% pop.)
	2000 (mln)	2012 (mln)	2012 (% total)	Growth (%)		
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

Notes: 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, http://www.itu.int/GfK, local ICT Regulators, and other sources.

For the measurement of the growth of cyber security incidents we use a set of seven more or less time-consistent data series in order to cope with the multiple dimensions of cyber security.[6] The growth of these indicators is normalized by the growth of Internet traffic (optimistic) or the growth of the number of users (conservative).[7] Table 2 gives the results. Our overall finding is that the number of cyber incidents per unit of transferred data tends to fall, suggesting that the Internet has become safer over time. This is shown particularly by the last two columns of Table 2. The average normalised growth of cyber incidents in the last four data years has fallen in all cases except for the number of phishing attacks.

Table 2 Relative growth in cyber security incidents, 2001-2011

Type of incident	Period	Avg. yearly growth full period	Normalised growth	
			Full period	2008-2011
Total vulnerabilities detected by Symantec	2001-2011	8.1	-20.8	-16.3
Browser vulnerabilities	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
Botnet-infected computers	2006-2009	-0.4	-24.4	-26.6
Unique phishing messages	2005-2007	23.3	-4.6	N.A.
Observed phishing domain names	2009-2011	15.5	-3.0	-3.0
Phishing attacks	2009-2011	24.4	5.8	5.8

Notes: Browser vulnerabilities include documented vulnerabilities in MS Internet Explorer, Apple Safari, Mozilla Firefox, Opera, and Google Chrome. Normalised growth rate is corrected for the growth in Internet traffic. Sources: 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).

A few caveats should be taken into account. No reliable and consistent data series are available on the average harm per incident. Part of the data on cyber incidents stem from Symantec, a firm that sells Internet security software and services. If anything, this firm has an incentive to exaggerate cyber threats. Table 2 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 cyber incidents are now averaged for the world as a whole. Better data quality, a better consistency over time, and statistical independence is required for future cyber security policy-making.

The finding that, the Internet 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 cyber incidents, and that the associated insecurity hampers the development of online economic activity.

1.3 Outline

The structure of the paper is as follows. Chapter 2 provides an overview of market failures related to cyber security. Particular attention is paid to security externalities and underlying issue related to awareness and attribution. Chapter 3 applies the concepts discussed in the previous chapter to the backbone systems of the Internet and the ‘last mile’ of the Internet infrastructure. Chapter 4 focuses on how the behaviour among end users (households, firms and governments) influences cyber security. Chapter 5 concludes.

2. When do markets fail to provide security?

The level of protection against cyber criminals that users and providers of Internet choose might not be optimal for society. This chapter explains the basic economic mechanisms that may cause this problem. Under what circumstance do free-functioning markets fail to provide socially optimal security? And what can governments do to reduce these market failures? We consider the following distinct sources of market failure: 1) non-excludability and non-rivalry, which forms the basis for distinguishing private goods, public goods, common goods, and club goods; 2) information asymmetry and its consequences: moral hazard and adverse selection; and 3) externalities (non-priced welfare effects) for which market solutions may be hindered by three problems: lack of awareness, attribution and enforcement. How these market failures matter for cyber security will be discussed in Chapters IV and V.

2.1 Public goods, common goods, and club goods

Markets are based on the exchange of ownership rights. A buyer gives up the ownership of the money that he owns (or that he is legally entitled to spend on behalf of someone else) in exchange for the ownership or use rights of the goods[8] owned by the seller. Without property rights, be they formal or informal, markets cannot exist and goods cannot be allocated efficiently.

For some types of goods property rights are insufficient to ensure their efficient allocation. When it is difficult to exclude people from using a good, it will also difficult to sell that good. In this case markets fail because property rights are too weak. When goods can be produced at zero (or very small) marginal costs (i.e. goods are non-rival), the quantity produced might be small relative to demand in order to maximize profits. In this case markets fail because property rights are too strong. Information nowadays is a good example of a non-rival good. Depending on the context, information can also be difficult to exclude. Both aspects of information have implications for cyber security.

Table 3 shows the four categories of goods that can be distinguished on basis of rivalry and excludability in consumption of the good. For private goods, the existence of property rights is sufficient for efficient allocation (provided there are no other market failures). Common goods, or common resource pool, are goods that are freely accessible, but that can be depleted (for example sea fish) or that can be congested (for example roads or DNS servers). Club goods cannot be depleted or congested, but access to these goods can be restricted by the owner (example: Internet exchanges). The last category is public goods, which are freely accessible and are not subject to depletion or congestion (for example protection against water provided by dikes; communication protocols).

Table 3 Property rights and good characteristics

		Is the use of the good excludable?	
		Yes	No
Is the use of the good rival?	Yes	Private goods (exclusive private ownership) *e.g. hardware devices*	Common goods (freely accessible, can be congested or depleted) *e.g. DNS servers*
	No	Club goods (restricted access, congestion or depletion not binding) *e.g. Internet exchanges*	Public goods (freely accessible, no congestion or depletion) *e.g. communication standards*

What can policymakers do to reduce the inefficiencies caused by non-excludability and non-rivalry? Depletion or congestion of Common goods can be avoided by regulating access to the common resource pool. Based on an analysis of successful management systems for communal resource pools, Ostrom (1990) and her research associates (Dietz et al., 2003) derived the following requirements for successful management of common goods: (a) conventions over who can use the common resources and when; (b) proportionality rules: what you take out of a commons has to be proportional to what you put in; (c) usage also has to be compatible with the commons' resilience and integrity; (d) everyone has to have some say in the management rules; (e) monitoring each other's resource use; and (f) adequate feedback systems: more attention to conflict resolution than to sanctions and punishment.

The owner of a club good restricts access to the good in order to maximize profits. With marginal (re-) production costs equal to zero,[9] it would be socially optimal to charge no price for this good. Policymakers can stimulate wider use of a club good without reducing the incentives for the owner to provide it by giving a subsidy on the access price or regulating the membership fee.

Public goods are a classic example of market failure that leads to government intervention. Firms have no incentive to produce a public good as they cannot charge a price to its users. As no price can be charged, a subsidy on its use also has no effect. In contrast with common resource pools, there is no reason for regulating access because there is no risk of depletion or congestion. For public goods, the optimal solution is to finance them by levying a tax and to provide unregulated access.

2.2 Asymmetric information

The safety of a connection over the Internet depends in part on the security levels of ISP's and other infrastructure providers and in part on the security levels of its end users. Knowledge about the security of a connection therefore requires knowledge about the behaviour of many different parties. This introduces uncertainty about security that is almost absent with centralised communication networks, like traditional telephone networks.

Lack of knowledge about the security behaviour of other users gives rise to a class problems that are known in economics as problems of information asymmetry. Asymmetry in information between users can give rise to two (related) types of problems: moral hazard and adverse selection. Moral hazard occurs when the incentives of users are not aligned and information is

asymmetric (monitoring might be impossible or difficult). In this situation, a user may act against the interests of other users as the other users cannot observe its behaviour. For example, a firm might not want to invest much in keeping its customer data secure as its customers most likely will not find out their data is insecurely stored - even after a security breach has taken place (see also Section 3.3 on externalities). When there is a moral hazard people will be less inclined to share data with each other, which can lead to welfare losses.

When asymmetric information is not limited to a single firm, but is widespread this can reduce the overall level of security offered in the market. Buyers who are unable to verify whether the level of security that is advertised is correct, will not be willing to pay a higher price for more secure products. Firms that offer superior security will not see higher demand for their for products compared to competitors that offer a similar product with inferior security features. Assuming that providing a secure product costs more than providing an insecure product, high-security firms will be competed out of the market by low-security firms. Competitive forces will reduce the level of security even when individual firms have no intention of providing products that are less secure than advertised.

If adverse selection makes it difficult to buy and sell secure products, firms or households could in principle buy additional security in the insurance market. If such insurance policies would be available, they would not raise security, but they would distribute its costs more evenly and predictably over the insured. However, this type of insurance has not taken 'taken off' due to adverse selection in the insurance market. Firms have an incentive to under-report data and security breaches, because revealing security breaches may harm their reputation and may affect their insurance premiums. For these reasons, insurance companies lack knowledge about cyber security risks, preventing them from charging appropriate insurance premiums.

Of course, insurance companies could simply charge premiums based on average historical risks. This will not work if the insured have more information about the risks they run. In this case, insurers would start to suffer losses as they would only attract clients with above-average risks (Moore et al. 2009, ENISA 2012b, Lelarge and Bolot 2009). Insurance firms can respond to adverse selection in the insurance market by offering contract with different levels of risk sharing, but this only mitigate the problem.

2.3 Externalities

An externality occurs when the production or consumption choices of economic agent A have a direct influence on the welfare situation of economic agent B without agent B's consent. Externalities lead to market failure if they affect agent B's welfare in ways other than though prices.[10] Such externalities lead to market failure as people do not take into full account the consequences for others.

Externalities can have positive or negative consequences for agent B. An example of a positive externality is that a new Internet connection not only benefits the new user, but also existing users. They get the opportunity to connect to the new user without having to pay. Only part of the gains to society from that new connection accrues to the new user, even though this user carried all the costs. A subsidy on internet connections could in this example lead to an increase in social welfare. An example of a negative externality is when an insecure computer is added to a network. The owner of the insecure computer might have decided that investing in security is

not worthwhile, but he did not take into account the consequences for the other users of the network. The user with the insecure computer captured all the benefits of the connection, but was not charged all the costs. As a result, the user did not invest sufficiently in security from society's point of view.

Whether an externality is positive or negative can be a matter of perspective. Improving the security of a computer can be seen as a positive externality or as a reduction of a negative externality caused by an insecure computer.

The examples mentioned above are illustrations of a particular type of externalities known as a network externalities. Positive network externalities exist if the utility of a service increases with the number of other users who are also using this service, e.g. smart phones and other communication devices.[11] Negative network externalities occur when the network is congestion-prone, or when the safety neglect by one network users creates higher security risks or costs for other network users (botnets).[12]

How can the problems caused by externalities be addressed? Standard solutions in economic theory are to tax activities with negative externalities (Pigouvian taxes) or sometimes to prohibit these activities, and to subsidies activities with positive externalities. If the number of agents causing and/or absorbing externalities is small, private negotiations might mitigate externalities without government involvement.

Suppose firm 2's profits are negatively affected by activity *x* of firm 1. If action *x* is illegal, then firm 2 may bring firm 1 to court, and the court will ensure that 2 is compensated by 1. If legal costs would be negligible, this would be an efficient market solution: the externality-causing party pays the victim. But now consider the situation that firm 1 is legally entitled to do activity *x* that causes the negative welfare effect for firm 2. Coase (1960) has shown that a second efficient market solution for the externality arises if firm 2 pays a compensation to firm 1 for stopping with its activity *x*. If the compensation is larger than the costs of stopping with activity *x* firm 1 will accept the compensation and the profits of both firms are improved.

However, if the compensation offered by firm 2 is smaller than the costs of stopping with activity *x*, firm 1 will refuse the compensation and will continue his activity. Now, if firm 2 does *not* increase its compensation offer to a level that is at least equal to firm 1's costs of stopping the activity, then the current situation is socially efficient, even if the externality persists. Coase (1960) shows that in a competitive economy with complete information, the efficient allocation of resources does not depend on the legal rules of ownership. Ownership rules, however, matter for the distribution of income and thus for efficiency in consumption: the utility of an extra euro is higher for households that have a lower income.

When more than two parties are involved, bilateral negotiations on compensation cannot completely neutralize the impact of an externality. Suppose there is a firm 3 which is also affected by firm 1's externality, then this firm will benefit from any agreement between firm 1 and firm 2 which reduces firm 3's incentive to negotiate with firm 1. In this situation firms 2 and 3 have a first-mover disadvantage when they act individually. If they manage to coordinate their actions, a first-best outcome is still feasible. With a large number of firms negotiations can become too complex, leading to coordination failure. Government intervention might be warranted in this case.

First-mover disadvantages also occur when the value of a particular investment critically depends on similar investments by others in a network. For instance, the adoption of security standards may go along with additional fixed costs for the adopting firms. If the additional security benefits only occur once other firms also adopt the same standards, firms have disadvantage if they are early adopters. The first-mover disadvantage may obstruct a broad adoption of socially desirable security standards. In these cases, it can be efficient for governments to assist in building up critical mass through selective procurement practices (requiring adoption of security standards), awareness campaigns, regulation that takes away the first-mover disadvantage, or subsidies for early adopters.

The problem of addressing externalities runs deeper for issues related to cyber security. Information on the externality usually is imperfect or asymmetric in this context. In particular, there are two distinct informational problems:

- *Awareness*: the causing party must know that its own activity (or neglect) has a negative impact on the welfare of other parties, and the disadvantaged party must be aware that it is being harmed.
- *Attribution*: externalised costs must be *attributable* to the economic agent whose Internet-related activities (or security neglect) caused the externality. In addition, it should also be known *by what activity or by what neglect* the externality is caused.

The first condition for a market solution is that the involved parties are *aware* of the existence of an externality. Awareness often is insufficient when it comes to cyber security. Network parties may be unaware of the fact that what they do (or refrain from doing) affects others. Many data breaches involving theft of personal data from a database only get revealed to the database owner when such data are published or leaked. Owners of infected computers mostly are not aware that their PC forms spreads malware to other computers, or perhaps only that it is a bit slower than before. Seen from the 'victim's' side, the awareness condition is not trivial either. The victim will often not be aware that his personal data are stolen from a database. A victim whose computer has been turned into a botnet instrument may experience a diminished functionality of their computer, and have no idea that his computer is taking part in a DDoS attack on a bank or website.

Table 4 shows the awareness criterion for a two-firm situation. Three different awareness positions may arise: mutual awareness, asymmetric awareness, and mutual unawareness. In cases A and B, firm 1 knows that its activities may increase the costs of another firm, but might not be informed about the identity of that firm. In cases A and C, firm 2 has noticed that its own costs increase due to the activities of another firm, but might not know the identity of that firm.

Table 4 Awareness of externalities

		Firm 2, absorbing the externality	
		Aware	Unaware
Firm 1, causing the externality	Aware	A Symmetric awareness	B Asymmetric awareness
	Unaware	C Asymmetric awareness	D Mutual unawareness

If firm 2 is aware of the externality, it needs to be able to attribute the externality to firm 1 and it has to establish by what activity or reprehensible neglect the damage is inflicted - otherwise a market-based solution will not occur. If the precise nature of the externality remains unclear, both firms could still settle for second-best solutions like a lump-sum compensation.

Awareness asymmetry is less likely to persist if it refers to case C of Table 4. If firm 2 is aware of the externality it has an incentive to gather information on the source. Once firm 2 has attributed the externality to firm 1, it will inform firm 1 about the externality in order to negotiate a solution. Awareness asymmetry of type D is more likely to persist as firm 1 has no incentive to uncover the identity of firm 2.

When informational problems about the externality have been solved, a coordination problem might arise. In a situation where one firm causes an externality for many other firms, no single absorbing firm will be prepared to pay the externality-causing firm in order to stop the externality. Only when the absorbing firms are able to cooperate, a solution without government intervention is possible. The coordination problem is (even) more complicated when there are a large number of firms causing the externality.

When firms can come to an agreement on mitigation of the externality, effective legal institutions are required to make contracts enforceable. Negotiations by market parties need some common legal, moral or otherwise disciplinary framework that they both accept and to which they both can refer for conflict settlement. This may be a national legal system, an international code of conduct, a reputation system, but it can also be another behavioural or moral code (cf. Platteau, 2000).[13] The reputation mechanism between parties with repeated business contacts may also work as a disciplinary force against opportunistic behaviour.[14]

As cyber externalities often have a cross-border character and an international legal framework is effectively missing,[15] transaction costs of negotiating and enforcing a compensation agreement for cyber externalities across national borders might very well be prohibitive in many cases. Cross-border externalities also make Pigouvian taxes and subsidies less attractive when adopted by individual countries.

2.4 Market power

Economies of scale may be a reason why some firms manage to capture a large part of the market. Smaller competitors have higher production costs which prevents them from lowering their prices below the price of the dominant firm. Firms that are able to influence the prices at which products are sold in the market are said to have market power. Market power leads to market failure if profit maximization induces the dominant firm to set a relatively high price, such that fewer products are sold than would have been the case if competition is intense.

In the context of cyber security, infrastructure providers can derive market power from the size of their network. Large providers are difficult to avoid because they control access to many internet users. Lack of alternative providers might not only raise prices, but also reduces incentives to secure connections as customers cannot switch to another firm that offers more security. In other words, some firms are "too-big-to-block". When a firm becomes highly dominant, governments might need to regulate its security behaviour directly. This might be challenging if firms operate internationally like backbone providers.

2.5 Overview

Table 5 summarizes the main sources of market failure that are relevant for cyber security. The second column lists possible consequences and the last column summarizes possible policy instruments.

Table 5 Market failures and policy instruments

Source of market failure	Possible consequences	Policy instruments
Non-rivalry (club goods)	restricted access	subsidy on access price / membership fee
Non-excludability (common goods)	exhaustion, free riding, no incentives for private production	property rights, regulation
Non-rival, non-excludable (public goods)	free-riding, no incentives for private production	public provision
Asymmetric information	moral hazard, adverse selection	mandatory disclosure, certification, minimum security
Externalities	uncompensated harm, free-riding, first-mover disadvantage	tax, subsidy, minimum security standards
Market power	lack of alternative, high-security products on the market	competition policy, regulation of monopolies

3. Market failures related to infrastructure

> "*Is it time now to start thinking about a new and possibly non-existent public utility, a common-user digital data communication plant designed specifically for the transmission of digital data among a large set of subscribers?*" (Baran, 1962: 40)

This chapter focuses on the market failures that may explain security problems related to the infrastructure of the Internet. A distinction is made between security-related market failures that play a role in the national parts of the Internet (section 3.1), and those that play a role in the international infrastructure of the Internet (section 3.2).

The quote on top of this page is from Paul Baran, a RAND researcher who investigated the design of a shock-resilient communication system communication system that could stand a thermo-nuclear attack. He concluded that telephone and other centralised communications systems of his day were vulnerable to disruption. The reason for this is that the network nodes (switching centrals) formed single points of failure. If the nodes are destroyed or congested, a centralised communication system easily breaks down.

Baran (1962) had three messages for making a communication system more resilient. All three messages we still find in today's Internet architecture:

1. The system should have enough redundancy in the form of alternative connections nodes between any pair of end users.
2. The checking for completeness and integrity of the messages should be done by the end users, rather than by the network nodes.[16]
3. Messages should be split and sent in digital packages that may follow different routes, according to the available capacity at individual network nodes. The routes travelled by the individual data packets can be very diverse and difficult to predict. It depends on the availability and congestion peeks in connection nodes. The packages are reassembled by the end user rather than by the nodes.

These choices make the end users more autonomous with regard to the contents of the messages sent, while the network operator's role is reduced. Nevertheless, the behaviour of infrastructure providers remains important for the security of the Internet.

3.1 National networks

The most important national network players are the ISPs. Other important players are the national registries that administer a national web address domains (such as the websites ending with suffixes like ".nl", ".uk", or ".de"), and the web-hosting agents that sell the temporary right to use a certain web name.[17]

ISPs generally operate in a market environment. They have several types of commercial contracts that could generate incentives for better security performance. With their clients (end users: firms, households, others) they have service-level contracts. With colleague ISP-networks they have peering agreements about the traffic they send over each other's lines. And finally

they may have transit contracts with IDXs and large international network operators about the traffic they send and receive through these backbone connections.

The contracts of ISPs with their customers guarantee a certain level of Internet-access availability, bandwidth allocation and transmission speed for uploading and downloading, and often some additional services.[18] ISPs get a problem with their clients if Internet access and transmission speed go down due to security problems. Their helpdesks will be flooded with phone calls from angry customers; if they are not to lose these customers they have to invest in helpdesk capacity and safety.[19] Bringing down the share of distressed customers gives ISPs a clear incentive to care about cyber security.

The incentives for ISPs to secure their networks might be insufficient. Competition between ISPs is based on price and connection speed, not on their security performance. Even though some ISPs offer spam-filter or anti-virus services, their (potential) clients generally cannot observe which of the ISPs performs better, because independent ratings of the security performance of ISPs are generally lacking. Customers or potential customers will, therefore, assume that an ISP's advertisements of its security performance are unreliable.

The result of a lack of trust by customers is adverse selection: offering better security services only leads to more costs, while it does not bring a more revenue. This is a suboptimal outcome for society as end users with a preference for secure Internet access are not adequately served. National governments can reduce this information problem by requiring ISPs to report security breaches[20], by imposing minimum norms for security levels, or by mandatory certification that discloses the level of certification provided.

Failure to adopt more secure standards is another factor that hampers Internet security. The adoption of superior security standards often involves substantial fixed costs for ISPs. In some cases they even have to run double systems for a while: one based on the old standard and one on the new standard. Whether an ISP's support of a new standard improves security depends on the behaviour of others as the standard can only be used effectively once it is widely adopted. This creates a first-mover disadvantage for ISP's: in isolation no ISP will find it worthwhile to switch to the new standard. Only when ISP's can coordinate their behaviour, new standards will be adopted.

An important example of a slow adoption of a secure standard is IPv6. The Internet Assigned Numbers Authority (IANA) is the international authority that gives out the IP addresses used as unique addresses for sending packets to individual computers. The currently used IP-address identifying system is called IPv4, which has 32-bit (four-byte) addresses, implying a maximum number of 4294967296 (232) addresses. However, the demand for IP-addresses is rapidly approaching this limit: in February 2011, the IANA issued the last free IPv4 address blocks to the regional Internet Registries. The IANA therefore has created a new protocol for computer addresses called IPv6.

The delay in the IPv6 roll-out has a negative impact on cyber security, because it is directly linked to a more secure safety protocol (IPSEC). Although IPSEC can optionally also be used in combination with IPv4, it forms an integral part of the actual versions of IPv6.[21] So, adoption of the IPv6 standard will imply a general increase in cyber security. Except for its IPSEC

component this is also caused by the fact that the IPv6 addresses are longer and more complex, which makes the hit rate lower for randomly targeting cyber criminals.

Governments can facilitate the adoption of more secure standards by setting a timetable for implementation and require that ISPs report the progress they make to the other ISPs. If necessary, governments could also make the new standard mandatory. Alternatively, governments can sometimes start using a new standard itself or provide a temporary subsidy on the use of the new standard.

Peering contracts with other networks provide another incentive for ISPs to keep their networks secure. Contracts with other networks are based on reciprocity, the so-called 'fair use' principle. If an ISP sends a more than proportional amount of malicious traffic, video traffic or real-time information traffic over its contract partner's network, this would be regarded as a violation of the fair-use principle.

Networks have a range of escalating options to retaliate for poor security practices with regard to outgoing malicious traffic. If earlier notifications have little results, this will damage the ISP's reputation vis-à-vis other ISPs. Malicious traffic (spam, phishing mails, virus-infected messages, DDoS activities of botnets) sent from infected machines within one ISP's network triggers abuse notifications from other ISPs, with requests to fix the problem. If the ISP does not improve its security, peering agreement can be cancelled (cf. Bauer and Van Eeten, 2009). The peering agreement will then be replaced by a fee-based transfer contract. In extreme cases an ISP can be blacklisted.[22]

Though the dependence of ISPs on the security of each other's networks may discipline most ISPs, it might not work for the largest ones. The largest networks are the Tier 1 networks[23], which have substantial market power. No single ISP can afford to exclude or blacklist them. According to Moore et al. (2009) much of the world's bad traffic at presently comes from these "too-big-to-block" networks. Too much market concentration weakens the disciplinary power of the existing commercial contract system between networks. When a firm becomes highly dominant, governments might need to regulate its security behaviour directly. This is not uncommon for firms that provide large infrastructures, including railway operators and telecommunication companies.

3.2 International backbone of Internet

Three market failures stand out as important obstacles for improving global cyber security. This section will subsequently review these market failures: (a) coordination failure in the adoption of safe Internet communication standards, (b) adverse selection generated by flawed products of certification agencies, and (c) under-investment in spare capacity due to externalities.

A first market failure is related to the trustworthiness of identity certificates. Certification authorities have a key role in establishing the digital identities of end users that exchange traffic via the Internet. This is particularly important if the communication requires the exchange of sensitive private information, as is the case for ecommerce, online banking and e-government traffic.

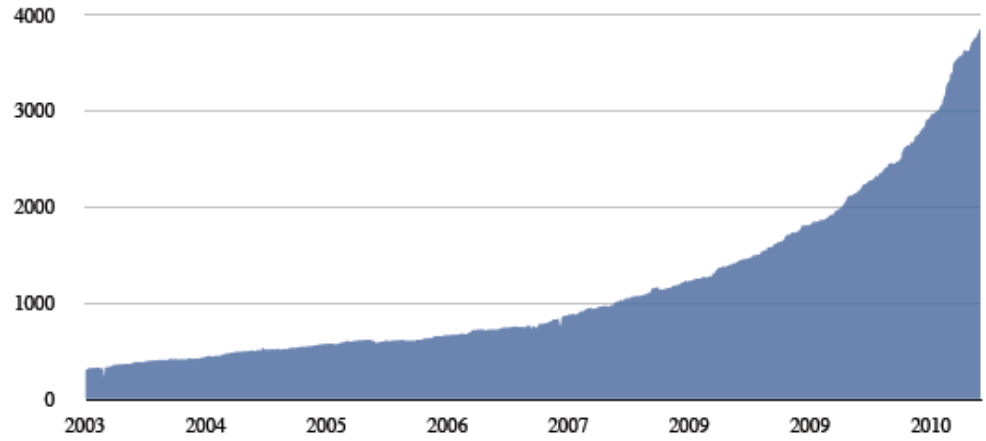
Recent security breaches (e.g. Diginotar) and malpractices at several certificate authorities have led to a global reduction of trust in these central mediators (cf. Arnsbak and Van Eijk, 2012).

Several of the resource persons interviewed for this research mentioned that an adverse selection is an important market failure in the market for certification services. Clients cannot or only inadequately judge the quality of the certification services. This strengthens a tendency towards a situation, in which the high-quality agencies can no longer credibly distinguish themselves from agencies that offer cheap inferior certification services.

Reportedly, many certificate users, including banks, buy too many cheap certificates that offer inferior protection against identity fraud and other criminal activities. One way to resolve adverse selection due to asymmetric information is to create a high-profile international supervisor of certification agencies, for example one that resides under the responsibility of key Internet-governance organisations like IANA and ICANN.

A second market failure relates to the adoption of new, more secure, standards like IPv6. The introduction of the IPv6 Internet architecture and the transition from IPv4 to IPv6 is a major change that entails costs for individual computer networks around the world. The adoption of IPv6 is a very slow process which can be seen from Figure 3

Figure 3 Number of networks prepared for IPv6 addresses



Source: Packet Clearing House, Weller and Woodcock (2013), based on advertised IPv6 addresses in global routing table.

Many networks have yet to begin their transition. In particular, in March 2013 more than seventy percent of the core connection points in the global Internet infrastructure –the Internet Data eXchange points or IDXs– were not prepared for the IPv6 standard.[24] This is shown in Table 6. In the Netherlands, the Amsterdam Internet Exchange is one of the larger IDXs, and it is prepared for IPv6; however, the Groningen Exchange Point and the Friesland Exchange Point were reported not to be ready yet.

Table 6 Readiness of Internet Exchange Points for applying IPv6, 2013

	EU	USA and Canada	Asia	Latin America	Australia, New Zealand	Other
Internet Exchange Points	108	89	51	31	15	63
Not ready for IPv6	67	73	40	25	10	49
% not ready for IPv6	62	82	78	81	67	78

Note: Mainly Russia and former USSR, Middle East, Africa. Source: Data Packet House website data retrieval February 2013 (https://prefix.pch.net/applications/ixpdir/summary/ipv6/).

Due to the slow adoption of IPv6, also the implementation of the cyber security standard IPSEC is delayed. The Internet addressing protocol has a key role in the routing of the Internet data packets. Delaying of the IPSEC security elements by some parts of the total Internet network has negative security externalities elsewhere in the network, because a network is always as strong as its weakest links. If cyber criminals exploit the lower standards in some part of the network, this may negatively affect the security elsewhere.

A third market failure could be that backbone providers and Internet Exchanges have insufficient incentives to maintain spare capacity. Redundancy in capacity might be needed to defend against large scale attacks that lead to congestion in parts of the Internet. If one route is congested, in principle data packets may be sent by another route. In the absence of capacity redundancy the scope for alternative routing is limited. Capacity redundancy in one network exerts a positive externality on the reliability of other networks. This may lead to underinvestment in spare capacity.

Cyber security and public-good aspects of Internet

The Internet has an open architecture, based on non-excludability with respect to the contents, origin or destination of the data traffic. Any private network may hook on, provided that they apply the basic data structure and addressing rules laid down in the Internet data transmission protocols.

Transmission protocols require all connection nodes, even if they are in private hands, to pass on data packets with the same degree of urgency, irrespective of their contents, origin or destination. As long as sufficient redundant connection capacity is available, all traffic can be served in an efficient and non-discriminatory way. This gives the Internet the characteristics of a public good: new nodes are not excluded and do not lead to congestion, i.e. they are non-rival.

The core of this open system is formed by the data transmission protocols issued and regularly updated by the Internet Society and its operational bodies (IETF, IAB).[25] The Internet Society was formed in 1992 with the purpose to provide a non-profit, multi-stakeholder corporate structure to support the development of Internet standards. The Internet Society and its operational bodies have neither formal property rights nor a juridical status for enforcing the adoption of their standards and transmission protocols by private parties. As a consequence adoption of safer standards and practices like the IPv6 protocol - that in the end would benefit all Internet users - is a slow and cumbersome process.

The problem of governing a global public good like the Internet can only be solved through international cooperation. Governments could solve this by an International Treaty on the Internet Commons in which they agree a timely incorporation of the IAB/IETF recommendations on safe data transmission that regulate ISP's.

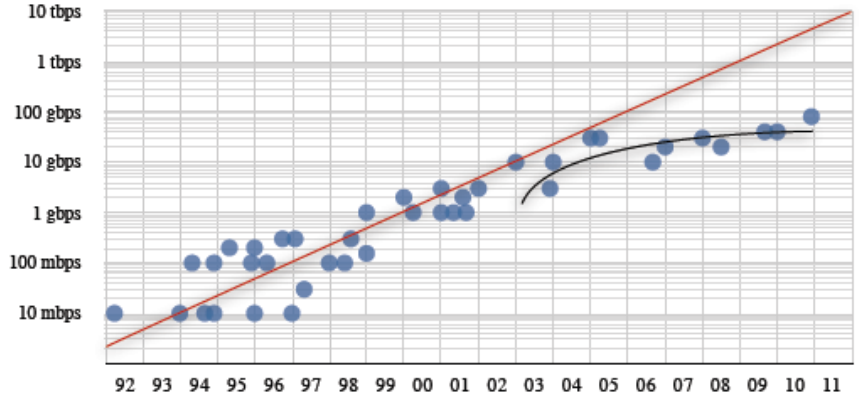
Odlyzko (2003) calculated that the entire US Internet traffic of end 2002 could have travelled on single fibre optic cable. Hence, much of the capacity was under-used at that time, and Odlyzko concluded that the overcapacity implied that transfer rates would be very low for the period to follow. This is what happened. The transfer fee paid for data traffic through the trunk

connections of the Internet is not only low but it has even has fallen since 2000. This lowered the attractiveness of doing further investments in fast connection capacity.

After the 'dot com' crisis of the 1990's the investment in fiber-optics R&D declined strongly. The results are shown in a stagnating speed growth of fibre-optic connection capacity (Figure 4). Each dot represents the deployment of a new interface speed within a major IXP, and the straight line is the same 115% annual growth in Internet data traffic speed.[26] The data express a trend that begins to change slope after 2001 and more or less hits a hard cap after the introduction of 10 gigabyte/second interfaces at the end of 2003.

Weller and Woodcock (2013) present evidence of an upcoming problem of underinvestment in backbone transmission capacity in parts of the OECD. According to them, a point of diminishing returns will quickly be reached, leading to slower traffic, congestion, and risks of spikes in transmission fees.[27]

Figure 4 Optoelectronic interface speeds used in the core of the Internet by year of deployment , 1992-2011



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

The resilience and supply security of Internet rests on a sufficient level of capacity redundancy. Work by Cohen *et al.* (2001) and Carmi *et al.* (2007) has shown that scale-free networks[28] like the Internet can be highly sensitive to intentional attacks, especially if their targets are not chosen randomly, but on the basis of their connectivity status. Systematic attacks on a few Tier 1 networks might be able disrupt the whole network. In March 2013 a large-scale (DDoS) attack[29] took place that came close to the type of intentional attack studied and simulated by Cohen *et al.* (2001). The botnet attack that was reported to originate from Cyberbunker in the Netherlands used a flaw in the Internet's DNS system to launch massive data attacks on Tier 1 networks.[30] The attack failed to bring the parts of Internet down, but it came closer than ever before.

A fourth type of market failure is related to the market power of the Tier 1 networks. Just like some networks cannot be blacklisted by ISP's, they might also be "too-big-to-block" for peer backbone providers. When a Tier 1 network would become highly dominant, governments might want to regulate its security behaviour directly. This might be especially challenging as backbone providers operate internationally.

3.3 Summary

Table 6 provides a summary of the market failures in national infrastructure discussed above, together with a number of policy instruments that could be used to remedy these market failures. A summary of market failures and their consequences relevant to the international infrastructure is given in Table 7.

Table 6 Market failures in national networks

Source of market failure	Possible consequences	Policy instruments
Asymmetric information		
Security is unobservable for ISP-customers	No competition on security performance of ISPs drives high-security ISP's out of the market	• Mandatory publication of security breaches • Minimum security standards • Mandatory certification
Externalities		
Standards adoption by ISP's	Adoption of secure standards by ISPs is hampered by first-mover disadvantages	• Set time table/ coordinate • Mandatory progress reports • Temporary subsidies • Government as first user • Mandatory standard adoption
Market power		
Provider is too-big-to-block	ISP's cannot afford to block large insecure international providers	• International regulatory initiatives • Stimulate capacity redundancy (alternative supply)

Table 7 Market failures at the international network level

Source of market failure	Possible consequences	Policy instruments
Asymmetric information		
Quality of certificates is unobservable	Insufficient competition on reliability of certificates drives high-security certificate authorities out of the market	• Mandatory publication of security breach parameters per certification agency • Create international supervising body (e.g. under IANA or ICANN) that monitors the quality of certification agencies and publishes their main results
Externalities		
Standards adoption by international network providers	Adoption of secure standards by Internet data exchanges, tier one providers and other parts of the international infrastructure is hampered by first-mover disadvantages	• International agreements
Network redundancy is public good	Stagnating investment in spare backbone connection capacity may render the Internet less resilient to sudden shocks (natural disasters, massive DDoS attacks)	• Create international facility for guaranteeing investment credit risk • Allow price increase for (now commoditised) transfer services to make investment in capacity redundancy more attractive
Market power		
Provider is too-big-to-block	Low competitive pressure on large international network providers with a low security performance profile because they are "too big to block" by peering partners	• International regulatory initiatives • Stimulate capacity redundancy (alternative supply)

4. Market failures related to end users

This chapter will discuss how market failures affect the security behaviour of end users of the Internet.[31] We make a distinction between three types of users: households, firms and governments.

The most visible types of cyber threats are those related to the applications used at the ends of the network. An application can be a hardware device or a software programs that communicates via the Internet or can be web-based code that operates through web browsers. Computer viruses form classical examples of cyber security threats at the application level. These threats differ from threats to the network infrastructure, because it lies within the power of the Internet's end-users to protect themselves against viruses by changing their behaviour and by investing in anti-virus software. Similarly, firms can protect themselves against hackers by installing better firewalls, better internal safety procedures, and by encrypting their databases.

4.1 Households

Households can influence their vulnerability to cyber threats in two ways. They choose the level of protection against avoidable cyber threats, and may limit the information they voluntarily share with others in Internet. The first choice concerns the level of investment in the safety of devices. Badly protected devices are vulnerable to external attacks (e.g. botnets), and thus create a negative security externality for the rest of the network.[32] By protecting their devices and consequently updating their antivirus software- they reduce the risk of virus infection for themselves but also for users with whom they are in contact. The risk of passing on infected mails or data to others is reduced by this action.

Suppose every computer but one has updated antivirus software installed, then the risk of infection by a (known) virus is negligible for the unprotected computer. In this situation, the user of the unprotected computer has no incentive to buy antivirus software. This user is free-riding on the security efforts of the other Internet users. As more people start free-riding the costs of protection for individual users will go up. This may lead to an inferior equilibrium in which viruses are widespread, and protection is too costly for any individual user. Statistical data on geographical spread of computer and software vulnerabilities suggest that this inferior security equilibrium is often found in developing countries.[33]

Passing on security risks to others forms a negative externality. Awareness, attribution and enforcement are fundamental problems for market solutions to underinvestment in security and security risks that are passed on to Internet contacts. Many households are inadequately informed about the risks they are taking and therefore do not see the full benefits of security investments. In addition, households generally do not know the level of protection of the people they are communicating with. Even when their computer is infected, they often have limited knowledge of the origin of the infection. Conversely, they do not know who to hold responsible when a security breach occurs. Even when the source of security breach is known, the size of the damage might be small relative to the costs of enforcement.

Policy makers may try to limit the externalities due to insecure computers through awareness campaigns and by imposing minimum security standards.

Household behaviour may indirectly stimulate (cyber) crime by using software that enables anonymous communication like TOR (short for The Onion Router). Similarly, e-currencies like Bitcoin enable anonymous transfers of money. Anonymous communication can be a good thing in countries lacking a free press. However, these networks also create 'underground' communication and payment systems that are widely used by cyber criminals. Anyone opening up his or her computer to such a network poses an externality on society by complicating law enforcement. This can be considered as a negative externality in countries where law enforcement is broadly regarded as beneficial to society. A second disadvantage of anonymous communication is that security breaches become more difficult to attribute. Policy makers may reduce the negative effects of anonymous communication by regulating the use of such software. For example, the government might demand that it can encrypt all communication on the network.

Another category of behaviour derives from the information that household members voluntarily share on Internet. The amount and diversity of personal information that becomes available is growing fast - partly because of the increasing popularity of social networks. Sharing personal information can have negative externalities from the viewpoint of cyber security. Especially on social networks there is social pressure to share information with others. Sharing less than other members lowers your social status. People that share much information raise the incentives for others to share more as well. The security and accessibility of social networks then becomes an important factor in the safety of Internet.

The externalities related to social status ("positional externalities") are not unique to social networks.[34] When much personal information is available, criminals will find it increasingly worthwhile to invest in technology that can systematically exploit these data for activities like identity theft, spam, and phishing.[35] Systematic identity theft would be less profitable for criminals if everybody would be careful with their personal data.

What is the order of magnitude of cyber security externalities? Rao and Reily (2012) have compared the economic impact of three externality-causing activities: driving automobiles, stealing automobiles, and spreading spam emails. Spam itself is a typical example of a negative externality for email users. Every day about 100 billion emails are sent to valid email addresses around the world; in 2010 an estimated 88 percent of this worldwide email traffic was spam (Rao and Reilly, 2012). Spam may cause disproportionally large costs for society yield compared to relatively small gains for the spam senders. Rao and Reily call this the externality ratio, and calculate it for driving automobiles, stealing automobiles, and spreading spam emails in the USA.

Table 8 shows that in the most conservative estimate the total externality costs for spam emails are about equal to those for automobile theft. The last column shows the externality ratios. The most conservative estimate finds that the externality ratio for spamming is a factor 2 to 3 higher than for automobile theft. It means that for relatively small gains for the spammer a disproportionally large negative effect is imposed on the rest of society.

Table 8 Externality ratio for spam compared to other externality-causing activities, USA

Activity	Revenue/benefit for the externality-causing agent	Cost externality	Externality ratio
Driving automobiles	\$0.60 p. mile	\$0.02–0.25 p. mile [a)]	0.03 – 0.41
Stealing automobiles	\$400 –1200 million p. year	\$8 –12 billion p. year	6.7–30.3
Email spam	\$160 –360 million p. year	\$14 –18 billion p. year [b)]	39 –112

Notes: a) estimated air pollution costs. b) Cost to end users. Source: Rao and Reily (2012).

This example shows the economic relevance of finding solutions to cyber externalities like spam. Cyber incidents like spam, information leaking by hackers, but also forms of reprehensible safety neglect mean that some Internet users impose costs on other Internet users. Like in Figure 7, government intervention may be required to ensure that social benefits and costs are fully internalised. Before choosing on this path, it is worthwhile to consider whether market solutions are feasible. So let us consider what preconditions must be fulfilled before market-solutions to cyber externalities can be reached.

4.2 Firms

Whereas a security breach with a household often only has limited consequences for others, a security breach with a firm can easily have consequences that go beyond the firm itself: it may directly expose confidential data of customers, suppliers and personnel to cyber threats. The interests of customers, suppliers, personnel and investors only partly overlap with the interests of the management of the firm.

Diverging interests do not in themselves induce to market failure. The common market solution would be that customers[36] desiring better protection of their data pay a higher price. Problems arise as it often is not possible or very costly for customers to monitor the behaviour of the firm that do business with. Customers simply have to trust the firm to make the investments necessary to achieve the security level that has been agreed on. Asymmetric information induces moral hazard behaviour by firms (not making the desired investments to prevent security breaches).

The impact of asymmetric information for security levels is exacerbated when it is difficult to verify whether a security breach has taken place. In this situation, firms have an incentive to keep security breaches silent for fear of reputation loss or having to pay damages. Even when a security breach can be attributed to the firm by its customers, it can be difficult to verify whether this is due to underinvestment or due to bad luck.[37]

Moral hazard can be countered by parties agreeing in advance on a penalty for the firm when a security breach would take place. The firm then has an incentive to invest sufficiently in security, even in the absence of monitoring as long as three conditions are met. First, the level of the penalty should reflect the damage a customer is expected to have in case of a security breach. Second, the penalty should be paid regardless of the reason for security failure - otherwise the firm might mislead its customers about the cause of the security breach. And thirdly, the security breach should not lead to bankruptcy of the firm. When a firm cannot pay all penalties that have been agreed on, the firm also has limited incentives to protect itself against it.[38]

Customers will have greater trust in firms that have can insure against damages caused by security breaches. Currently, these types of insurances hardly are available as monitoring still is difficult for insurance companies as well. This means that firms need to rely on their own financial reserves to improve their trustworthiness. This market-based solution to the disadvantages of information asymmetry may induce scale economies (based on the available financial reserves) and raise entry barriers, introducing another market imperfection.

Markets can limit the consequences of information asymmetry through formation of reputation. Firms do care about the security of their customers' data because a good track record on security signals to customers that they make appropriate investments. The more reliable a firm's track record is, the more customers will value its services. Reputation is a valuable asset for the firm, and it forms an incentive to keep its data secure in the future as well.[39]

Reputation as an incentive to counteract asymmetric information failures with respect to security investment may work not in all circumstances. Reputation takes time to develop, so it hardly works in new markets, because few firms have a track-record of any length.[40] Uncertainty about future innovations might make it unattractive for firms to build a reputation for rare security breaches. Moral hazard within firms may complicate the firm's ability to develop a reputation of being reliable.[41]

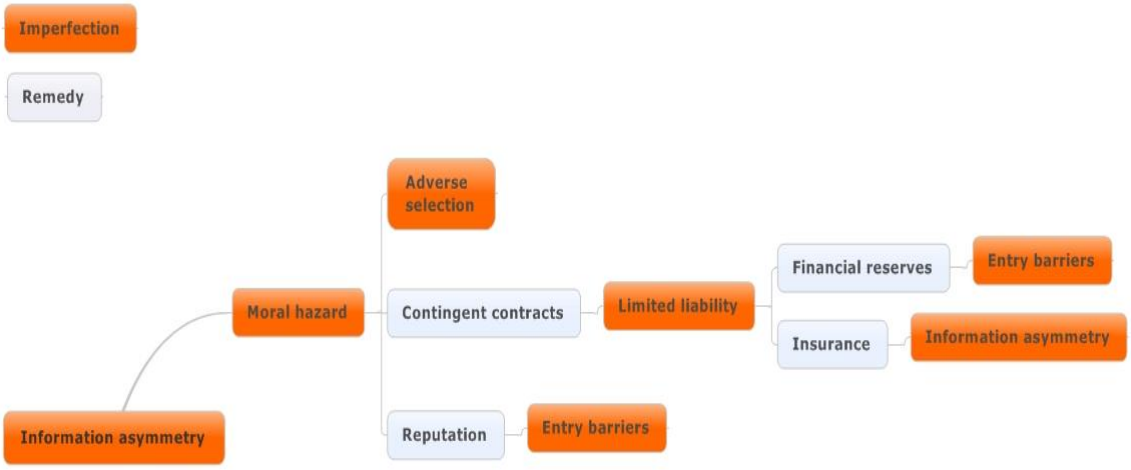
Once a firm has established a reputation it might deter entry by other firms that have not had the opportunity to develop a reputation. Formation of reputation as a response to asymmetric information therefore reduces competition by raising entry barriers.

Even when asymmetric information gives rise to modest underinvestment in security, its consequences can be large because of an accumulation effect: firms use the services from other firms to handle their data. It is not just the security level of the firm that you do business with that matters, but also the security levels of the firm's suppliers. An example of this is the data storage and transfer service offered by Dropbox. This company employing about 70 employees has 50 million customers and relies on Amazon's Simple Storage Service (S3) rather than on its own servers. Dropbox users are dependent not just on Dropbox' security measures, but also on that of Amazon (OECD 2012, Internet Outlook 2012, Chapter 2).

Problems of underinvestment in security due to asymmetric information are not unique for data handling and storage, but also apply to software development. The security of a new software package is difficult to assess by potential buyers. Reputation mechanisms might not be sufficiently strong to provide an adequate solution for software packages that have strong positive network externalities for its users. Reputations require time to form. Positive network effects create a first-mover advantage for software developers. This creates perverse incentives to rush products to market before they have been adequately tested (Andersen and Moore, 2008). The market will be dominated by the firms that moved first, rather than by the firm that has the best reputation for security of its product.

Summarizing, asymmetric information on the level of security provided by firms does not necessarily lead to market failure as markets support mechanisms that re-align incentives. The drawback of these market-based solutions is that they lead to other market imperfections. Figure 5 gives an overview of market remedies and imperfections discussed above that might arise in response to information asymmetry.

Figure 5 Information asymmetry, market remedies, and market failures



Policy makers might limit information asymmetry and its consequences in various ways. First, awareness problems can be mitigated by requiring transparency on security breaches. Second, problems related to attribution can be improved by setting clear rules on who is liable for security breaches. Third, policy makers can address asymmetric information by offering certification and enforcing minimum standards. Such policies can help firms to credibly commit to security levels and as a secondary effect might reduce entry barriers.

4.3 Governments

Governments interact with firms and households on Internet for various purposes, including providing general information and tax returns. Some of these interactions involve information that the government's clients would like to remain private. Sometimes clients are required by law to supply information and sometimes they need to share information to benefit from a government service.

As is the case with firms the level of security provided by the government is not well observable by its clients. Although the problems caused by information asymmetry are similar, there are three reasons why governments behave differently from firms when it comes to securing other peoples data. First, for some transactions clients are obliged to interact with the government over the Internet. Clients that do not trust the government to spend enough effort to maintain security do not have the option to avoid interaction. It is generally not possible to switch to a competing government that has a better security reputation. While most firms to care about security because of competition from other firms, most governments experience little competitive pressure from other governments.

A second difference between governments and firms is that governments are often democratically controlled. Clients can put pressure on the government to improve their security through political parties. In anticipation of such pressure, ministers have an incentive to promote and monitor security before security breaches have taken place. In theory at least, the incentives of the government should be in line with the interests of most of the voters.

A third difference is that governments usually are larger than firms. This has positive and negative consequences. On the positive side, governments are widely recognized and have a reputation to maintain. On the negative side, governments are complex organizations that employ many people. This makes governments more vulnerable to asymmetric information within the organization. Chief executive officers may have a hard time controlling firms, but the job is tougher for ministers trying to govern the country.

A common response to asymmetric information in large organization is to impose more rules. In some important cases, however, rules are insufficient to achieve a secure environment. In particular, when the government relies on firms for providing security, governments need to take into account the reputation of the firms they do business with -- just like everybody else does. In bureaucratic organizations “soft” specifications of tenders submitted by firms are likely to be undervalued. Instead, “hard” specifications like the price of the offered products or services will be the decisive factor. This leads to the purchases that seem secure on paper, but can be fundamentally flawed in practice.[42]

4.4 Summary

It was argued that individual households have an incentive to under-invest in security, and that free-rider problems make it difficult to keep Internet a safe place. The externalities of unsafe behaviour by a single household are small, but when unsafe behaviour is common it can have serious consequences for all Internet users. A high level of security may require government intervention like information campaigns or subsidies for investment in security software.

The free-rider problems faced by consumers also apply to firms, but problems due to information asymmetry are likely to have more impact. As a firm’s customers usually are not able to verify how much the firm invests in security, which discourages transactions. Markets provide various mechanisms to alleviate the problems caused by information asymmetry, but they come at the expense of higher entry barriers and less competition. Policy makers might limit information asymmetry and its consequences by promoting transparency and by regulation liability for damage caused by security incidents. In addition, policy makers can provide certification and require minimum standards.

Table 8 Market failures related to end users

Source of market failure	Possible consequences	Policy instruments
Asymmetric information		
Security of (personal) data is unobservable	End users have no reliable information on a firm's handling of private customer information, and therefore reduce their transactions	• Mandatory disclosure of security breaches • Minimum security standards • Mandatory certification
Firms cannot compete on security	Firms may not invest in data protection because clients cannot reliably assess the quality of certification agencies; high-security firms are driven out of the market	• Mandatory disclosure of security breaches • Minimum security standards • Mandatory certification
Externalities		
Insecure computers reduce security of the network	Firms and households under invest in the security of their own computers as they externalities for other Internet users	• Awareness campaigns • Minimum security standards
Anonymous communication	Use of software that enables anonymous communication (e.g. TOR) undermines attribution of security incidents and hampers law enforcement	• Regulation of software that enables anonymous communication
Social networks	Excessive revealing of private information in social networks attracts systematic criminal activities (phishing, spam, identity theft)	• Awareness campaigns • Facilitating reliable identification

5. Concluding remarks

The Internet has become a part of daily life for many people. And if the past decade is of any guidance, the role of the Internet in the economy is going to increase substantially. As a consequence of this rapid development, the security of communication over the Internet will become even more important than it already is today.

The security of the Internet depends on the behaviour of both infrastructure providers and end users. We show that there are several reasons why these parties have insufficient incentives to invest in cyber security. Under which conditions will markets provide solutions for cyber security issues, and what can governments do when market fail to do so?

We have identified three reasons why markets might fail to deliver an optimal level of security on the Internet.

1. Information asymmetry
2. Externalities
3. Market power

Information asymmetry might occur in various situations. For example, end users are not able to verify whether an Internet Service Provider (ISP) correctly informs its customers about its security performance. This uncertainty makes end users reluctant to pay for security. For ISPs this means that their investments in cyber security do not give them an advantage over competitors; additional security will only increase costs. Similar problems apply to Certificate Authorities. Internet users that want to have certainty about the identity of the people or organizations they connect with, depend on commercial Certificate Authorities (CA). The service quality of CA information, however, cannot be assessed by individual end users.

Externalities might also be a reason for insufficient investments in security. Often, only part of the benefits of investments in security accrue to the investor. For example, improvements in the security of one ISP's services will also benefit customers of other ISPs. When externalities are strong, governments may promote cyber security by subsidizing the use of secure technology or by setting minimum cyber security standards. Temporary policy measures will suffice for the promotion of the adoption of safer communication protocols.

Market power, a third type of market failure, can also lead to suboptimal Internet security. Large international network providers with low security performance feel little pressure from ISPs and other peering partners to improve their security levels as they are "too-big-to-block". Governments might impose minimum security standards in order to improve security. International coordination would be required for these standards to be enforceable.

An economic perspective on Internet security is useful not only for identifying weak spots, but also for finding solutions to security problems. In time, economics may prove to be indispensable for making the Internet a safer place.

Annexes

Annex 1 Internet basics

The logical structure of the Internet allows all connected users to broadcast a message to any other site on the network, no matter in which country. The Internet browser of the sending party first splits a message in small packets with an address label attached. The individual packets travel by the speed of light and may take any route that is free at that moment, until eventually they arrive at the destination computer where all packets are reassembled by the Internet browser of the receiving partner.

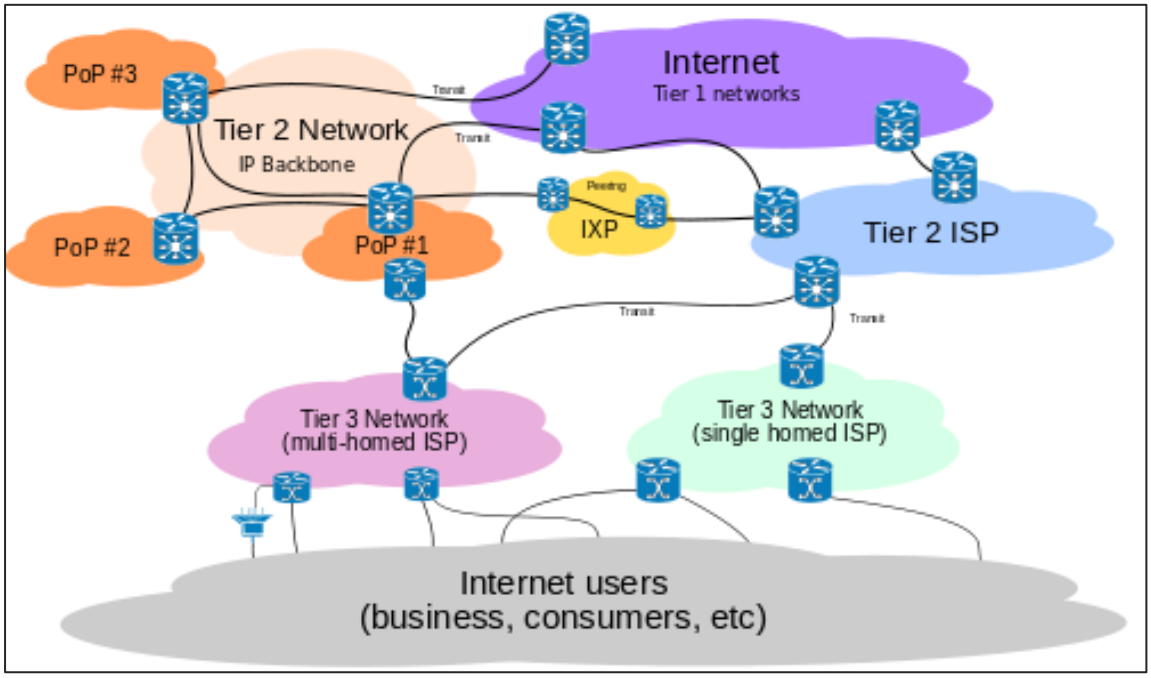
The Internet is a network of networks. Networks can be ranked by their connectivity status:

- Tier 1 networks: owned network links to all major networks in the world, so they do not need to send their data packets over connections owned by other networks. They can reach every other network on the Internet without purchasing IP transit or paying settlements to other networks.[4] The world has about a dozen Tier 1 networks (most of US origin).
- Tier 2 networks are large networks with direct connections to Tier 1 networks and with Internet data exchange points (IXP) where trunk connection lines come together. Tier 2 networks generally cater many local Tier 3 networks (ISPs, hosting providers).
- Tier 3 networks are ISPs and other local networks that have service-level contracts with end-users in a particular country or region, and with owners of 'last mile' physical networks such as a telecom or cable companies.[5] Many telecommunication firms have also developed ISP activities to draw additional business from the physical (copper, fibre) networks they own. In the latter case, the ISP-owning firms also own the 'last-mile' network.

[4] It is difficult to determine whether a network is paying settlements if the business agreements are not public information, or covered under a non-disclosure agreement. The Internet "peering community" is roughly the set of peering coordinators present at Internet exchanges on more than one continent.

[5] In 2011 the Internet consisted of 5039 independent Internet service provider (ISP) networks (Weller and Woodcock, 2013). Examples in the Netherlands are firms like XS4ALL and Online.

Figure A1 Internet as a network of networks

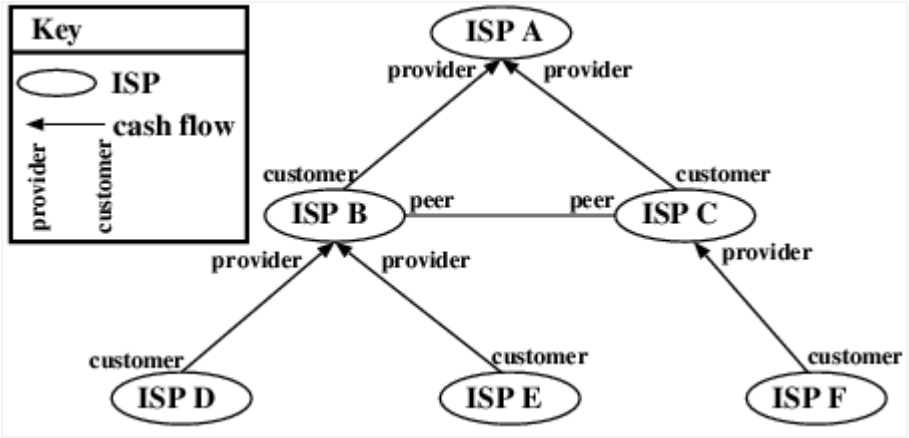


Source: Wikipedia (lemma "Internet", http://en.wikipedia.org/wiki/Internet).

The Tier 1 networks plus the IDX connection points are also called the Internet backbone. A Tier 3 network that depends on only one Tier 2 network is called a single-homed network and the Tier 3 network is called multi-homed network if it is connected to more than one Tier 2 network. Multi-homed networks are more stable and less sensitive to congestion and disruptions.

The interconnecting links between networks take two contractual forms: transit agreements or peering agreements. Transit agreements are commercial contracts in which a customer (which may itself be an ISP) pays a service provider for access to other parts of the Internet; these agreements are most common at the edges of the Internet. Peering agreements are the carrier interconnection agreements that are within Internet exchange points (IXPs). Via the peering agreements carriers exchange traffic for one another's customers; they are most common in the core of the Internet and are the source of the Internet bandwidth commodity. Most of the peering agreements are closed-purse contracts, based on the mutual benefits of open exchange between each pair of partners. The figure below shows that between ISPs a hierarchy may exist. In the figure below ISP A is a Tier 1 or Tier 2 network that caters fee-paying services to several lower-level networks. The ISPs B and C have a traffic-sharing (or 'peering') agreement that is settlement free ('closed purses').

Figure A2 Peering and non-peering contracts between local networks



Source: CAIDA, AS measurement system (http://as-rank.caida.org/?mode0=as-intro#relationships).

The Internet is a complex system with innumerable connections between pieces of hardware and software situated all over the globe. Researchers have begun mapping the interconnections of the Internet by using distributed programs (on approximately 5000 computers worldwide) that search out a path to another point on the Internet every few minutes. Using this data, Carmi *et al*. (2007) produced the conceptual map (below) to explore the functional organisation of the Internet (i.e. the importance of certain nodes), not simply the number of connections. This shows three distinct sets of nodes in the Internet. The first is a dense core of 100 or so critical nodes that have a large number of connections to other nodes and form the "nucleus" of the Internet. The second set lies outside of the nucleus and is composed of approximately 5000 isolated nodes that are extremely dependent on the critical nodes in the nucleus as they have few if any other connections. In between these two sets of nodes is the final category composed of around 15000 peer-connected nodes that are self-sufficient.[6]

[6] If the critical core nodes are removed, only about 30% of the isolated nodes become entirely isolated from the system. "*The remaining 70% can continue communicating because the middle region has enough peer-connected nodes to bypass the core*", the number of links required to complete the data transfer simply increases from about 4 or 5 to 8 or 10 (Graham-Rowe, 2007). On measuring the structure of the Internet, see also the DIMES project (Shavitt and Shir, 2005).

Annex 2 Types of cyber security incidents

Table A1 Types of CYBER security incidents

Type	Brief description
Exploit kits	Production and trade in ready-to-use software packages that "automate" cyber crime. An important characteristic of exploit kits is their ease of use (usually through a web interface) allowing people without technical knowledge to purchase and easily use them.
Phishing	The combined use of fraudulent e-mails and legitimate looking websites by cyber criminals 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 paper authors into a fraudulent referee procedure for scientific journals.
Rogueware	Threat consists of any kind of fake software that cyber criminals distribute (e.g. via social engineering techniques) in order to lure users to their malicious intentions. 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. Adversaries using this threat force the e-mail messages to be received by mail recipients. Removing spam is time consuming for recipients and costly in terms of resources (network and storage) for the service providers.
Cyber espionage	Industrial and state-driven intrusion in online accessible data system for stealing private-owned information assets.
Identity theft	An attack that occurs when an adversary steals user credentials and uses them order to serve malicious goals, mostly related with 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	Attacks that exploit the trust between Internet users and search engines. Attackers deliver bait content for searches to various topics. In this way, users searching for such items are being diverted to malicious content.
Information leakage	Refers to the revealing of information by hackers or others, making it available to an unauthorized party. This information can be further processed and abused, e.g. to start an attack or gain access to additional information sources.
Rogue certificates	Identity certificates are a means of defining trust in Internet. Attackers steal, produce and circulate rogue certificates which break the aforementioned chain of trust, giving them the capability of engaging in attacks that are undetectable for end users. By using rogue certificates, attackers can successfully run large scale man-in-the-middle attacks. Moreover, rogue certificates can be used to sign malware that will appear as legitimate and can evade detection mechanisms.
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.
Botnets	Creating a network of "zombie" computers infected by a piece of malicious software (or "malware") designed to enslave them to a master computer, the so-called botnet herder. These compromised systems are called bots (or 'zombies') and they communicate with the botnet herder that can maliciously direct them. Botnets are multiple usage tools that can be used for spamming, identity theft as well as for infecting other systems and distribute malware.
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.

Source: survey constructed from ENISA (2013); Rogers and Ruppersberger (2012).

References

Akerlof, G., 1970, The Market for "Lemons": Quality Uncertainty and the Market Mechanism, *The Quarterly Journal of Economics*, vol. 84(3), pp. 488-500.

Alchian, A. and H. Demsetz, 1972, Production, information cost, and economic organization, *American Economic Review*, vol. 62(5), pp. 777-795.

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.

Anderson, R. and T. Moore, 2006, The economics of information security, *Science*, vol. 27(314), pp. 610-613.

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

Arnbak, A. and N. van Eijk, 2012, Certificate Authority Collapse: Regulating Systemic Vulnerabilities in the HTTPS Value Chain, paper presented at Telecommunications Policy Research Conference, August 2012, Institute for Information Law, University of Amsterdam.

Arora, A., T. Rahul and T.H. Xu, 2004, Optimal Policy for Software Vulnerability Disclosure, paper Carnegie Mellon University, Pittsburgh.

Asghari, H., 2010, *Botnet mitigation and the role of ISPs: A quantitative study into the role and incentives of Internet Service Providers in combating botnet propagation and activity*, Delft University of Technology, Delft.

Axelrod, R., 2010, Beyond the Tragedy of the Commons, *Perspectives on Politics*, vol. 8(2), pp. 580-582.

Baran, P., 1962, *On distributed communication networks*, Document P-2626, Rand Corporation (http://www.rand.org/pubs/papers/P2626.html).

Bauer, J. and M. Van Eeten, 2009, Cyber security: stakeholder incentives, externalities and policy options, *Telecommunications Policy*, vol. 33(1), pp. 706-719.

Bertschek, I., D. Cerquera and G. Klein, 2011, More Bits - More Bucks? Measuring the Impact of Broadband Internet on Firm Performance, SSRN eLibrary No 1852365, ZEW, Mannheim.

Bernat, L., 2010, Economics of malware: addressing the security externalities of end users, Interim report - Internet Service Providers, DSTI, Committee for Information, Computer and Communication Policy, DSTI/ICCP/REG(2010)1, OECD, Paris.

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

Bodeau, D., R. Graubart, L. LaPadula, P. Kertzner, A. Rosenthal and J. Brennan, 2012, Cyber resilience metrics: version 1.0, Rev.1, MITRE, Bedford MA.

Boebert, W., 2010, A survey of challenges in attribution, in: Comittee on Deterring Cyber attacks (ed.), Proceedings of a Workshop on Deterring Cyber attacks: Informing Strategies and Developing Options for U.S. Policy, National Academies Press, Washington DC, 41-52.

Bortz, A., A. Barth and A. Czeskis, 2011, Origin cookies: session integrity for Web applications, paper Web 2.0 Security & Privacy conference 2011, held in conjunction with the 2011 IEEE Symposium on Security and Privacy (http://w2spconf.com/2011/papers/session-integrity.pdf).

Boyd, D. and N. Ellison, 2007, Social Network Sites: Definition, History, and Scholarship, *Journal of Computer-Mediated Communication*, vol. 13(1) (http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html).

Brynjolfsson, E., L. Hitt and H. Kim, 2011, Strength in numbers: how does data-driven decisionmaking affect firm performance?, Working paper, MIT and University of Pennsylvania (http://ssrn.com/abstract=1819486).

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).

Carmi S. et al., 2007, A model of Internet topology using k-shell decomposition, *Proceedings of the National Academies of Sciences of the United States of America*, vol. 104 (27), pp. 1 1150-1 1154. (http://www.pnas.org/content/104/27/11150.full)

Carpenter, B. (ed.), 2000, Charter of the Internet Architecture Board, Request for Comments No. 2850, IAB website (http://tools.ietf.org/html/rfc2850#page-6), retrieved May 2013.

Cavallini, S., S. di Trocchio. F. Bisogni, M. Tancioni and P. Trucco, 2010, Development of a methodology and research of quantitative data on the economics of security and resilience in critical communications and information infrastructures, Final Report, SMART 2009/0006, Formit, Rome.

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.

Claffy, K., 2011, Underneath the hood: ownership vs. stewardship of the Internet, *ACM SIGCOMM Computer Communication Review*, vol. 41(5), pp. 46-47.

Claffy, K. and D. Clark, 2013, Workshop on Internet Economics (WIE2012) Report, Tech. rep., Cooperative Association for Internet Data Analysis (CAIDA), University of California, Supercomputer Centre. (http://www.caida.org/publications/papers/2013/wie2012_report/)

Clark, D. and S. Landau (eds), 2010, Untangling attribution, in: *Comittee on Deterring Cyber attacks*, Proceedings of a Workshop on Deterring Cyber attacks: Informing Strategies and Developing Options for U.S. Policy, National Academies Press, Washington DC, pp. 25-40.

Coase, R., 1960, The problem of social costs, *Journal of Law and Economics*, vol. 3(October), pp. 1-44.

Cohen, G.(ed.), 2010, Targeting Third-Party Collaboration, in: Committee on Deterring Cyber attacks, *Proceedings of a Workshop on Deterring Cyber attacks: Informing Strategies and Developing Options for U.S. Policy*, National Academies Press, Washington DC, pp. 313-326.

Cohen, R., K. Erez, D. ben-Avraham and S. Havlin, 2001, Breakdown of the Internet under intentional attack, *Phys. Rev. Lett*, vol. 86(16), pp. 3682-3685. (http://havlin.biu.ac.il/PS/cebh410.pdf).

Committee on Deterring Cyber attacks, 2010, *Proceedings of a Workshop on Deterring Cyber attacks: Informing Strategies and Developing Options for U.S. Policy*, National Academies Press, Washington DC.

Cornes, R. and T. Sandler, 1986, *The theory of externalities, public goods, and club goods*, Cambridge University Press, Cambridge.

Crespi, F., 2007, IT services and productivity in European Industries, in: L. Rubalcaba and H. Kox (eds), *Business services in European economic growth*, Palgrave -MacMillan, Basingstoke, pp. 116-127.

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.

Dietz, A., A. Czeskis, D. Balfanz and D. Wallach, 2012, Origin-bound certificates: a fresh approach to strong client authentication for the Web, paper by IETF TLSWorking Group and Google, presented at 21st USENIX Security Symposium, Aug. 2012. (https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final162.pdf).

Dietz, Th., E. Ostrom and P. Stern, 2003, The struggle to govern the commons, *Science*, vol. 302(12 December 2003), pp. 1907-1912.

Donaldson, D. and R. Hornbeck, 2012, Railroads and American Economic Growth: A "Market Access" Approach, MIT/Harvard, draft paper (https://economics.uchicago.edu/workshops/Hornbeck%20Richard%20-%20Railroads.pdf).

Doyle, J, and J. Caroll, 2002, National Adress Translation, online paper CISCO Press, Indianapolis (http://www.ciscopress.com/articles/article.asp?p=25273).

EC, 2013a, Cyber security strategy of the European Union: an open, safe and secure cyberspace, Joint Communication to the European Parliament and the Council, JOIN(2013)1Final, European Commision, Brussels.

EC, 2013b, Proposal for a Directive concerning measures to ensure a high common level of network and information security, COM(2013)48final, Brussels.

EC, 2013c, Impact assessment, Commission staff working paper accompanying the Proposal for a Directive concerning measures to ensure a high common level of network and information security, SWD(2013)32final, Brussels.

EC, 2012a, Overview of progress on the 101 Digital Agenda actions and Digital Agenda Review package, Commission Staff Working Document, European Commission, DG CONNECT, Brussels. Retrieved January 29, 2013: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1382.

EC, 2012b, Digital Agenda for Europe - a good start and stakeholder feedback, Commission Staff Working Document SWD(2012) 446 final, European Commission, DG CONNECT, Brussels.

EC, 2012c, Cyber security, Special Eurobarometer #390, TNS Opinion and Social, at the request of Europan 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.

ENISA, 2012, Economics of security: facing the challenges - a multidisciplinary assessment, European Network and Information Security Agency, Heraklion.

ENISA, 2012a, Cyber incident reporting in the EU: an overview of security articles in EU legislation, European Network and Information Security Agency, Heraklion.

ENISA, 2012b, Incentives and barriers of the cyberinsurance market in Europe, European Network and Information Security Agency, Heraklion.

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

FCC, 2011, Cyber security Tip Sheet for small businesses, Cyber security Roundtable- Securing And Empowering Small Businesses With Technology, May 16, 2011 (www.fcc.gov/cyberforsmallbiz).

Fornefeld,.M., G. Delaunay and D. Elixmann, 2008, The impact of broadband on growth and productivity, study commissioned by the European Commission, Micus, Düsseldorf.

Frank, R., 2008, Should public policy respond to positional externalities?, *Journal of Public Economics*, vol. 92(8-9), pp. 1777-1786.
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.
Gelman, R., 2010, Civil liberties and privacy implications of policies to prevent cyber attacks, in: Comittee on Deterring Cyber attacks (ed.), *Proceedings of a Workshop on Deterring Cyber attacks: Informing Strategies and Developing Options for U.S. Policy*, National Academies Press, Washington DC, 273-309.
GOVCERT.NL, 2011, Cyber securitybeeld Nederland 2011, Ministerie van Veiligheid en Justitie, The Hague.
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.
ICANN, 2011, Draft rationale for approving registry agreement with ICM's for XXX sTLD, 18 March 2011 (http://www.icann.org/en/minutes/draft-icm-rationale-18mar11-en.pdf).
Hardin, G., 1968, The Tragedy of the Commons, *Science*, vol. 162 (3859), pp. 1243-1248.
Haucap, J. and U. Heimeshoff, 2013, Google, Facebook, Amazon, eBay: is the Internet driving competition or market monopolization? Düsseldorff Institute for Competition Economics (DICE), Discussion Paper No. 83 (http//hdl.handle.net/10419/68229).
Helbling, Th., 2010, What Are Externalities? What happens when prices do not fully capture costs?, IMF, *Finance and Development*, December, pp. 48-49.
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 ()
Hofmokl, J., 2010, The Internet commons: towards an eclectic theoretical framework, *International Journal of the Commons*, vol. 4(1), pp. 226-250. (http://www.thecommonsjournal.org/index.php/ijc/article/view/111/106).
Holt, L. and M. Jamison, 2009, Broadband and contributions to economic growth: lessons from the US experience, *Telecommunications Policy*, vol. 33 10-11), pp. 575-581.
Horrigan, W., 2013, Big Data: A Perspective from the Bureau of Labor Statistics, *AMSTATNEWS-The membership magazine of the American Statistical Association,* January 1, 2013 (http://magazine.amstat.org/blog/2013/01/01/sci-policy-jan2013/).
Huberman, B. and R. Lukose, 1997, Social Dilemmas and Internet Congestion, *Science*, vol. 277 (5325), pp. 535-537.
ITU/WCIT, 2012, Final Acts Of The World Conference On International (Dubai, 2012), Dubai.
Jentzsch, N., S. Preibusch and A. Harasser, 2012, Study on monetising privacy: An economic model for pricing personal information, European Network and Information Security Agency (ENISA), Heraklion.
Kannan, K. and R. Telang, 2005, Market for Software Vulnerabilities? Think Again, *Management Science*, vol. 51(5), pp. 726-740.
Katz, M. and C. Shapiro, 1985, Network Externalities, Competition and Compatibility, *American Economic Review*, vol. 75(3), pp. 424-440.
Kent S. and K. Seo, 2005, Security Architecture for the Internet Protocol, Internet Engineering Task Force Request For Comment 430, (http://tools.ietf.org/html/rfc4301).

Koopmans, Tj., 1957, Three essays on the state of economic science, McGraw-Hill, New York.
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).
Krishnamuthy, B., K. Naryshkin and C. Wills, 2011, Privacy leakage vs. Protection measures: the growing disconnect, paper Web 2.0 Security & Privacy conference 2011, held in conjunction with the 2011 IEEE Symposium on Security and Privacy (http://w2spconf.com/2011/papers/privacyVsProtection.pdf).
Lehr, W., 2012, Mobile Broadband and Metrics Challenges, presentation at 3rd Workshop on Internet Economics (WIE 2012, 12-13th December, UCL, San Diego), MIT, Cambridge MA.
Lelarge, M. and J. Bolot, 2009, Economic incentives to increase security in the Internet: the case for insurance, paper at IEEE INFOCOM 2009 Conference, Conference Proceedings, pp. 1494-1502.
Levin, D., 2011, The economics of Internet markets, NBER WP #16852, Cambridge MA.
Liebenau, J., S. Elaluf-Calderwood, P. Karrberg, 2012, Strategic Challenges for the European Telecom Sector: The Consequences of Imbalances in Internet Traffic, *Journal of Information Policy*, vol. 2, pp. 248-272.
Liebenau, J., S. Elaluf-Calderwood, 2012, Understanding the measuring and characteristics of quantitative data on Internet traffic, presentation at CAIDAWorkshop (12-13th December, UCL, San Diego), LSE, London.
Liebowitz, S. and S. Margolis, 1994, Network externality: an uncommon tragedy, *Journal of Economic Perspectives*, vol. 8(2), pp. 133-150.
Lindahl, E., 1958, Just taxation - a positive solution, in: A. Peacock and R. Musgrave (eds), *Classics in the theory of public finance*, MacMillan, London.
Loeper, J., 2011, Coordination in heterogeneous federal systems, *Journal of Public Economics*, vol. 95(7), pp. 900–912.g23
Microsoft, 2012, Microsoft Security Intelligence Report: worldwide threar assessment, volume 13: January through June 2012, Microsoft Corporation.
Moore, T, and R. Anderson, 2011, Economics and Internet security: a survey of recent analytical, empirical and behavioural research, WP TR-03-11, Computer Sience Group, Harvard University, Cambridge MA.
Moore, T., R. Clayton and R. Anderson, 2009, The economics of online crime, *Journal of Economic Perspectives*, vol. 23(3), pp. 3-20.
Morgan, P., 2010, Applicability of traditional deterrence concepts and theory to the cyber realm, in: Comittee on Deterring Cyber attacks (ed.), *Proceedings of a Workshop on Deterring Cyber attacks: Informing Strategies and Developing Options for U.S. Policy*, National Academies Press, Washington DC, 55-76.
Motiwala, M. A. Dhamdere, N. Feamster and A. Lakhina, 2012, Towards a cost model for network traffic, Cooperative Association for Internet Data Analysis, University of California, Supercomputer Centre (http://gtnoise.net/papers/2012/motiwala:ccr2012.pdf).
Mushaq, A., 2010, Man in the Browser: Inside the Zeus Trojan (http://threatpost.com/en_us/blogs/manbrowser-inside-zeus-trojan-021910).
Myles, G.D., 1995, *Public economics*, Cambridge University Press, Cambridge.
NCSC, 2012, Cyber securitybeeld Nederland2012, Nationaal Cyber Security Centrum, Den Haag.
Nordhaus, W., 2002, Productivity growth and the new economy, Brookings Papers on Economic Activity, 2, pp. 211-265.

Odlyzko, A., 2012, On the classification and the value of communications, presentation at 3rd Interdisciplinary Workshop on Internet Economics (University of California San Diego, La Jolle), School of Mathematics / Digital Technology Center, University of Minnesota.
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, 2011a, Future Global Shocks - improving risk governance, OECD Reviews of Risk Management Policies, 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
Ostrom, E., 1990, *Governing the Commons: The Evolution of Institutions for Collective Action*, Cambridge University Press.
Papandreou, A., 1998, *Externality and institutions*, Clarendon Press / Oxford University Press, Oxford.
Péllissié du Rausas, M., J. Manyika, E. Hazan, et al., 2011, Internet matters: the Net's sweeping impact on growth, jobs and prosperity, McKinsy Global Institute, May 2011 (www.mckinsey.com/mgi/).
Platteau, J.Ph. (ed.), 2000, *Institutions, Social Norms and Economic Development*, Harwood Academic Publishers, Amsterdam.
Plattner, B. and S. Frei, 2010, Internet-Kriminalität - ein gut organisierter Wirtschaftszweig, IO New Management 10, ETH, Zürich.
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*, vol. 26(3), pp. 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.
Quarterman, J. and A. Whinston, 2010, Economic Incentives for Internet Security through Reputation and Insurance, paper APWG and IEEE-SA Roadmapping Session.
Saltzer, J., D. Reed and D. Clark, 1981, End-to-End Arguments in System Design, in: IEEE Computer Society, Proceedings of the Second International Conference on Distributed Computing Systems (Paris, April 8-10, 1981), pp. 509-512.
Schmidt, A., 2012, At the boundaries of peer production: the organization of Internet security production in the cases of Estonia 2007 and Conficker, *Telecommunications Policy*, vol. 36(6), pp. 451-461.
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).

Shavitt, Y. and E. Shir, 2005, DIMES: Let the Internet Measure Itself, *ACM SIGCOMM Computer Communication Review*, vol. 35 (5), pp. 71-74 (http://www.eng.tau.ac.il/~shavitt/pub/CCR05.pdf).

Smits, M., S. Sonneveld, S. Arlman and V. Makhija, 2011, Interned: hoe het Internet de Nederlandse economie verandert, study commissioned by Google, Boston Consulting Group, Amsterdam.

Spar, L., 1999, The public face of cyberspace, in: I. Kaul, I. Grunberg and M. Stern (eds), *Global public goods - international cooperation in the 21st century*, Oxford University Press, New York/Oxford, pp. 344-363.

Stiglitz, J., 1999, Knowledge as a public good, in: I. Kaul, I. Grunberg and M. Stern (eds), *Global public goods - international cooperation in the 21st century*, Oxford University Press, New York/Oxford, pp. 308-325.

Stryszowski, P., 2012, The Impact of Internet in OECD Countries, OECD Digital Economy Papers, No. 200, OECD Publishing, Paris.

Symantec, 2007, Symantec Internet Security Threat Report - Trends for July–December 06, Vol. XI, Symantec. (http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_Internet_security_threat_report_xi_03_2007.en-us.pdf)

Symantec, 2012, Internet Security Threat Report: 2011 Trends- main report, Vol. 17, Symantec Inc., Mountain View, Calif. (http://www.symantec.com/content/en/us/enterprise/other_resources/bistr_main_report_2011_21239364.en-us.pdf)

The Economist, 2013, *The new politics of the Internet: everything is connected*, *The Economist*, January 5th 2013.

Tinbergen, J. 1955 (1952), *On the Theory of Economic Policy*, North-Holland, 2nd ed., Amsterdam.

US Department of Commerce, 2011, Cybersecurity, innovation and the Internet economy, The Department Of Commerce Internet Policy Task Force, Washington DC.

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

Van Leeuwen, G. and H. van der Wiel, 2003, Do ICT spillovers matter? Empirical evidence for the Netherlands, CPB Discussion Paper #26, CPB Netherlandse Bureau for Economic Policy Analysis, The Hague.

Veblen, T., 1899, Theory of the Leisure Class: An Economic Study in the Evolution of Institutions, Macmillan 1994 edition, New York.

Verizon, 2008, 2008 Data Breach Investigations: A comparison of risk factors among the finance, food, retail, and tech industries - supplementary report, Verizon Business Risk Team, http://www.verizonenterprise.com/resources/whitepapers/wp_supplemental-report-specifics-for-the-financial-services-food-beverage-retail-and-tech-services-industries_en_xg.pdf).

Verizon, 2010, 2010 Data Breach Investigations Report: study conducted by the Verizon RISK Team in cooperation with the United States Secret Service, (http://www.verizonenterprise.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf).

Verizon, 2011, 2011 Data Breach Investigations Report (DBIR): study conducted by the Verizon RISK Team with cooperation from the U.S. Secret Service and the Dutch High Tech Crime Unit, (http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf).

Verizon, 2012, 2012 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, (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.

Wu, T., 2012, Der Master Switch: Aufstieg und Niedergang der Medienimperien, MITP, Heidelberg (original version 2010, The Master Switch: the rise and fall of Information Empires).

Wu, T., 2006, Network neutrality: competition, innovation and non-discriminatory access, Testimony at Hearing by House Committee on the Judiciary Telecom & Antitrust Task Force, US House of Representatives, Washington DC.

Wu, T., 2005, Network neutrality, broadband discrimination, *Journal on Telecommunications and High Technology Law*, 2, 141-179.

Yoo, C.S., 2006, Network neutrality and the economics of congestion, *The Georgetown Law Journal*, vol. 94, pp. 1846-1908.

Zittrain, J., 2008, *The future of the Internet and how to stop it*, Yale University Press, New Haven - London.

Endnotes

[1] TechTarget estimates that in September 2012 over 1.01 billion people participated in some sort of social network.
[2] E.g. Kosinski, *et al.* (2013).
[3] Among the few studies that apply a 'market failure' approach to a specific aspects of cyber security are: Bauer and Van Eeten (2009), OECD (2008), Rao and Reilly (2012) and Moore, Clayton and Anderson (2009).
[4] 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 cyber crimes, and the level of concern they feel about this type of crime (EC, 2012c).
[5] Europe in this case includes Russia and other non-EU countries.
[6] The first five indicators reported by Symantec, a leading producer of anti-virus software and firewalls in semi-annual reports (e.g. Symantec, 2007); the last two items are reported by the Anti-phishing Working Group of the Internet Policy Committee (e.g. APWG, 2008-2012).
[7] 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.
[8] For brevity, this section mostly uses 'goods' as an abbreviation for both goods and services.
[9] Marginal costs may be zero up to some number of users, as is true for swimming pools.
[10] In a market economy externalities that run through prices are widespread as any transaction eventually will have some indirect influence prices set with other transactions (however small it may be). These common externalities are called 'pecuniary' externalities (Cornes and Sandler, 1986 and Miles 1995).
[11] The value received by consumers can be split in two parts. One component is the value that the product itself would have even if there are no other users. The second component (synchronization value) is the value derived from the fact that the product allows to interact with other users of the product. Cf. Liebovitz and Margolis (1994); Katz and Shapiro (1985).
[12] Cf. Verizon (2011); Van Eeten and Bauer (2008); Anderson *et al.* (2008); Moore *et al*. (2009).
[13] Dutch penal law allows for criminal punishment of 'intentional and unlawful entry in someone else's computer and digital database system' with a maximum prison sentence of one year and a maximum of four years if the obtained data are used for own profits or if they are sold to third parties (article 138ab, Wetboek van Strafrecht).
[14] A reputation system stimulates co-operative outcomes in a market context (Axelrod, 2010). Firms that do not work together might otherwise face some form of retaliation in the future. Once retaliation starts, the outcomes are unpredictable, because non-cooperative or retaliatory solutions are inherently unstable (cf. Morgan, 2010).
[15] The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) published a technical code "Information technology - Security techniques - Code of practice for information security management". Several countries have their own, often voluntary data privacy codes.

Chapter IV

[16] Twenty years later this principle is called the 'end-to-end' principle (e.g. Saltzer, Reed and Clark, 1981).
[17] For example, in the Netherlands SIDN is the national registry.that manages over 5 million ".nl" domain names. There is more than one ".nl" domain name for every five people in the Netherlands – a higher ratio than for any other country-code domain in the world. More than 1600 independent commercial registrars operate under SIDN as web hosting agents.
[18] E.g. TV transmission, telephony, spam filters, website hosting, and leasing of routers.
[19] An OECD study found that customer support costs may amount to 1-2 per cent of total revenues of a medium-sized ISP (Van Eeten and Bauer, 2008). Costs go up even more if it would be necessary to make expensive outgoing calls to customers whose computer has become part of botnets.
[20] Examples of mandatory reporting paramets could be the % of spam messages in total outgoing email, the % of botnet-infected PC's per ISP, the update frequence of the offered anti-virus software, frequency of incoming phishing email, the number of employees working in consumer helpdesks, and the incidence of major data breaches per ISP. One could start with security parameters that require the least monitoring of traffic, and extend this list after a public debate on ISP traffic monitoring (see further Section IV.3). Because these data are not published or even kept secret, customers cannot judge the security quality of the ISP.
[21] The US Dept of Commerce (2011) notes that the complexity of IPSEC (due to its great number of features and options) could be a source of future weaknesses or holes discovered later on. The benefits of implementing and using IPSEC (cf. Kent and Seo, 2005) are: (a) it provides security directly on the IP network layer and secures everything put on top of the IP network layer; (b) relatively mature protocol that has proven to be a secure and trusted method of securing data; (c) transparent to applications in the sense that IPSEC is not limited to specific applications; and (d) transparent to end users and therefore no need to train users on security mechanisms.
[22] SpamCop has for a long time been an independent international blacklist for spam, although it has now been taken over by Cisco. SpamCop now functions in the context of Cisco's IronPort SenderBase Security Network. According to Cisco: "*SenderBase scores are assigned to IP addresses based on a combination of factors, including email volume and reputation. Reputation scores in SenderBase may range from -10 to +10, reflecting the likelihood that a sending IP address is trying to send spam. Highly negative scores indicate senders who are very likely to be sending spam; highly positive scores indicate senders who are unlikely to be sending spam. SenderBase is a designed to help email administrators better manage incoming email streams by providing objective data about the identity of senders. SenderBase is akin to a credit reporting service for email, providing data that ISP's and companies can use to differentiate legitimate senders from spam sources. SenderBase provides objective data that allows email administrators to reliably identify and block IP addresses originating unsolicited commercial email (UCE) or to verify the authenticity of legitimate incoming email from business partners, customers or any other important source*" (https://ironport.custhelp.com/app/answers/detail/a_id/120). Another famous anti-spam organisation is Spamhaus with an effective policy of blacklisting IP-addresses that according to them are spam distributors. The practices of Spamhaus lack a solid legal backing and the proportionality of their action is under debate.
[23] Cf. Annex 1 for an explanation.
[24] The Internet exchange points (abbreviated: IXPs) is a physical infrastructure through which Internet service providers (ISPs) exchange Internet traffic between their networks via direct, physical connection cables. Many IXPs have not yet secured an IPv6 subnet from their Regional Internet Registry to facilitate IPv6 peering by their participant Internet Service Providers (Weller and Woodcock, 2013).

[25] The Internet Society is the parent company of the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). The IAB oversees the technical and engineering development of the Internet. It has a number of Task Forces, of which the most important are the IETF and the Internet Research Task Force (IRTF). The IAB acts as representative of the interests of the IETF in liaison relationships with other organizations concerned with standards and other technical and organizational issues relevant to the worldwide Internet. The IAB provides oversight of the process used to create Internet standards. The IAB also serves as an appeal board for complaints of improper execution of the standards process, through acting as an appeal body in respect of an Internet Engineering Steering Group (IESG) standards decision. The IAB consists of thirteen full members, including the chair of the IETF and twelve sitting members that take part as individual, and not as representatives of any company, agency, or other organization. Ex-officio and liaison members of the IAB may also attend IAB meetings but shall not participate in determination of official actions. The IAB publishes minutes of all its meetings on the Internet, and conducts an open meeting at every IETF meeting.

[26] Cf. Figure 2 in Section 1.2.

[27] Since 2003, the overall connection capacity has mainly grown in other areas than Europe and North America, like Asia and Latin America (Weller and Woodcock, 2013).

[28] The most notable characteristic in a scale-free network is the relative commonness of 'nodes' with a connectivity degree that greatly exceeds the average. The highest-degree nodes are often called "hubs. The scale-free property strongly correlates with the network's robustness to failure. It turns out that the major hubs are closely followed by smaller ones. These ones, in turn, are followed by other nodes with an even smaller degree and so on (cf. Wikipedia, lemma 'Scale-free networks').

[29] See explanation in Table 4.

[30] More details are described by Prince (2013). Early May 2013, the Spanish government (and at the request of the Dutch government) arrested one of the managers of Cyberbunker who reportedly coordinated the massive DdoS on Spamhaus from a van with mobile servers that operated from different places in North Spain.

[31] Some firms also actively compromise the security of others by illegally reselling data, espionage, sabotage, phishing, or other forms of crime.

[32] Cf. Verizon (2011); Van Eeten and Bauer (2008).

[33] Cf. Symantec (2012); Microsoft (2012); Verizon (2012); APWG (2012).

[34] These problems are well documented in the economic literature (e.g. Veblen, 1899; Frank, 2011).

[35] According to TechTarget over 1.01 billion people participated in some form of social media use in September 2012. For clever data analysis firms the social media data form an open vault of information. To this we may add an endless stream of blog posts and Twitter accounts. Cf. Kosinkski *et al.* (2013).

[36] This discussion applies to other stakeholders of the firm as well.

[37] In a similar situation, the customer has knowledge about the investment behavior of the firm, but cannot enforce its contract as the firm's behavior cannot be observed by third parties.

[38] Firms with small financial reserves are unlikely to invest in protection against rare incidents.

[39] A possible way to achieve this is by allowing accounting rules for firms that allow the firm's data-holding reputation to serve as part of a firm's intangible but quantifiable goodwill assets, provided that some auditability requirements are met.

[40] It might lead to a chicken-or-egg problem: a market is needed to build a track-record, but the market cannot function without reputation.

[41] When the actions individual employees (including directors) cannot be fully observed by the owners of the firm, they do not have sufficient incentives to maintain the firm's reputation. Moral hazard and internal monitoring failure between owners and employees then leads to insecure behaviour. However one may argue that it is in the firm's own interest to abate such incentive misalignment within firms.

[42] The Dutch government chose Diginotar, a small local company, to issue security certificates for the Dutch government because it proposed the lowest price for the demanded services. Weak security of Diginotar's network made it an easy target for hackers, compromising the security of electronic communication with and within the Dutch government.