Security Economics and European Policy

Ross Anderson[1], Rainer Böhme[2], Richard Clayton[1] and Tyler Moore[1]

[1]Computer Laboratory, University of Cambridge, UK, [2]Technische Universität Dresden, DE

Abstract In September 2007, we were awarded a contract by the European Network and Information Security Agency (ENISA) to investigate failures in the market for secure electronic communications within the European Union, and come up with policy recommendations. In the process, we spoke to a large number of stakeholders, and held a consultative meeting in December 2007 in Brussels to present draft proposals, which established most had wide stakeholder support. The formal outcome of our work was a detailed report, 'Security Economics and the Internal Market', published by ENISA in March 2008. This paper presents a much abridged version: in it, we present the recommendations we made, along with a summary of our reasoning.

1 Introduction

Until the 1970s, network and information security was the concern of national governments. Intelligence agencies used eavesdropping and traffic analysis techniques against rival countries, largely in the context of the Cold War, and attempted to limit the penetration of their own countries' networks by rival agencies. From the 1970s until about 2004, however, the centre of gravity in information security shifted from governments to companies. As firms became ever more dependent on networked computer systems, the prospect of frauds and failures has increasingly driven investment in research and development.

Since about 2004, volume crime has arrived on the Internet. All of a sudden, criminals who were carrying out card fraud and attacks on electronic banking got organised, thanks to a handful of criminal organisations and a number of chatrooms and other electronic fora where criminals can trade stolen card and bank account data, hacking tools and other services. Hacking has turned from a sport into a business, and its tools are becoming increasingly commoditised. There has been an explosion of crimeware – malicious software used to perpetrate a variety of online crimes. Keyloggers, data theft tools and even phishing sites can be constructed using toolkits complete with sophisticated graphical user interfaces. The

'quality' of these tools is improving rapidly, as their authors invest in proper research, development, quality control and customer service.

Most commonly, crimeware is spread by tricking users into runing code that they got in email attachments or downloaded from a malicious web site. However, its distribution is becoming more sophisticated as the criminal economy develops. For example, one so-called affiliate marketing web site offers to pay webmasters a commission ranging from US$0.08 to US$0.50 per infection to install iframes that point to an attacker's site which distributes crimeware (Jakobsson and Ramzan 2008). Meanwhile, network and information security is of growing economic importance in Europe (as elsewhere): sales of anti-virus software, cryptographic products, and services ranging from spam filtering through phishing-site 'take-down' to brand protection and copyright enforcement are in the billions of euros per annum. The economic study of information security is thus of rapidly growing relevance to policy makers.

Since about 2000, researchers have realised that many security failures have economic causes (Anderson and Moore 2006). Systems often fail because the organisations that defend them do not bear the full costs of failure. For example, in countries with lax banking regulation, banks can pass more of the cost of fraud to customers and merchants, and this undermines their own incentive to protect payment systems properly. In addition, so long as anti-virus software is left to individuals to purchase and install, there may be a less than optimal level of protection when infected machines cause trouble for other machines rather than their owners.

Our key message is that in order to solve the problems of growing vulnerability and increasing crime, policy and legislation must coherently allocate responsibilities and liabilities so that the parties in a position to fix problems have an incentive to do so. For a variety of reasons, the state will have a role to play, either as policeman, or regulator, or coordinator. In the specific case of the European Union, regulatory options range from direct legislation (previous examples being the Data Protection Directive and the Electronic Commerce Directive), sector-specific regulation (such as the recent Payment Services Directive), coordinating groups (such as the Article 29 Working Party on data protection law), the funding of research, down to the collection and publication of information.

In our complete report[1], we provide a more complete regulatory context and weigh the different options in greater detail. In this short paper, we describe just the final recommendations we made, along with our reasoning. By way of disclaimer, we note that these recommendations are our own and do not necessarily reflect the policy of ENISA or any other European institution.

[1] "Security Economics and the Internal Market", available at http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf.

1.1 Economic Barriers to Network and Information Security

We used five general headings to classify and analyse the economic barriers to network and information security, which form the structure of our paper: information asymmetries, externalities, liability, diversity, and the fragmentation of legislation and law enforcement.

Information Asymmetries Asymmetric information can be a strong impediment to effective security. Akerlof's model of the 'market for lemons' (Akerlof 1970) appears to apply to many security product markets. The tendency of bad security products to drive out good ones from the marketplace has long been known, and at present the main initiative to overcome asymmetric information supported by the Commission and Member State governments is the Common Criteria.

It has also long been known that we simply do not have good statistics on online crime, attacks and vulnerabilities. Companies are hesitant to discuss their weaknesses with competitors even though a coordinated view of attacks could allow faster mitigation to everyone's benefit. In the USA, this problem has been tackled by information-sharing associations, security-breach disclosure laws and vulnerability markets.

Externalities Many important security threats are characterised by negative externalities. For example, home computers are increasingly being compromised and loaded with malware used to harm others. As a result, a user who connects an unpatched computer to the Internet does not face the full economic consequences of her action. A further set of externalities affect Internet service providers (ISPs). Small-to-medium ISPs have an incentive to clean up user machines (as being a source of spam damages their peering relationships (Serjantov and Clayton 2005)) while large ISPs at present enjoy a certain impunity.

Network externalities also affect many protective measures. For example, encryption software needs to be present at both ends of a communication in order to protect it; the first company to buy encryption software can protect communications with its branches, but not with its customers or its suppliers. In other circumstances, investments can be strategic complements: an individual taking protective measures may also protect others, inviting them to free-ride.

Liability Dumping Firms seeking to manage risk often dump it on less powerful suppliers or customers. Software and service suppliers impose licenses on customers disclaiming all liability, including for security failures, and may also take 'consent' to the installation of spyware. This may delay the emergence of a market for more secure languages and tools, and lessen demand for the employment of professional software engineering methods.

Another example is the problem of mobile phone security; mobile phones have a long and complex supply chain, starting from the intellectual property owners, the chipmaker, the software supplier, the handset vendor, the network operator and the service provider. Each of these players seeks to have others bear the costs of security as much as possible, while using security mechanisms to maximise its own power in the chain. One side effect has been the failure of the OMA DRM Architecture V2 to come into widespread use, which in turn may have depressed the market for music downloads to mobile phones.

A third example is in payment services. The recent Payment Services Directive goes some way towards harmonisation of service rules across the EU but still leaves consumer protection significantly behind the USA. Banks are allowed to set dispute resolution procedures by their terms and conditions, and do so in their favour – as found for example in the recent report of the UK House of Lords Science and Technology Committee into Personal Internet Security (House of Lords 2007), which recommended that the traditional consumer protection enshrined in banking law since the nineteenth century should be extended to electronic transactions too.

Lack of Diversity Lack of diversity is a common complaint against platform vendors, whether Microsoft or Cisco or even Symbian. This is not just a matter for the competition authorities; lack of diversity makes successful attacks more devastating and harder to insure against, as high loss correlation renders some market segments uninsurable. Thus the market structure of the IT industry is a significant factor in society's ability to manage and absorb cyber risks.

Communication service providers are also affected; smaller ISPs find it cheaper to use single peering points, with the result that only large ISPs offer their customers resilience against peering point outage. This not only places these smaller ISPs (which are mainly small-to-medium enterprises (SMEs) and providing services to SMEs) at a disadvantage but shades over into critical national infrastructure concerns.

Fragmentation of Legislation and Law Enforcement Fragmentation of jurisdictions hinders rapid response. For example, the most important factor in deterring and frustrating phishing attacks is the speed of asset recovery. A bank learning of a customer account compromise needs to be able to trace and freeze any stolen assets quickly. The phishermen send hot money through the banks of Member States with a relaxed attitude to asset recovery. This issue spills over to money laundering.

A serious problem is that traditional mechanisms for international police cooperation are too slow and expensive for the Internet age. They evolved when international investigations were infrequent and dealt with matters that were either procedurally simple (such as the extradition of a fugitive) or a large investigation of mutual interest (such as drug smuggling). They do not cope well (or in some cases at all) with volume crime that crosses national boundaries.

2 Information Asymmetries

There has long been a shortage of hard data about information security failures, as many of the available statistics are not only poor but are collected by parties such as security vendors or law enforcement agencies with a vested interest in under- or over-reporting. These problems are now being tackled with some success in many US states with security-breach reporting laws, which we describe in Section 2.1. We also consider other opportunities for collecting relevant data in Section 2.2.

2.1 Security-Breach Notification

The first security-breach notification law to be enacted in the United States was California's A.B.700 in September 2002 (California State Senate 2002). It applies to public and private entities that conduct business in California and requires them to notify affected individuals when personal data under their control has been acquired by an unauthorised person. The law was intended to ensure that individuals are given the opportunity to take appropriate steps to protect their interests following data theft, such as putting a 'lock' on their file at credit agencies. It was also intended to motivate companies holding personal data to take steps to keep it secure. Indeed, (Acquisti et al. 2006) found a statistically significant negative impact on stock prices following a breach. Breach disclosure laws have also had the positive effect of contributing valuable data on security incidents to the public domain.

The California law has been followed by further laws in at least 34 other states[2], although they differ somewhat in their details. The variations have led to calls for a federal statute, but although bills have been introduced in Congress, none have had much success so far. In Europe, a security breach notification law has been proposed that would require notification to be made where a network security breach was responsible for the disclosure of personal data (European Commission 2006). This is a very narrow definition and will only deal with a small fraction of the cases that a California-style law would cover. Many incidents, such as criminals fitting an automatic teller machine (ATM) with a skimmer that steals card details (BBC 2007), would only be covered by a California-style law.

The US experience demonstrates the disadvantages of a patchwork of local laws, and the obvious recommendation is that a security breach notification law should be brought forward at the EU level, covering all sectors of economic activity rather than just telecomms companies. Indeed, the point of security breach notification is to avoid all the complexity of setting out in detail how data should be protected; instead it provides incentives for protection. It does not impose the bur-

[2] http://www.ncsl.org/programs/lis/cip/priv/breach.htm

den of a strict liability regime across the whole economy, but relies on 'naming and shaming'. Competent firms should welcome a situation where incompetent firms who cut corners to save money will be exposed, incur costs, and lose customers. This levels up the playing field and prevents the competent being penalised for taking protection seriously.

Recommendation 1: We recommend that the EU introduce a comprehensive security-breach notification law.

As well as informing the data subjects of a data breach, a central clearing house should be informed as well. This ensures that even the smallest of breaches can be located by the press, investors, researchers, and sector-specific regulators. The law should set out minimum standards of clarity for notifications – in the US some companies have hidden notices within screeds of irrelevant marketing information. Finally, notifications should include clear advice on what individuals should do to mitigate the risks they run as a result of the disclosure; in the US many notifications have just puzzled their recipients rather than giving them helpful advice.

2.2 Further Data Sources

While breach-disclosure notification laws also serve as a useful data source on information security, a wider selection of data needs to be collected in an unbiased manner. A number of sources already collect relevant data, which comes in many forms. For the past twelve years, the US-based Computer Security Institute has annually surveyed enterprises, asking respondents whether they have been attacked and, if so, what the resulting losses were (Computer Security Institute 2007). In 2003, Eurostat started collecting data on Internet security issues from both individuals and enterprises in in its 'Community Surveys on ICT Usage (European Commission 2006). Many security vendors also regularly publish reports on attack trends (e.g., (Symantec 2007)). Industry groups also sometimes disclose useful statistics, including the Anti-Phishing Working Group and APACS, the UK payments association. Finally, some academics conduct useful data collection and analysis (e.g., analysing phishing website lifetimes (Moore and Clayton 2007) and tracking botnets (Zhuge et al. 2007)).

While governments can specify requirements for data collection, it is up to the stakeholders to actually provide the data. Security vendors will feel it in their interest to provide inflated statistics; phishing statistics often seem particularly fishy. For example, the anti-phishing group PhishTank has boasted about the large number of sites it identifies (OpenDNS 2007), when in reality the number of duplicates reduces the overall number several fold. APACS provides another example by asserting a 726% increase in phishing attacks between 2005 and 2006 (with merely a 44% rise in losses) (APACS 2007).

ISPs, by contrast, have an incentive to undercount the amount of wickedness emanating from their customers, particularly if they are held to account for it. But there is an even more pernicious problem with ISP reporting: ISPs hold important private information about the configuration of their own network that influences measurements. In particular, policies regarding dynamic IP address assignment can greatly skew an outside party's estimate of the number of compromised machines located at an ISP. ISPs also regard the size of their customer base as a company secret, which makes cross-ISP performance comparisons difficult.

In more mature sectors of the economy, we can see useful examples of statistical institutions collecting business data jointly with industry bodies. For example, safety and accident statistics for cars are collected by police and insurers, while media circulation figures are typically collected by private firms, some of them jointly owned and controlled by publishers and advertisers.

At the behest of the European Commission, ENISA recently investigated whether to establish a framework for sharing collected data on information security indicators between interested parties (Casper 2008). They identified around 100 potential data sources, then surveyed a core of potential partners (CERTs, MSSPs, security vendors, etc.) who were invited to a workshop to further gauge interest. Unfortunately, there was very little desire for sharing raw data, aggregated data, or indeed any information that doesn't already appear in the publicly-issued reports. Hence mandatory reporting of particular indicators may be required for sharing to happen.

We recommend that ENISA's information sharing efforts focus on industries with a clear benefit but where sharing is not already taking place in every Member State – and the two industries where more information should be made available are the financial industry and ISPs.

Individual banks are usually keen to keep data on fraud losses private. But one notable exception is the UK, where APACS has published aggregated figures for the annual amount lost to phishing attacks, as well as ATM crime and other financial fraud (APACS 2007). While the incentives are against individual financial institutions revealing losses publicly, a country-wide aggregation may still aid policymakers without inhibiting honest reporting very much. As far as we can tell, no other Member State publishes statistics of this kind. As banks collect such statistics for operational, internal control and audit purposes, and aggregating them nationally is straightforward, we believe this practice should become standard practice in the EU. The statistics are particularly critical to the formulation of policy on network and information security since the majority of the actual harm that accrues is financial. Without a good measure of this, other figures – whether of vulnerabilities, patches, botnets, or bad traffic – lack a properly grounded connection to the real economy.

Recommendation 2: We recommend that the Commission (or the European Central Bank) regulate to ensure the publication of robust loss statistics for electronic crime.

In many cases, fraud statistics are already collected by the police or banking associations, so regulatory action should aim at harmonisation of definitions, metrics and release cycles across Member States. A good first step would be to require figures broken down broadly as the APACS statistics are and show losses due to debit and credit card fraud (subdivided into the useful categories such as card cloning versus cardholder-not-present, national versus international, and so on).

As for the information that should be published by and about ISPs, it is well known at present within the industry that some ISPs are very much better than others at detecting abuse and responding to complaints of abuse by others. This is particularly noticeable in the case of spam. A small-to-medium sized ISPs may find its peering arrangements under threat if it becomes a high-volume source of spam, so such ISPs have an incentive to detect when their customers' machines are infected and recruited into botnets. Large ISPs don't face the same peering-arrangement pressures, so as a result some send significantly larger quantities of spam and other bad traffic than others. We feel it would be strongly in the public interest for quantitative data on ISPs' security performance to be made available to the public.

Recommendation 3: We recommend that ENISA collect and publish data about the quantity of spam and other bad traffic emitted by European ISPs.

As Europe has some 40,000 ISPs, a staged approach may be advisable – with initial reports collected using sampling, followed if need be by action through telecomms regulators to collect more detailed statistics. However, even rough sample data will be useful, as it is the actions of the largest ISPs that have the greatest effect on the level of pollution in the digital environment.

Anyway, we feel that ENISA should take the lead in establishing these security metrics by setting clear guidelines, collating data from ISPs and other third parties, and disseminating the reported information. To begin with, ENISA could make a positive contribution by collecting and disseminating data on the rate at which ISPs are emitting bad packets. Such data could serve as a useful input to existing interconnection markets between ISPs since high levels of bad traffic can be costly for a receiving ISP to deal with.

The types of digital pollution to be measured must be defined carefully. To track spam, useful metrics might include: the number of spam messages sent from an ISP's customers; the number of outgoing spam messages blocked by an ISP; the number and source of incoming spam messages received by an ISP; and the number of customer machines observed to be transmitting spam for a particular duration. To track other types of malware, the number of infected customer machines would be relevant, along with the duration of infection.

Once data are available on which ISPs are the largest polluters, the next question is what should be done about them. This moves us from the heading of 'information asymmetries' to our next heading, 'externalities'.

3 Externalities

Externalities are the side effects that economic transactions have on third parties. Just as a factory belching smoke into the environment creates a negative externality for people downwind, so also people who connect infected PCs to the Internet create negative externalities in that their machines may emit spam, host phishing sites and distribute illegal content such as crimeware. The options available are broadly similar to those with which governments fight environmental pollution (a tax on pollution, a cap-and-trade system, or private action). Rather than a heavyweight central scheme, we think that civil liability might be tried first. We first discuss the different stakeholders to whom pressure might usefully be applied before detailing our recommendation.

3.1 Who Should Internalise Externalities Caused by Malware?

At present, malware used to harm others is the backbone of the underground economy in electronic crime. Such malware is installed using social engineering, by exploiting weaknesses in core platforms (operating systems, communications systems and server software) or via applications. Responsibility for correcting the externality might plausibly fall on several stakeholders.

One option is to assign responsibility to the software vendors for making software vulnerable in the first place. We consider what can be achieved using the stick of software liability in Section 4. However, we note here that the incentives are not as misaligned for core platforms – Microsoft has been improving its security for some time and suffers negative publicity when vulnerabilities are publicised. However, exploits at the application level require a different approach. Users readily install add-on features to web browsers, load web applications from untrustworthy firms, and run unpatched or out-of-date software. Users might also not install or update anti-virus software.

The machine owner is another important stakeholder. But there is a big difference between large and small owners. Large companies manage their machines by having a network perimeter where devices such as firewalls minimise exposure to compromise and restrict outbound communications from compromised machines; they also employ technicians to repair infected devices.

Individual end users and SMEs can do much less. They can and should maintain updated software, from the OS to applications and anti-virus tools; but they cannot protect themselves at the network perimeter as effectively as large businesses can, and can have tremendous difficulty repairing compromised devices.

The next influential stakeholder is the ISP. Compared to the others, ISPs are in a good position to improve the security of end-user and SME machines. ISPs control a machine's Internet connection, and therefore its ability to harm others. There

are many steps an ISP can take to limit the impact of malware-infected customer devices onto others, from disconnection to traffic filtering. ISPs can also communicate with customers by telephone or post, not just by Internet channels.

ISPs are divided on whether they should actively isolate infected customer machines, let alone whether they should try to prevent infections. One survey found that 41% of ISP respondents believed that they should clean up infected hosts, with 30% disagreeing and 29% uncertain (McPherson et al. 2007). Taking costly steps to repair customer machines, potentially including the unpopular move of temporarily cutting off service, is undesirable for ISPs when most of the negative effects are not borne by others.

3.2 Policy Options for Coping with Externalities

If ISPs should take action to raise the level of end-user security, then how can we best encourage them? A laissez-faire approach of encouraging best practice through self-regulation is tempting but likely to be insufficient. This is because the incentives on taking costly remedial action are weak at best (van Eeten and Bauer 2008), and since the poor performance of even a minority of ISPs can overshadow the operations of the best. Assigning liability for infected customers to ISPs is undesirable in practice due to the potentially high transaction cost of lawsuits, and the difficulty of valuing the monetary loss associated with individual events.

An alternative is to introduce fixed penalty charges if ISPs do not take remedial action within a short time period of notification. Upon notice of malicious activity, ISPs should place the machine into quarantine, clean up the offending content and reconnect the user as soon as possible. At present, there is great variation in the response times for ISPs when notified that a customer's machine is infected – the best ISPs remove phishing sites in less than one hour, while others take many days or even weeks to respond. Introducing a fixed penalty for machines that continue to misbehave after a reasonable duration, say 3 hours, would drastically speed up remedial action.

Fixed penalties are useful because they avoid the problem of quantifying losses following every infringement. They have been used effectively in the airline industry, where the EU has introduced penalties for airlines that deny passengers boarding due to overbooking, cancellations or excessive delays. The goal of this regulation is provide an effective deterrent to the airlines. Fixed penalties are also routinely used for traffic violations. Again, the penalties deter violations while simplifying liability when violations occur. The threat of penalties should alter behaviour so that, in practice, fixed penalties are rarely issued.

For fixed penalties to work, a consistent reporting mechanism is important. Fortunately, existing channels can be leveraged. At present, several specialist security companies already track bad machines and notify ISPs to request cleanup.

This process could be formalised into a quarantine notice. End users could also send notifications to `abuse@isp.com`, as is already possible for reporting spam.

One issue to consider is to whom the fixed penalty should be paid. To encourage reporting, the penalty could be paid to whoever sent the notice. What about duplicate payments? One compromised machine might send millions of spam emails. If a fixed penalty had to be paid for each received report, then the fine may grow unreasonably large. Instead, the penalty should be paid to the first person to report an infected machine, or perhaps to the first ten who file reports.

Given the threat of stiff penalties for slow responses, ISPs might become overzealous in removing reported sites without first confirming the accuracy of reports. This might lead to a denial-of-service-attack where a malicious user falsely accuses other customers of misdeeds. There is also the established problem that firms who want a machine taken down for other reasons – because they claim that it hosts copyright-infringing material, or material defamatory of their products – are often very aggressive and indiscriminate about issuing take-down notices. These notices may be generated by poorly-written automatic scripts, and result in risk-averse ISPs taking down innocuous content.

In theory, a user can tell her ISP to put back disputed content and assume liability for it, but often the ISP will then simply terminate her service, rather than risk getting embroiled in a legal dispute. In many countries, ISPs have got into the habit of writing their contracts so that they can terminate service on no notice and for no reason. So there has to be a 'put-back' mechanism that users can invoke to get their ISPs to reconnect an incorrectly classified machine quickly by assuming liability for any wicked emanations. Consumers only need assume liability if they skip the quarantine process. In practice, we anticipate most consumers will elect to participate in the ISP's cleanup service.

It is not the purpose of our report to provide a detailed design of a fixed-penalty system, as this would have to evolve over time in any case. We nonetheless feel that it is the single measure most likely to be effective in motivating the less well-managed ISPs to adopt the practices of the best.

Recommendation 4: We recommend that the European Union introduce a statutory scale of damages against ISPs that do not respond promptly to requests for the removal of compromised machines, coupled with a right for users to have disconnected machines reconnected by assuming full liability.

We learned from the stakeholders' meeting that this is the most controversial of our recommendations. We therefore say to the ISP industry: do you accept it is a problem that infected machines remain connected to the Internet, conducting attacks for extended periods of time? And if so, what alternative means do you propose for dealing with it? Do we need policemen in each ISP dealing with infected machines, or could the ISPs' own staff do it more efficiently and cheaply?

4 Liability Assignment

A contentious political issue is liability for defective software. The software industry has historically disclaimed liability for defects, as did the motor industry for the first sixty years of its existence. There have been many calls for governments to make software vendors liable for the harm done by shoddy products. As society depends more on software, we will have to tackle the 'culture of impunity' among its developers.

To illustrate the many complexities surrounding software liability, we now describe an example using a navigation system. Suppose that a citizen purchases a navigation system to use with a mobile home and, relying on it, is directed by a software error down a small country lane where his mobile home gets stuck, as a result of which he incurs significant towing and repair costs. This case is interesting because navigation can be supplied in a number of ways as a product, as a service, or as a combination of both, for example:

1. one could buy a self-contained GPS unit in a shop;

2. a driver can also get a navigation system in the form of software to run on his PDA or laptop computer;

3. navigation is also available as a service, for example from Google Maps;

4. many high-end mobile phones have built-in GPS, and can also provide route advice either through embedded software or an online service;

5. a GPS receiver in a driver's mobile phone might connect to route-finding software in his laptop;

6. a driver's proprietary system might run on an open platform such as Linux;

7. as well as proprietary route-finding systems, there is a project[3] to build a public-domain map of the whole world from GPS traces submitted by volunteers.

So which of the above suppliers could the mobile home owner sue? Certainly it is common for GPS equipment vendors to put up disclaimers that the driver has to click away on power-up, but the Product Liability Directive (European Economic Community 1985) should aid consumers. This suggests that, at least at the consumer level, we should be able to deal with the liability issues relating to embedded systems – that is, the software inside cars, consumer electronics and other stand-alone devices – as a product-liability matter.

[3] See http://www.openstreetmap.org

However, the Product Liability Directive does not apply to business property. Thus although our mobile-home driver can sue, a truck driver whose load of seafood got stuck and spoiled in exactly the same narrow lane has no recourse under the Product Liability Directive. The Unfair Contract Terms Directive, or other legal doctrines, might come to the rescue. To be fair, this complexity is a general problem for Community law and is not IT-specific. There is a further problem of jurisdiction: a business might rely on software downloaded from a website in California, which makes it clear that the contract is governed by the laws of California, and subject to the exclusive jurisdiction of that state. If the contract contains an exclusion that is valid under California law, then there may be little that the business can do if it is damaged by a software failure. Again, this is a general problem: there may be little the Community can do, as even if EU courts took jurisdiction their judgments would not be enforceable in California.

4.1 Software and Systems Liability Assignment

The above example should illustrate that software liability is both widely misunderstood and complex. But something may still need to be done. Our civilisation is becoming ever more dependent on software, and yet the liability for failure is largely disclaimed and certainly misallocated. We take the pragmatic view that software liability is too large an issue to be dealt with in a single Directive, because of the large and growing variety of goods and services in which software plays a critical role. We suggest that the Commission take a patient and staged approach. There are already some laws that impose liability regardless of contract terms (e.g., for personal injury), and it seems prudent for the time being to leave standalone embedded products to be dealt with by regulations on safety, product liability and consumer rights. Networked systems, however, can cause harm to others, and the Commission should begin to tackle this.

A good starting point would be to require vendors of PCs and other network-connected programmable devices to certify that their products are secure by default. It is illegal to sell a car without a seatbelt, so why should shops be allowed to sell a PC without an up-to-date operating system and a patching service that is switched on? This gives a more direct approach to the problem than assigning more specific rights to sue for damages. However, vendors who sell insecure systems should then be exposed to lawsuits from ISPs and other affected parties.

Recommendation 5: We recommend that the EU develop and enforce standards for network-connected equipment to be secure by default.

The precise nature of ‘secure by default’ will evolve over time. At present, the most important issue is whether the operating system is patched when the customer first gets it, and subsequently. The most likely solution would be to redesign

the software so that the machine would not connect to any other online service until it had visited the patching service and successfully applied an update. Regulation should seek to enforce the principle of security by default rather than engineer the details, which should be left to market players and forces. Note that we are careful to specify 'all network-connected equipment', not just PCs; if we see more consumer electronic devices online, but lacking mechanisms to patch vulnerabilities, then in due course they will be exploited.

One of the stakeholders expressed concern at the likely costs if all consumer electronics required Common Criteria certification to EAL4; our view is that it would be quite sufficient for vendors to self-certify. However, the vendor should be liable if the certification later turns out to have been erroneous. Thus if a brand of TV set is widely compromised used to host phishing sites, the ISPs who paid penalty charges for providing network connectivity to these TV sets should be able to sue the TV vendor. It would then be a matter for the court to decide fault on the facts. (We expect that once one or two landmark cases have been decided, the industry will rapidly adapt.)

In this way the Commission can start to move to a more incentive-compatible regime, by relentlessly reallocating slices of liability in response to specific market failures. The next question is what other liability transfers should be made initially. The most important matters at the present time have to do with patching – at which we now look in greater detail.

4.2 Patching

Patching is an unfortunate but essential tool in managing the security of information systems. Patching suffers from two types of externality. First, it is up to the software developer to create patches, but the adverse effects of a slow release are felt by consumers and the online community generally, rather than the companies directly involved. Second, the deployment of patches is costly, especially for large organisations. The publication of a patch often reveals the vulnerability to attackers, and then the unpatched, compromised machines are used to harm others; so the local benefits of patching may be less than the local costs, even when the global benefits greatly exceed the costs.

The first key challenge is to speed up patch development. The lag between vulnerability discovery and patch deployment is critical. During this period, consumers are vulnerable to exploits and have no recourse to protect themselves. Software vendors are often slow in deploying patches, and there is great variation in the patch-development times exhibited by different vendors. Among 5 leading OSs, Microsoft and Red Hat are fastest, Sun and HP are slowest by far, and Apple is in the middle (Symantec 2007). Consumer-oriented OSs tend to patch faster, perhaps because there is greater consumer demand and awareness.

For a sample of vulnerabilities exploited by Chinese websites in 2007 (Zhuge et al. 2008), nearly half were actively exploited in the wild before a patch was disclosed. Furthermore, the time lag between a vulnerability being disclosed and appearing in the wild is just two days, while patches took nearly two weeks to be published (if they were released at all). This suggests that there is scope for speeding up patch dissemination.

Vulnerability disclosure is often what triggers the development and deployment of patches. Yet the process by which the vulnerability is disclosed can affect the time vendors take to release patches. Some security researchers advocate full and immediate disclosure: publishing details (sometimes including exploit code) on the Bugtraq mailing list[4]. While undoubtedly prompting the vendors to publish a patch, full and immediate disclosure has the unfortunate side effect of leaving consumers immediately vulnerable. Vendors, for their part, typically prefer that vulnerabilities never be disclosed. However, some vulnerabilities might go undiscovered by the vendor even when they're being exploited by miscreants, and non-disclosure creates a culture in which vendors turn a blind eye.

A more balanced alternative is responsible disclosure as pioneered by CERT/CC in the US. CERT/CC notifies vendors to give them time to develop a patch before disclosing the vulnerability to the public. When the vulnerability is finally disclosed, no exploit code is provided. Empirical analysis comparing the patch-development times for vulnerabilities reported to Bugtraq and to CERT/CC revealed that CERT/CC's policy of responsible disclosure led to *faster* patch-development times than Bugtraq's full disclosure policy (Arora et al. 2005). The researchers also found that early disclosure, via CERT/CC or Bugtraq, does speed up patch-development time.

Another option is to assign liability for vulnerabilities to the software vendor until a patch is made available and consumers have had a reasonable chance to update. (Cavuso_lu et al. 2006) compare liability and cost-sharing as mechanisms for incentivising vendors to work harder at patching their software. It turns out that liability helps where vendors release less often than they should.

Recommendation 6: We recommend that the EU adopt a combination of early responsible vulnerability disclosure and vendor liability for unpatched software to speed the patch-development cycle.

While quantitative measurements are difficult to obtain, the view among security professionals is that patches are already available for the majority of exploits used by attackers. Over half of the exploits in the study by (Zhuge et al. 2008) first appeared on Chinese websites only after a patch had already made available. Hence, a second key challenge is to increase the uptake of patches among users.

So why do some users remain unpatched? While most operating systems offer automatic patching, many third-party applications like web browser add-ons do

[4] http://www.securityfocus.com/archive/1.

not. Vendors who do not provide automated patches could be held liable as part of the 'secure default' approach discussed in Recommendation 5. Meanwhile, some perfectly rational users (especially at the enterprise level) choose not to patch immediately because of reliability and system stability concerns.

Vendors must make patching easier and less of a nuisance for consumers. One simple way of doing this is to decouple security patches from feature updates. Users may not want to add the latest features to a program for a variety of reasons. Feature updates could disrupt customisation, slow down performance, or add undesirable restrictions (e.g., DRM). Even though most feature updates are beneficial, the few exceptions can turn users off patching, even when it is in their interest to do so.

Recommendation 7: We recommend security patches be offered for free, and that patches be kept separate from feature updates.

4.3 Consumer Policy

Where consumers are involved one may need more protection. A particularly important context is the resolution of payment disputes. Many online frauds result in debits from bank accounts, whether via transactions for nonexistent goods or services, via fraudulent use of credit card data, or via direct attacks on online banking systems. The impact of fraud on the citizen thus depends critically on the ease of obtaining restitution. However this varies rather widely across Member States. Where banks can dump liability for fraud on merchants, or where banks and merchants can dump it on the customer, there arises a further moral hazard; when the parties most able to reduce fraud are shielded from its effects, they may make less effort than they should to prevent it.

The question of varying fraud liability and dispute resolution procedures has been raised from time to time, and so far has been avoided by legislators – most recently when the Payment Services Directive was being negotiated from 2002 to 2005 (European Union 2005). It is time for the Commission to tackle this issue.

Recommendation 8: The European Union should harmonise procedures for the resolution of disputes between customers and payment service providers over electronic transactions.

Competition is relevant here too. Consumers are in a weak position vis-à-vis competing vendors of products where there is an 'industry position' of disclaiming liability for defects (as with cars two generations ago, or software and online services today), yet they are in an even weaker position facing a monopoly supplier. In both cases, they are faced with shrink-wrap or click-wrap licenses that impose contract terms on them on a take-it-or-leave-it basis.

Shrink-wrap licenses are thought by legal scholars to be defective. The main applicable law in the EU is the Unfair Contract Terms Directive (European Union 2002), which makes a consumer contract term unfair 'if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer'. This is widely flouted by the software industry. For example, Article 5 requires that 'terms must always be drafted in plain, intelligible language'; yet in practice, end-user license agreements (EULAs) are written in dense legalese and made difficult to access; a large amount of text may appear via a small window, so that the user has to scroll down dozens or even hundreds of times to read it. Article 7 further requires Member States to ensure that 'adequate and effective means exist to prevent the continued use of unfair terms in contracts concluded with consumers by sellers or suppliers'.

Some companies use deceptive marketing techniques that break various EU laws. Spyware programs "monitor user activities, and transmit user information to remote servers and/or show targeted advertisements" (Edelman 2008). Spyware's installation strategies violate the Unfair Contract Terms Directive. In almost all cases, the installation will be done without valid, free consent, so spyware also violates the Data Protection Directive and the E-Privacy Directive (European Union 2002). As if that were not enough, spyware programs are often made deliberately hard to uninstall.

Dealing with spyware through regulation is difficult, since most spyware companies are based outside the EU (typically in the US). While directly regulating the practices of spyware vendors is difficult, effective sanctions are still possible by punishing the companies that advertise using spyware. In the 1960's, a number of unlicensed 'pirate' radio stations aimed at UK consumers were launched from ships just outside the UK's jurisdiction. The Marine Broadcasting Offences Act of 1967 made it illegal for anyone subject to UK law to operate or assist the stations. This immediately dried up advertising revenues, and the unlicensed stations were forced to fold. A similar strategy could undermine spyware, since many of the advertisers are large international companies that do business in the EU (Edelman 2004). While advertisers might object that they could be framed by competitors, an examination of the resulting evidence should vindicate any false accusations.

Another abusive practice already the target of regulation is spam. The EU Directive on Privacy and Electronic Communications (European Union 2002) attempts to protect consumers from spam. For the most part, it prohibits sending any unsolicited messages to individuals, requiring their prior consent. However, Article 13 paragraph 5, states that protections only apply to 'natural persons', and leaves it up to Member States to decide whether to allow unsolicited communications to business. Direct marketing lobbies argued that spamming businesses was essential to their trade. In practice, the business exemption has undermined the protections for consumers. It gives spammers a defence against all messages sent to 'work' domains. It also drives up costs for businesses, who must contend with

spam sent from potentially millions of other businesses. Finally, it is also difficult (in practice impossible) to draw clear lines between 'natural' and 'legal' persons in this context: some businesses (one-man firms, barristers, partners in some organisations) are legally 'natural' persons, while email addresses of identifiable individuals in companies relate to 'natural' persons. So there is a strong case to abandon the distinction. Therefore, we recommend repealing Article 13 paragraph 5, the business exemption for spam.

Putting all these together:

Recommendation 9: We recommend that the European Commission prepare a proposal for a Directive establishing a coherent regime of proportionate and effective sanctions against abusive online marketers.

The issues raised in this section on consumer policy are not limited to abusive marketing and unfair banking contracts. Perhaps the most important example concerns the foundation of the Single Market itself. It is a long-established principle that EU citizens can buy goods anywhere in the Union. The challenge now is that physical goods are increasingly bundled with online services, which may be priced differently in different Member States, or even unavailable in some of them. The bundling of goods and services is an area of significant complexity in EU law. Moreover, the segmentation of online service markets can affect information security. Sometimes market segmentation in B2B transactions impacts consumers; for example, citizens in one country can find it hard to open a bank account in another because of how credit-reference services are bundled and sold to banks. This in turn reduces consumers' ability to exert pressure on banks in countries where online banking service is less competitive by switching their business elsewhere.

The 2006 Services Directive takes some welcome first steps towards harmonising the market for services (European Union 2006). This Directive tries to remove many protectionist measures erected over the centuries by Member States to cosset domestic service providers. In our view another aspect warrants attention: the deliberate use of differential service provision as a tool by marketers, both as a means of discriminatory pricing and in order to undermine consumer rights.

Single-market service provision is very much broader than the scope of our report. Like the liability for defects in software – and in services – it is such a large topic that it will have to be tackled a slice at a time, and by many stakeholders in the Commission. We encourage ENISA to get involved in this policy process so that security aspects are properly considered in consumer-protection questions.

Finally, universal access to the Internet may also benefit from action under the heading of consumer rights. If all the ISPs in a country align their terms and conditions so that they can disconnect any customer for no reason, this should be contrary to public policy on a number of grounds, including free speech and the avoidance of discrimination. Even those citizens who are unpopular with some vocal lobby group must have the right to Internet connectivity.

Recommendation 10: ENISA should conduct research, coordinated with other affected stakeholders and the European Commission, to study what changes are needed to consumer-protection law as commerce moves online.

5 Dealing with the Lack of Diversity

Diversity can help security. Physical diversity deals with geographical distribution of redundant infrastructure components and network routes, whereas logical diversity means that distributed systems do not share common design or implementation flaws. A lack of diversity implies risk concentration which negatively affects insurability and thus an economy's ability to deal with cyber risks.

5.1 Promoting Logical Diversity

For logical diversity to happen, alternatives must be widely available and adoption well-balanced. In the information industries, this has rarely occurred: technical lock-in, positive network externalities and high switching costs tend to yield dominant-firm markets (Shapiro and Varian 1999). Nonetheless, there are steps governments can take to improve, or at least not hinder, the prospects for diversity.

A policy to foster diversity must first ensure the availability of viable alternatives. One option is to promote open standards to facilitate market entry. But even successful open standards do not always deliver diversity. Another option is to promote diversity in public procurement. Consumers and firms are short-sighted when selecting software; positive network externalities lead them to discount increases in correlated risk. Governments need not be so myopic, but there are limits to the impact governments can have through public procurement policies alone.

Regulatory responses may occasionally be required. However, regulation tends to work rather more slowly than the industry. Cisco used to have a very dominant market position in the routers deployed in the Internet backbone. A vulnerability in Cisco routers (Zetter 2005) was disclosed that could have removed a significant portion of the Internet backbone if a flash worm had been disseminated. So the lack of diversity among routers used to be a critical concern. But the market for backbone routers has balanced recently, given competition from Juniper and others. The market for mobile-phone software similarly used to be dominated by Symbian, but that has also corrected itself somewhat thanks to challenges by Apple, Google, Microsoft and others. Finally, the market for web browsers is now more competitive following years of dominance by Internet Explorer. In general, we feel the authorities should maintain a watching brief for competition issues that

persist and have security implications.

Recommendation 11: We recommend that ENISA should advise the competition authorities whenever diversity has security implications.

5.2 Promoting Physical Diversity in CNI

Pitcom, a UK parliamentary group, has published a useful overview of critical national infrastructure (CNI) vulnerability aimed at legislators (Pitcom 2006). They show how an Internet failure could damage other parts of the CNI such as finance, food and health. Telecomms and power are known to be closely coupled: if a high voltage power line fails the engineers who go to fix it will keep in touch by mobile phone. But the mobile phones depend on the power supply to keep base stations operating. This particular problem can be fixed using satellite phones; but what other problems should we anticipate?

In principle, network designers avoid single points of failure using redundant components. However, as systems scale, they may be introduced beyond an individual network's control. For example, a major concern about single points of failure for the Internet is the growth of Internet Exchange Points (IXPs) such as LINX in London, AMSIX in Amsterdam, DECIX in Frankfurt, etc., and how one IXP per country tends to grow much larger than its rivals. ISPs use IXPs to reduce the costs of providing their customers with connectivity to the rest of the Internet.

The value of joining an IXP can increase as more ISPs join, leading to winner-take-all dynamics where one IXP is much larger than its local rivals. 11 EU countries have just one IXP; in almost all the others the largest IXP is 4 or more times the size of the next largest – the exceptions being Estonia, Spain, Belgium, and Poland (in each of which there are 2 roughly equal size IXPs, not a stable equilibrium) and France which, for complex historical reasons, is much more fragmented with 5 similar sized exchanges. These pressures towards a dominant IXP lead to possible single points of failure at the IXP itself. Some leading IXPs have invested heavily in redundancy; others haven't, mainly because of the expense.

CNI is now understood to be a multi-national issue. One of the key difficulties in this area is that CNI companies do not wish to discuss how they might be vulnerable, while governments have limited understanding of the real world: for example the COCOMBINE project in Framework 6 examined IXPs but failed to understand why peering does or does not take place between particular ISPs, and merely attempted to find spatial patterns, with limited success (D'Ignazio and Giovanetti 2006a; D'Ignazio and Giovannetti 2006b). Hence the most obvious policy option to adopt is that of encouraging information sharing – and more, better informed, research into the actual issues.

Recommendation 12: We recommend that ENISA sponsor research to better understand the effects of IXP failures. We also recommend they work with telecomms regulators to insist on best practice in IXP peering resilience.

6 Fragmentation of Legislation and Law Enforcement

As well as providing the right incentives for vendors and service providers, and protection for consumers, it is important to catch cyber-criminals, who at present act with near impunity thanks to the fragmentation of law enforcement efforts. In order for the police to prosecute the criminals they catch, cyber-crimes must be offences in all Member States. Furthermore, as nearly all cyber-crimes cross national borders, cooperation across jurisdictions must be improved.

To a first approximation, existing legal frameworks have had no difficulty in dealing with the Internet. However, the cross-jurisdictional nature of cyberspace has meant that many criminals commit their offences in another country (often many other countries) and this leads to difficulties in ensuring that they have committed an offence in the country in which they reside.

The practical approach that has been taken is to try and harmonise national laws within a consistent international framework. The relevant treaty for the specific harms that cannot be dealt with by existing 'offline' legislation is the 2001 Convention on Cybercrime (Council of Europe 2001) which sets out the required offences, provides the requisite definitions and sets out a uniform level of punishments. All of the EU states have signed the convention, but some six years later only 12 have ratified, while 15 have failed to do so. If the harmonisation approach is to bear fruit, this process needs to be speeded up.

Recommendation 13: We recommend that the European Commission put immediate pressure on the 15 Member States that have yet to ratify the Cybercrime Convention.

Co-operation across law enforcement jurisdictions is essential for online crime, yet there are very serious impediments against police forces working together. Police forces must make tough choices in deciding which crimes to investigate. In the case of electronic crime, one of the first questions is how many local citizens are affected, and how many local computers are being used to launch attacks. Using this criteria, most attackers are not worth pursuing, even if in aggregate they are having a devastating effect. Even those cases that are deemed worth pursuing invariably lead to computers located in other countries. The current structures for international co-operation were designed for physical crimes, where cross-border activity is rare. They slow down investigations and drive up costs.

When a crime involves another country, law enforcement agencies may first attempt to establish a joint operation between police forces. In a typical joint op-

eration, the country where the investigation began does most of the work while the co-operating country serves warrants and obtains evidence as requested by the originating force. Joint operations are largely unfunded and carried out on a quid pro quo basis, so they cannot be relied upon as the baseline response to all cybercrimes. Co-operation may also be possible via a mutual legal assistance treaty (MLAT). MLATs require a political decision taken by the requested country's foreign ministry to determine whether co-operation can commence, and are very slow to process. So many investigators prefer to avoid using them where possible.

The problem of countries working together for a common cause while preserving national sovereignty has already been tackled by the military – whether it was SHAPE in World War II or NATO today. The model is that each country takes its own political decision as to what budget to set aside for fighting cybercrime. Part of this budget funds liaison officers at a central command centre. That command centre decides what tasks to undertake, and the liaison officers relay requests to their own countries' forces. This is in effect a permanent 'joint operation' that avoids the glacial speed of MLATs. The key is that countries trust their liaison officers to assess which requests carry no political baggage and can be expedited.

Recommendation 14: We recommend the establishment of an EU-wide body charged with facilitating international co-operation on cyber-crime, using NATO as a model.

7 Security Research and Legislation

Security research is important, and occurs at a number of places in the value chain. First, blue-sky (typically academic) researchers think up new algorithms, protocols, operating-system access-control schemes and the like. Second, applied researchers investigate how particular types of systems fail, and devise specific proposals for submission to standards bodies. These researchers can be academic, industrial, or a mix. Third, research and development engineers produce prototypes and write code for specific products and services. Fourth, users of these products or services discover vulnerabilities. These are often design or implementation errors rather than flaws in the underlying security technology.

Public policy has got in the way of security research on a number of occasions. The debate on cryptography policy during the 1990s led to EC Regulation 1334/2000 on Dual Use Goods under which the export of cryptographic software in intangible form (e.g. researchers swapping source code) became subject to export control. Many small software developers are unaware of this control regime and may be technically in breach of its implementation provisions in some Member States. More recently, in some Member States, well-meant but poorly drafted legislation has impeded security research. In Germany, the criminal law code (Strafgesetzbuch) has been amended with a new section 202c that makes it an of-

fence to produce, supply, sell, transmit, publish or otherwise make accessible any password, access code or software designed to perpetrate a computer crime, or in preparation for such a crime. This has been opposed as excessive by many researchers who see it as threatening those who possess system engineering tools for innocuous purposes (Anderson 2007). In the UK, the Government amended the Computer Misuse Act to make it an offence to "supply or offer to supply, believing that it is likely to be used to commit, or to assist in the commission of [a computer offence]" so that it is the meaning of 'likely' which will determine whether an offence has been committed. The government's response to concern about the circumstances in which an offence would be committed has been to promise to publish guidance for prosecutors as to when the law should be invoked.

In both cases the concern is that IT and security professionals who make network monitoring tools publicly available or disclose details of unpatched vulnerabilities could be prosecuted. Indeed, most of the tools on a professional's laptop, from nmap to perl, could be used for both good and bad purposes. The resulting legal uncertainty has a chilling effect on security research (Clayton 2007).

The industry needs an advocate in Brussels to ensure that its interests are taken into account when directives and regulations are being formulated – and as they evolve over time. In the case of export control, we recommend that ENISA push for cryptography to be removed from the dual-use list. In the case of dual-use tools that can be used for hacking as well as for bona-fide research and administrative tasks, we recommend ENISA take the position that sanctions should only apply in the case of evil intent.

Recommendation 15: We recommend that ENISA champion the interests of the information security sector within the Commission to ensure that regulations introduced for other purposes do not inadvertently harm security researchers and firms.

8 Conclusions

As Europe moves online, information security is becoming increasingly important: first, because the direct and indirect losses are now economically significant; and second, because growing public concerns about information security hinder the development of both markets and public services. While information security touches on many subjects from mathematics through law to psychology, some of the most useful tools for both the policy analyst and the systems engineer come from economics.

In our report, of which this is an abridged version, we provided an analysis based on security economics of the practical problems in network and information security that the European Union faces at this time. We have come up with fifteen policy proposals that should make a good next step in tackling the problems. We

therefore hope that they will provide the basis for constructive action by ENISA and the European Commission in the future.

Acknowledgements

The authors are grateful to acknowledge input from the attendees at the ENISA stakeholders' meeting on December 10th, 2007; from people in the security industry who talked to us, mostly off the record; from colleagues in the security groups at Cambridge and Dresden; from members of the Advisory Council of the Foundation for Information Policy Research, particularly Nick Bohm, Alan Cox, Douwe Korff, Jim Norton and Martyn Thomas; and from Alexander Korff of Clifford Chance. Responsibility for any errors and omissions of course remains with the authors alone.

References

Acquisti, A., Friedman, A., and Telang, R. "Is there a cost to privacy breaches? An event study", in *5th Workshop on the Economics of Information Security (WEIS)*, Cambridge, United Kingdom, June 2006.

Akerlof, G. "The market for 'lemons': quality uncertainty and the market mechanism". *Quart. J. Economics (84)*, 1970, pp. 488—500.

Anderson, N. "German 'anti-hacker' law forces hacker sites to relocate". *Ars Technica*, 14 August 2007. http://arstechnica.com/news.ars/post/20070814-german-anti-hacker-law-forcing-hacker-sites-to-relocate.html

Anderson, R., and Moore, T. "The Economics of Information Security", *Science* (314:5799), October 2006, pp. 610—613.

APACS. "Card fraud losses continue to fall", Press Release, APACS, 14 March 2007. http://www.apacs.org.uk/media_centre/press/07_14_03.html

Arora, A., Krishnan, R., Telang, R., and Yang, Y. "An empirical analysis of vendor response to disclosure policy", in *4th WEIS*, Cambridge, Massachusetts, June 2005.

BBC. "Devices attached to cash machines", *BBC News*, 15 October 2007. http://news.bbc.co.uk/1/hi/england/cambridgeshire/7044894.stm

California State Senate. *Assembly Bill 700*, 2002. http://info.sen.ca.gov/pub/01-02/bill/asm/ab_0651-0700/ab_700_bill_20020929_chaptered.pdf

Casper, C. "Examining the feasibility of a data collection framework", *ENISA*, February 2008.

Cavuso_lu, H., Cavuso_lu, H., and Zhang, J. "Economics of patch management", in *5th WEIS*, Cambridge, United Kingdom, June 2006.

Clayton, R. "Hacking tools are legal for a little longer", *Light Blue Touchpaper*, 19 June 2007. http://www.lightbluetouchpaper.org/2007/06/19/hacking-tools-are-legal-for-a-little-longer/

Computer Security Institute. "The 12th Annual Computer Crime and Security Survey", October 2007. http://www.gocsi.com/

Council of Europe. *Convention on Cybercrime*, CETS 185, November 2001. http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG

Edelman, B. "Advertisers using WhenU", July 2004. http://www.benedelman.org/spyware/whenu-advertisers/

Edelman, B. "Spyware: Research, testing, legislation, and suits", June 2008. http://www.benedelman.org/spyware/

van Eeten, M., and Bauer, J. "The Economics of Malware: Security Decisions, Incentives and Externalities", *OECD*, May 2008. http://www.oecd.org/dataoecd/25/2/40679279.pdf

European Commission. "i2010 Benchmarking Framework", November 2006. http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/060220_i2010_Benchmarking_Framework_final_nov_2006.doc

European Commission. "Report on the outcome of the Review of the EU regulatory framework for electronic communications networks and services in accordance with Directive 2002/21/EC and summary of the 2007 reform proposals", November 2007. http://ec.europa.eu/information_society/policy/ecomm/doc/library/proposals/com_review_en.pdf

European Economic Community. "Council Directive of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (85/374/EEC)", July 1985.

European Union. "Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts", April 1993. http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31993L0013&model=guichett

European Union. "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)", July 2002. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

European Union. "Directive 2006/123/EC of the European Parliament and of the Council of of 12 December 2006 on services in the internal market", December 2006. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:376:0036:0068:EN:PDF

European Union. "Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC Text with EEA relevance", November 2007. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:01:EN:HTML

House of Lords Science and Technology Committee. *Personal Internet Security, 5th Report of 2006—07*, The Stationery Office, London, August 2007.

D'Ignazio, A., and Giovannetti, E. "Spatial dispersion of peering clusters in the European Internet", *Cambridge Working Papers in Economics 0601*, January 2006. http://econpapers.repec.org/paper/camcamdae/0601.htm

D'Ignazio, A., and Giovannetti, E. "'Unfair' discrimination in two-sided Peering? Evidence from LINX", *Cambridge Working Papers in Economics 0621*, February 2006. http://econpapers.repec.org/paper/camcamdae/0621.htm

Jakobsson, M., and Ramzan Z. *Crimeware: Understanding New Attacks and Defenses*, Addison Wesley, Upper Saddle River, New Jersey, 2008.

McPherson, D., Labovitz, C., and Hollyman, M. "Worldwide Infrastructure Security Report Volume III", *Arbor Networks*, 2007. http://www.arbornetworks.com/report

Moore, T., and Clayton, R. "Examining the impact of website take-down on phishing" in *2nd Anti-Phishing Working Group eCrime Researcher's Summit (APWG eCrime)*, Pittsburgh, Pennsylvania, October 2007, pp. 1—13.

OpenDNS. “OpenDNS shares April 2007 PhishTank statistics”, Press Release, 1 May 2007. http://www.opendns.com/about/press_release.php?id=14

Pitcom. “Critical national infrastructure, briefings for parliamentarians on the politics of information technology”, November 2006. http://www.pitcom.org.uk/briefings/PitComms1-CNI.doc

Serjantov, A., and Clayton, R. “Modelling incentives for e-mail blocking strategies”, in *4th WEIS*, Cambridge, Massachusetts, June 2005.

Shapiro, C., and Varian, H. *Information Rules. A Strategic Guide to the Network Economy*, Harvard Business School Press, Boston, Massachusetts, 1999.

Symantec. “Internet security threat report volume XII”, September 2007. http://www.symantec.com/business/theme.jsp?themeid=threatreport

Zetter, K. “Router flaw is a ticking bomb”, *Wired*, 1 August 2005. http://www.wired.com/politics/security/news/2005/08/68365

Zhuge, J., Holz, T., Han, X., Guo, J., and Zou, W. “Characterizing the IRC-based botnet phenomenon”, *Reihe Informatik Technical Report TR-2007-010*, December 2007. http://honeyblog.org/junkyard/reports/botnet-china-TR.pdf

Zhuge, J., Holz, T., Song, C., Guo, J., Han, X., and Zou, W. “Studying malicious websites and the underground economy on the Chinese web”, in *7th WEIS*, Hanover, New Hampshire, June 2008.