# Towards a European Strategy for Internet Security

## An evolving landscape

The digital ecosystem with the Internet at its centre, has become the nervous system of our economy and society. Businesses and citizens are reaping huge economic and social benefits from online services and electronic interconnections. The pervasiveness of the Internet is a huge opportunity. But its [1>[2>[3>distributed architecture, which cuts across a high number of actors both public and private, and the distributed sharing of responsibility along the Internet chain also makes Internet open to all kind of attacks. <3]<2]<1]The number of disruptions and attacks targeting electronic networks and services and the seriousness of their impact have also increasingly hit the headlines. Threats can now originate from anywhere in the world and, impact any other part of the planet. A constant expansion of the threat landscape targets not only networks but also individual companies and public authorities and is eroding citizen's trust in engaging in the digital economy.

Securing the smooth functioning of this [4>vital infrastructure<4] is therefore essential to our economic stability and growth as well as to the well-being of the European society. Failure to do so, would pose an enormous risk to the proper functioning of the single market in terms of lost growth, jobs and prosperity, ([5>and to reaching the goal of achieving a true digital single market by 2015 and the objectives of the EU2020 Strategy<5]). The increasing sophistication of threats and the global interconnectedness call for [6>a much tighter cooperation and collaboration<6] between governments, between public and private sectors, taking-up respective responsibilities. Such [7>cooperation<7] should particularly be based on [8>information exchange<8], to ensure full transparency and lack of information asymmetry.

The continuous improvement of [9>security and resilience is contributing also to make the fight against cybercrime more effective.<9]

## Key questions:

***Is further action at EU level needed to contribute to a higher level of Internet Security?***
***If yes, [10>which should be the objectives<10] and [11>priority areas<11] for EU action?***

- *more [12>comprehensive, consistent and structured EU approach to Internet security<12]*
- *keeping the current [13>voluntary approach<13]*
- *towards a binding approach and[14> regulatory measures<14]*
- *[15>Strengthening the national and European cooperation at technical and strategic levels<15]*
- *[16>Strengthening the international cooperation<16]*
- *Government to government information sharing mechanisms*
- *[17>Public-private information sharing mechanisms<17]*

***What [18>[19>information sharing mechanisms<19]<18] would be needed between actors to improve preparedness against Internet security threats?***
***Is there an appropriate level of awareness on Internet security in the EU, among [20>[21> [22>citizens<22]<21]<20], [23>businesses<23] and [24>government bodies<24]?***
***If not, what [25>channels<25] and means could be used to [26>spread information about security threats and protective measures<26], in particular to [27>end-users?<27]***

- *national and [28>European security campaigns<28], incl. [29>simulations of pan-European or worldwide cyber attacks<29]*
- *[30>cyber-champion competitions<30]*
- *Hackathons?*

***Are there [31>other aspects that you consider worth raising in this context<31]?***

## Key facts

***…. on the importance of Internet to the economy***

- The [32>digital ecosystem enables the creation of high-quality jobs and supports smart and sustainable economic growth.<32]
- In Europe, the ICT sector and investments in ICT deliver around half of our productivity growth. The ICT sector alone represents almost 6% of the European GDP.
- Eighty percent of young Europeans are globally interconnected through on-line social networks 1, and approximately USD $8 trillion changes hands globally each year in ecommerce 2.
- The World Bank estimates that with 10% percent increase in high speed Internet connections, economic growth increases by 1.3%.

***…. on cyber-crime***

Cyber-attacks affect the deployment of ICT solutions used by citizens in their day-to-day lives, such as online payment and e-government services. Citizens are victims of various forms of on-line crimes ranging from stolen credit cards and identities to [33>child sexual abuse<33]. For example, [34>Germany saw an increase of 8.1% in Internet-related crimes during 2010<34]3. Estimates suggest that victims lose around 290 billion EUR each year worldwide as a result of cybercrime. A report by Symantec estimates that cybercrime has affected 431 million adults around the world in 2010 at cost of $388 billion in monetary and time losses

***… [35>on recent cyber attacks<35]***

In April 2011 Sony was the target of a devastating cyber attack that cost the company nearly $175 million (some estimate it as high as $ 2 billion 4) and stolen information about more that 100 million users. This economic loss was almost as much as the company suffered as a result of the devastating tsunami in May 2011.

The Dutch SSL certificate authority, DigiNotar, [36>suffered an attack in June 2011<36] which led to its subsequent bankruptcy.

Since 2008 the EU Emissions Trading Scheme has been subject of several attacks. In January 2011, around 30 million-worth of emissions allowances were stolen from the national registries.

In February 2011, more than 150 of the French finance ministry's 170,000 computers were hacked for documents related to the Group of 20 meeting hosted there.

The [37>computer systems of the European Commission and the European External Actions Service became subject to an attack in March 2011 and those of the European Parliament in January 2012<37].

Increasingly and contrary to prevailing general opinion, SMEs are becoming the target for organised cyber attacks. Since the beginning of 2010, 40% of all targeted attacks have been

directed at small and medium-sized businesses, compared to only 28% directed at large companies 5.

***…. on the wider impacts, on physical infrastructure, of cyber-attacks or Internet disruptions***

The attacks are not targeting only cyber space but can also seek to harm vital physical installations for public service and private business. [38>[39>[40>Critical infrastructures<40]<39]<38] in energy, finance and transport rely on Information and Telecommunications Technologies and the Internet and are thereby vulnerable as well, not only to attacks but also to technical disruptions that can spread [41>in an unpredictable manner throughout the networks<41]. According to the World Economic Forum in the next ten years there is a [42>10% likelihood of a major Critical Information Infrastructure breakdown with potential economic damages of over $ 250 billi<42]on.

1 *Eurostat, Internet Access and Use, 14 December 2010*
2 *McKinsey Global Institute, Internet Matters: the Net's sweeping impact on growth, jobs and prosperity.*
*Report May 2011*
3 *http://www.dw-world.de/dw/article/0,,15093336,00.html*
4 *http://www.reuters.com/article/2011/05/05/us-sony-insurance-idUSTRE74472120110505*
5 *http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf*

| | |
|---|---|
| [1] | Distributed<br>by Marten on June 6, 2012 at 5:48 p.m.<br>The distribuited architecture ensures no single point of failure. |
| [2] | Distributed<br>by Marten on June 6, 2012 at 5:48 p.m.<br>The distribuited architecture ensures no single point of failure. |
| [3] | Distributed<br>by Marten on June 6, 2012 at 5:48 p.m.<br>The distribuited architecture ensures no single point of failure. |
| [4] | Vital<br>by PeterSchein on June 8, 2012 at 11:30 a.m.<br>I agree that the infrastructure is vital. that should be the slogan. |
| [5] | Strategy<br>by PeterSchein on June 8, 2012 at 1:39 p.m.<br>What counts is outcome, not referencing one strategy paper by the other |
| [6] | Mixing state and business<br>by PeterSchein on June 8, 2012 at 11:28 a.m.<br>State should be free from business. It should set the rules for the market, not amalgamate with business. |
| [7] | too weak<br>by Marten on June 6, 2012 at 5:39 p.m.<br>Cooperation is too weak. We witness a market failure right now, companies lack incentive to fix their security bugs |

| | |
|---|---|
| [8] | Levels<br>by Marten on June 6, 2012 at 6:46 p.m.<br>Is is the task of the companies that their solutions are safe. They are not the same level and governments would be stupid to share sensitive information with them. Rather we need mechanisms where the source code gets public and when found vulnerabilities are not fixed in a reasonable time the companies get penalized in a dissuasive was or unrecommended / illegal for use by public officers. |
| [9] | That is important<br>by PeterSchein on June 8, 2012 at 11:31 a.m.<br>Indeed, go for the source of the problem, bad engineered software. |
| (9.1) | Re: That is important<br>by Paul Rhein (LU) on June 11, 2012 at 8:11 a.m.<br>I do agree. With all the cyber-efforts (NIS, CERTs, Exercises etc..) that are beyond any doubt necessary and useful activities. However we seem to be curing a patient which should not be ill in the first place or at least not to this exetend. We need to further involve the IT industries and take them accountable for the problems caused by their products in a way that we launch a process of further improving the quality of the solutions on the market.<br><br>tags: the root |
| [10] | Source code review<br>by Marten on June 6, 2012 at 5:25 p.m.<br>Only by reviewing source code and fixing the security bugs you could harden the systems. therefore source code has to be mandated open for critical components. |
| [11] | Education<br>by uzurutuza on June 6, 2012 at 4:46 p.m.<br>I find the given objectives/priority areas generally sound and correct. I miss an important educational objective. Most of the objectives are focusing on reaction, coordination and being prepared upon new threat disruptions. But cybercrime comes in form of social engineering attacks and exploiting vulnerabilities in poorly written software. Regulatory measures can help on |

| | |
|---|---|
| | creating certification mechanisms for security (specially on Critical Infrastructures), but priority must be given to educate ICT industry developers in secure programming practices to avoid vulnerabilities, and educate citizens in identifying digital abuse campaigns (spam, phishing, e-fraud).<br><br>tags: education, secure programming initiatives |
| [12] | Actions<br>by PeterSchein on June 8, 2012 at 1:37 p.m.<br>What is needed are actions which actually do make a difference, like * reviewing source code of critical components * sanctioning suppliers who do not fix security flaws uncovered * develop static analysis, testing and software quality tools * naming and shaming * warranty and compensation schemes in the case that the user is unable to fix the problem * poke yoke security settings for users * strengthen consumer protection in the field of virus / malware tools which are often a source of scam themselves. * Exit programme to employ virus developers to work on something else, like improving security * Strengthening data protection rules * develop software systems for traffic management what counts is tangible, technical activities, not awareness raising and smusing with the security industries. |
| [13] | Threat<br>by Marten on June 6, 2012 at 5:31 p.m.<br>Without threatening regulation and combatting parasitarian esecurity business models the EU Commission would not get anything out of that. |
| [14] | Privacy must be protected by legislation<br>by ahartman on June 4, 2012 at 1:43 p.m.<br>Due to the high cost of privacy protection, and the economic temptation to use private information for personal or corporate gain (e.g. Facebook) it is important for governments to enact protective legislation with appropriate penalties for privacy violation, and appropriate certification and privacy audit procedures.<br><br>tags: Privacy audit certification legislation |
| | |

| | |
|---|---|
| [15] | Scientific Coordinator<br>by pmassonet on June 1, 2012 at 2:14 p.m.<br>The EU could certainly play a coordination role for more operational protection for citizens and companies. This could be achieved via better cooperation between CERT. The role of CERTS is wide and covers prevention, detection, response and recovery. However in practice the recommendations remain high level. I would like to see more coordination in testing and monitoring of internet security. This could provide real-time alerts to EU citizens and improve prevention. For the moment it is very difficult to know when you are visiting a dangerous web site or when you are taking an action that could trigger an attack. If the EU could make any steps towards improving operational security on the internet that would be of great value to EU citizens. |
| [16] | with accountability<br>by gus on June 11, 2012 at 12:49 p.m.<br>Too often, initiatives at international cooperation involve closed discussions that exclude some sectors and some processes to ensure accountability and transparency. |
| [17] | Disclosure of source code<br>by Marten on June 6, 2012 at 5:22 p.m.<br>The EU should mandate disclosure of the source code for critical software components. Professionals in the security industry tell that security by obscurity does not work. Only disclosure would simplify to find security bugs and lead to a hardening of systems. Esp. as more and more hardware components come from China lack of dislosure poses a serious national security risk because software of device drivers is a mere security risk. |
| [18] | CERTs and ENISA<br>by uzurutuza on June 6, 2012 at 5:00 p.m.<br>Public and Private CERTs, ENISA and European Cybercrime Centre should play an important role on information sharing between actors. But I think there is a need of one only coordination point between all actors in Europe, strengthening visibility (for actors and both citizens) and coordinating such a distributed number of actors.<br><br>tags: coordination |

| | |
|---|---|
| [19] | CERTs and ENISA<br>by uzurutuza on June 6, 2012 at 5:00 p.m.<br>Public and Private CERTs, ENISA and European Cybercrime Centre should play an important role on information sharing between actors. But I think there is a need of one only coordination point between all actors in Europe, strengthening visibility (for actors and both citizens) and coordinating such a distributed number of actors.<br><br>tags: coordination |
| [20] | certainly not<br>by osimod on May 31, 2012 at 10:14 p.m.<br>we do not realize even the more basic risks. we're still at an age where few make a back-up, and technology evolves so quickly. |
| [21] | certainly not<br>by osimod on May 31, 2012 at 10:14 p.m.<br>we do not realize even the more basic risks. we're still at an age where few make a back-up, and technology evolves so quickly. |
| [22] | awareness<br>by uzurutuza on June 7, 2012 at 9:03 a.m.<br>I think citizen awareness has risen when it comes on viruses, spam, and noise threats. But with the increase of social network usage, awareness of citizens' data privacy needs to be enforced. Everyday I see people sharing personal information without even thinking on their possible future consequences. Also, note that usage of eServices using digital signature based cards are not fulfilling my expectations. I guess regulation is needed here.<br><br>tags: privacy digital signature |
| [23] | industrial companies<br>by uzurutuza on June 7, 2012 at 9:08 a.m.<br>We are on the way, but most industrial companies are still far away from appropriate level of awareness. This business need to create products, and security comes to a second place. Only attacks like "stuxnet" worm made a number of industrial businesses to start looking at security. Should we wait for more attacks in order to move forward?<br><br>tags: industrial companies |

| | |
|---|---|
| [24] | not quite<br>by Fishman on June 1, 2012 at 9:07 a.m.<br>From my experience from 7 years working in public, government institution, appears that IT security is treated rather like something that has to be, but is not treated seriousely. Underpayment for stuff dealing and responsible for IT security infrastructure leads to stagnation, lack of will to make something better and finally stuff migration to better payed positions in commercial companys. Only the most visible things are done, and only just so so that they work. So my guess is that avareness in the government sector is bery low, and something is done only when something bad is happening. Then starts a hunt for a guilty among IT stuff, but not among people who with they decisions, leaded to it. |
| [25] | locally organized trainings<br>by Fishman on June 1, 2012 at 9:31 a.m.<br>In my opinion, groups that are most exposured to cyber threats are children and elders. Children, becouse in most cases they use computer for fun and doesn't realize risk that can lie behind it. Also becouse they are so trastfull that doesn't think that someone can do something bad to them this way. The other group, elders, and by that term I mean people who are more or less over 45-50, they are a group that was an observers of computer revolution in modern world in 90's but mostly doesn't took part in it. They are afraid of technology, and even if thay are encouraged by they children to use computer on daily basis, they doesnt realize the threat, not they understand the source of it. In this point this two groups are comparable. My idea is that locally organized trainings (that would be part of country wide programm) recommended by people who are some kind of public trust persons, aimed at specific subjects as home computer/laptop security, security during traveling, recognizing and dealing with spam (especially phishing), and many other could be arranged to give people chance to gain needed knowledge, and brake the bareer of fear of unknown. |
| (25.1) | Re: locally organized trainings<br>by kvanhoever on June 3, 2012 at 9:18 a.m. |

| | |
|---|---|
| | I agree with the previous comment and would like to elaborate a little. Based on recent study (not yet published) indeed the group of 15-24 are most vulnerable for risks. The study did not cover younger then 15, but from experiences with those youngsters we know, there is low or no awareness of the possible threats. The channels mentioned in this document are too high level and aimed at ICT-literate people. Channels should be down-to-earth and should start as soon as possible: in school! To be set up in all schools, throughout the total eduction path starting with children of 6 years, because, yes, they to are roaming around on internet not aware of what consequences some of their actions on the iPad of mam and dad have; or the smartphone, or the iPod.<br><br>tags: channels |
| [26] | White hat<br>by Marten on June 6, 2012 at 5:26 p.m.<br>Work togehter with the white hat hacker community and blame and shame companies which do not fix exploitable vulnerabilities. |
| [27] | It secueritx<br>by Marten on June 6, 2012 at 5:43 p.m.<br>It Security is mostly about objective vulnerabilities of systems, not education for users. Must be poke-yoke. |
| [28] | marketing<br>by uzurutuza on June 7, 2012 at 9:10 a.m.<br>The use of marketing channels, online and traditional media is fundamental.<br><br>tags: marketing |
| [29] | Scientific coordinator<br>by pmassonet on June 1, 2012 at 2:23 p.m.<br>Simulations are a great first step to improve coordination between different European countries. But the long term goal should be testing and monitoring of internet security at a European level. |
| [30] | Cyber Games - the new Chess<br>by ahartman on June 3, 2012 at 1:52 p.m.<br>I am a great advocate of increasing the visibility and popularity of competitions to expose cyber weaknesses and privacy and security loopholes. There should be an effort |

| | |
|---|---|
| | to make hacking competitions a more universal sport, with formal competitions, rules and prizes rather like chess championships or some of the other sports-like events (e.g. the Math Olympiad) |
| (30.1) | Re: Cyber Games - the new Chess<br>by uzurutuza on June 7, 2012 at 9:20 a.m.<br>There are already some international competition in these topics: OWASP secure coding competition, Defcon is a worldwide computer hacker convention were Capture The Flag competition takes place, etc. What we need is to make it sound and use the results of these competitions to improve knowledge and awareness.<br><br>tags: competitions |
| [31] | Source code<br>by Marten on June 6, 2012 at 5:36 p.m.<br>Without the ability to review source code there is nothing but reliance on the software vendors. Security bugs have to be fixed as fast as possible, the earlier they are found, the better for the future. The EU should legally mandate disclosure of software code for critical components of the online infrastructure like Web browsers, widely deployed plugins, network stacks, web servers etc. and invest in source code review and analysis, also automated penetration and review tools, and coding styles for safer networks. |
| [32] | evidence<br>by Marten on June 6, 2012 at 5:43 p.m.<br>Needs evidence. |
| [33] | real world<br>by PeterSchein on June 8, 2012 at 11:33 a.m.<br>this happens in the real world, online only makes it easier to track it down. |
| [34] | Reporting<br>by PeterSchein on June 8, 2012 at 11:32 a.m.<br>Reporting of online crimes is still cumbersome. so there would be a large darf figure and better reporting leads to more cases. |
| [35] | Scientific Officer<br>by pmassonet on June 6, 2012 at 10:35 a.m.<br>We should also mention cyber warfare and |

| | |
|---|---|
| | state sponsored attacks such as the recent Stuxnet and Flame attacks on the Iranian nuclear research infrastructure (see http://www.telegraph.co.uk/technology/news/9305704/Barack-Obama-ordered-Stuxnet-cyber-attack-on-Iran.html#) |
| (35.1) | Re: Scientific Officer<br>by uzurutuza on June 7, 2012 at 9:34 a.m.<br>I agree with the previous comment. Stuxnet and Duqu were serious attack, and very advanced cyber-weapons targeting very specific computer systems (Siemens PLC controller software). The recently discovered Flame modular malware was already running 5 years ago! It uses the most advanced techniques for distribution, it used valid Microsoft certificates so computers trust in it, and very targeted attack for spionage. It is worth mentioning.<br><br>tags: stuxnet duqu flame |
| (35.1.1) | Re: Re: Scientific Officer<br>by pmassonet on June 11, 2012 at 9:51 a.m.<br>Another interesting reference on possible state sponsored cyber attacks. India is authorizing state sponsored attacks to protect it's critical infrastructures: http://www.theregister.co.uk/2012/06/11/india_state_sponsored_attacks/ |
| [36] | suffered an attack<br>by Marten on June 6, 2012 at 5:23 p.m.<br>The point was that they were insecure and vulnerable. You cannot blame that on the attacker who merely uncovered the fact. |
| [37] | Silly<br>by Marten on June 6, 2012 at 5:28 p.m.<br>This was just a silly dos attack, that doesn't count. |
| [38] | Not only Critical Infrastructures<br>by uzurutuza on June 7, 2012 at 9:40 a.m.<br>All kind of embedded systems are being connected, and this will have a big impact. House appliances, cars, trains, smart cities, health monitoring devices, etc. very soon. The potential damage of someone controlling our washing machines, someone able of changing our car direction, health damage, and so on is also worth mentioning.<br><br>tags: embeddded systems |

| | |
|---|---|
| [39] | Not only Critical Infrastructures<br>by uzurutuza on June 7, 2012 at 9:40 a.m.<br>All kind of embedded systems are being connected, and this will have a big impact. House appliances, cars, trains, smart cities, health monitoring devices, etc. very soon. The potential damage of someone controlling our washing machines, someone able of changing our car direction, health damage, and so on is also worth mentioning.<br><br>tags: embeddded systems |
| [40] | Not only Critical Infrastructures<br>by uzurutuza on June 7, 2012 at 9:40 a.m.<br>All kind of embedded systems are being connected, and this will have a big impact. House appliances, cars, trains, smart cities, health monitoring devices, etc. very soon. The potential damage of someone controlling our washing machines, someone able of changing our car direction, health damage, and so on is also worth mentioning.<br><br>tags: embeddded systems |
| [41] | unpredictable<br>by Marten on June 6, 2012 at 5:30 p.m.<br>Well, that means the security officials do not act very professional in their risk assessmentn and protection. Even in the case of Japan the problem was insufficient costal protection in a culture that suffered Tsunami througout his history. |
| [42] | Calculation scheme<br>by Marten on June 6, 2012 at 5:45 p.m.<br>Where do the figures stem from? What are the models? Appeal to autority is a fallacy. |