BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Post Bits of Freedom
Postbus 10746
1001 ES Amsterdam

Bank 55 47 06 512
KvK 34 12 12 86

M +31(0)646282693
E simone.halink@bof.nl
W https://www.bof.nl

European Commission
Per email: CNECT-H4@ec.europa.eu

Subject
Public Consultation Improving Network and Information Security (NIS) in Europe

Amsterdam
11 October 2012

Dear Sir, Madam,

Bits of Freedom welcomes the opportunity to provide input to the Public Consultation on Improving Network and Information Security (NIS) in Europe. We submitted our answers to the online questionnaire but would like to provide you with additional comments in this letter.

Improving cybersecurity in Europe

Stuxnet and Diginotar are examples of serious information security incidents that shook up Europe over the last couple of years. As Europe and its Member States become more and more dependent on information and communications technology (ICT) systems, they become more vulnerable to attacks on such systems. Cybersecurity therefore rightfully is high on the European political agenda.

However, if we focus too much on incidents such as these, cybersecurity policy will be the result of emotional reactions: we jump from incident to incident, not taking the time to devise structural solutions. Meanwhile, internet freedom is at risk, for example by considering extensive monitoring of internet traffic, and we run the risk of undermining the most important infrastructure of the 21st century: the internet.

Bits of Freedom believes that Europe deserves better cybersecurity. We are also convinced that smart and focused measures can significantly improve our cybersecurity. We explain this below.

Basic principles of European cybersecurity policy

a. Cybersecurity is personal security. Cybersecurity policy often focuses on the protection of vital infrastructures, like power plants and water facilities. But cybersecurity also concerns another important topic: the protection of civilians and their most valuable and intimate information. It would be a disaster if the sensitive and valuable data of millions of Europeans (such as communications, medical and location data) would be inadvertently exposed.

b. Cybersecurity must respect fundamental rights. Cybersecurity measures that are regularly suggested often affect our fundamental rights. For example, an 'internet kill switch' would limit the fundamental right to communication freedom. Mass surveillance of internet traffic severely limits our privacy. Such measures are therefore unacceptable: the European Court of Human Rights ruled on different occasions that the very essence of fundamental rights may not be impaired. As a consequence, the necessity, proportionality, subsidiarity and effectiveness of new cybersecurity measures must always be demonstrated beforehand. This means that such measures must be tailored to the issue they attempt to solve.

c. Cybersecurity requires transparency. Cybersecurity policy can have far reaching societal consequences for, amongst others, fundamental rights and the functioning of the internet. For that very reason, public oversight of cybersecurity policy is a necessity and transparency in this field is mandatory. Policy must be based on real and verifiable threat and risk analyses (both before implementation of the policy and periodically thereafter) and must be focused on the specific risk it attempts to address.

d. Absolute cybersecurity does not exist. Even though cybersecurity is an important policy goal, absolute security does not exist. Security in general is by definition the result of a cost-benefit analysis. In the field of cybersecurity, this analysis is informed by the fact that a small group of people with relatively little money can already cause immense damage, for example by developing advanced malware like Stuxnet. Of course, risks can be prevented as much as possible by providing basic security measures, by spreading risks as much as possible, and by providing fall-back mechanisms. Nonetheless, we must accept that even then, certain cybersecurity risks cannot be excluded, as the costs of prevention are simply too high (both in euros and the impact that preventative measures would have on our fundamental freedoms).

Eight measures for modern cybersecurity policy

1. Cybersecurity policy must focus on personal security. Over the last couple of years European and national legislation increasingly require the central storage of sensitive data of millions of Europeans (such as fingerprints, car license numbers, telephone and email-traffic data and location data). The access restrictions to this kind of data are often insufficient, as is illustrated by the situation in the Netherlands, where data of telecommunications subscribers is easily accessible to law enforcement officers and requested almost three million times a year. This must change: principles like data minimization and decentralization can prevent data breaches, simply because there is no or insufficient data to be compromised. Governments must therefore also store less data: the necessity of storage and the purpose thereof must always be proven beforehand. Moreover, data must be destroyed when storage is no longer necessary. Governments must further limit the access to data as much as possible and implement security by design and privacy by design principles in their IT-systems. In order to limit vulnerabilities, governments must ensure a healthy diversity in IT-systems when buying products and services. The principles mentioned in this paragraph equally apply to the private sector: the storage of-, and access to private data by such companies must be restricted and the security of systems must be higher.

2. Cybersecurity requires investment in knowledge and capacity, not in new authorities. Responses to cyberincidents are often inadequate due to lack of knowledge and capacity. Europe and its Member States must therefore invest in extra people with relevant expertise and the training of current staff. For example, governments must attract more staff with a technical background and ensure that law enforcement officers are trained in digital investigation methods. Investments in relevant education and scientific research are also necessary to ensure that knowledge of cybersecurity can be further developed and safeguarded in the future.

3. Internet users must be able to protect themselves. Europe and its Member States must ensure that internet users (including many organizations in the public and private sector) can protect themselves against cyber threats. The tools and support that are currently available to internet users is often insufficient. Meanwhile, many incidents are caused by basic vulnerabilities that can be prevented by taking basic security measures, like regular software-updates. Cybersecurity therefore begins with education on such measures, the promotion of usage of cybersecurity technology, like encryption software and anonymisation technology, and the development of secure software. This means that Europe and its Member States may not require backdoors in encryption technology and must not support the development thereof.

4. Europe and its Member States must give the right example. Lack of control or large dependence on third parties in information management creates a considerable security risk and undermines the credibility of cybersecurity policy. Europe and its Member States therefore need additional knowledge and capacity in the area of ICT, so that they can control their own infrastructures and can better estimate the consequences and risks of envisaged policies.

5. Outsourcing cybersecurity must be the exception. Europe and its Member States have the important role to ensure a safe and secure information society. Ensuring this remains at the core of their task. Precisely because of the large societal interests at stake, governments must be reluctant to support self regulation and public-private partnerships. This means that Europe and its Member States can only invoke the assistance of private parties in the field of cybersecurity if (i) they demonstrate the necessity thereof beforehand, (ii) formulate the conditions for cooperation, (iii) are fully transparent about this cooperation, and (iv) - where fundamental rights are concerned – guarantee parliamentary control.

6. The exchange of incident information must be stimulated. Public and private organizations are for their safety partly dependent on the information they receive from others: they can better secure their information systems on the basis of information on known threats and vulnerabilities. Europe and its Member States must promote the exchange of such information, for example via platforms for the exchange of vulnerabilities, attack patterns and infected IP-addresses. Where possible, such information must be publicly shared. Such systems must have built in safeguards that prevent the exchange of personal data, the abuse of this information and errors in the exchanged information. Europe and its Member States must also ensure that knowledge on vulnerabilities in information technologies are publicized as soon as possible. Finally, they must promote reporting of vulnerabilities through drafting guidelines for responsible disclosure.

7. Data and security breaches must be notified. Data and security breaches lead to identity fraud and loss of trust in information technology. Europe, its Member States and private parties must therefore be legally required to report unauthorized access to personal data to stakeholders. A public register for data and security breaches must enable public and private parties to learn from past mistakes and create insight in current threats.

8. Supervisory authorities must be able to act effectively. European data protection authorities monitor the protection of personal data. Other supervisory authorities, like the Dutch National Cyber Security Centre (NCSC), focus on increasing resilience in the digital domain. These authorities must be able to determine whether a particular cyberincident forms a significant risk for our information security and must, if necessary, be able to respond in an expedient and effective

manner. That means that these authorities must have sufficient budget and powers. In addition, (international) cooperation between supervisory authorities must be promoted.

About Bits of Freedom

Bits of Freedom is a Dutch digital rights organization, focusing on privacy and communication freedom in the digital age. We fight for an internet that is open to everyone, where everyone can continue sharing information, where private communication remains private and where lawful information remains accessible. We combine a broad range of legal and technical experience, a constructive lobby where possible, and sharp action where necessary. Bits of Freedom is based in Amsterdam, the Netherlands. We are active both on the national and European level and are one of the founders and a member of European Digital Rights initiative (EDRi).

We trust to have informed you sufficiently. Please do not hesitate to contact me should you wish to discuss the content of this contribution in more detail.

Yours sincerely,

Simone Halink

Bits of Freedom