Response to European Commission Consultation on the EU Internal Security Strategy

1. Introduction

European Digital Rights (EDRi) considers a coherent strategy on Europe's internal security to be very important. However, we believe that there is substantial room for improvement on the efforts of the European Union to create a policy to protect the (digital) rights of its citizens and inhabitants. We therefore welcome the opportunity to contribute to this consultation, to improve the vision of what such a policy must include.

In this response, we will describe issues that need to be addressed, including possible solutions. This contribution focuses mainly on topics concerning IT security and so-called cybercrime. A sound security strategy must address the digital policy of the European Union. Security of infrastructure and the safety of a citizen are intertwined as are the security of infrastructure and the digital rights of the citizen.

We will mainly address the challenge of improving the IT security culture, the challenges regarding assessments of risks to our digital security and finally we recommend actions in order to fix the problems we address.

2. The culture of insecurity

The proper functioning of technical infrastructure is vital for a modern information society. The simple truth is that the technical infrastructure our society relies on is very insecure. This has many reasons for t his, but two of the most important are the culture of IT (in)security fostered by a lack of accountability and the fact that the technology was not built with current applications in mind, let alone with the failures human beings are prone to. These problems need to be recognised and addressed, if we are going to be serious about our security.

2.1. Addressing technical insecurities

A sound internal security strategy of the European Union is not complete without a proper approach to the risks to IT security, as technical infrastructure is the foundation of our communication, economics and politics – and its importance will continue to increase as the digitalisation of the everyday life progresses.

If the security of private organisations and the public sector has loopholes and a breach of systems occur, the privacy and digital rights as well as the functioning of communication infrastructure and businesses are at stake. We also need to understand that the addition of prefix ´cyber´ tends to confuse more than it adds in precision. It definitely should not mean that common sense can be cast aside or normal policy-making processes can be ignored. Many principles from the "real world" also apply to technical environments. The current reality of handling technical insecurities often lacks transparancy and there are currently no incentives for organisations[1] to care about these issues beside the internal risks generated by a possible breakdown of their own operations. Even these risks are often underestimated. This inward-looking approach fails to recognise that IT risks are not only present for the infrastructure of organisations themselves but also impose a negative externality on third parties. When we combine with the fact that IT infrastructures are dominated by monocultures in terms of the technology used, we find ourselves in a situation where current practices pose a systemic risk to security the European Union. The longer it takes for EU policies and regulatory environment to recognise this problem, the more difficult and more expensive it gets to resolve it. The baseline is that weak spots in security must be identified and fixed and the information about this must be shared with the public in order to allow mitigating measures to be taken.

The way in which the so-called "Heartbleed Bug" was addressed is a good example of the way incidents that affect essential IT infrastructure can be addressed. Open discussion, availability of patches and the use of monitoring and testing tools made it possible to handle the incident in the right manner. It also showed that further work is needed to address our dependency on some critical open source projects.

If, for example, the brakes of a car malfunction in normal conditions, the manufacturer of the car may be held liable. There is the need to follow the same logic when addressing malfunctions in IT infrastructure and services. There is a strong need to strenghten capacity to identify and solve IT security issues, especially if the source code of the software is not openly available but depends on the policy of the publisher.

For these reasons, the security of technical infrastructure and all technical products such as hard- and software must be of the highest priority. There needs to be a proper assessment of technical risks and a proper response to breaches and disaster recovery.

2.2. Human rights by design

Several laws and current proposals regarding technology and law enforcement neglect the digital rights of individuals, to the detriment of overall security. One of the main reasons for this is that almost all technology that is currently used was not designed with human rights principles in mind. This presents majorg challenges when it comes to developing and enforcingmeaningful regulation. A striking example was obviously the Data Retention Directive - legislation developed without an evidence base, implement to solve unspecified problems in a manner which undermined the fundamental rights of European inhabitants and those who communicated with them. The European Union should take the lead and

[1] An organisation in this document means both the private and public sector, as well as companies, government bodies, producers and processors of data.

create a policy based on effectiveness, proportinality and the rule of law.

3. Assessing technical risks

Prevention is always better than a cure. In the field of IT infrastructure, this means that development of products must also incorporate the principles of "security by design" and "defence in depth". These principles must apply to the way organisations approach their digital infrastructure as a whole. Organisations need to use a proper IT risk assessment and act on the basis of such analyses in order to reduce those risks.

3.1. Risk assessment done right

Risk assessment is often done with only the internal operations of organisations in mind. Many companies don't grasp the idea that IT is part of their core business and needs to be treated with an appopriate degree of priority. Procedures often only cover measures such as backups in case of technical errors and data loss, but a proper risk assessment also includes risks for third parties. This does not, however, include the risk for privacy of customers because risks for human rights can't easily be assessed the same way own operational risk can be assessed. This is because the operating authority cannot know about the individual privacy contexts of its users and is likely to fail if it tries to assess these and base policy on such an assessment. It must be assumed that a technical risk implies a risk for violating human rights as soon as personal data is at stake.

However, a reasonable assessment includes threats that are present which would permit attackers to misuse systems by launching attacks against others (i.e. denial of service, data breaches etc.).

Proper risk management also needs to access the risks that are present coming from third parties, because organisations need to assume that errors also occur in the systems and equipment that they rely on. Without an assessment of such risks, an organisation is not easily able to respond in the right manner in order to protect itself and its customers or users. Proper risk assessments reduce the attack surface of organisations in a quantifiable fashion.

There are many benefits for a proper risk assessment, not only for the operating authorities but also for the information society as a whole. It is therefore crucial to stimulate organisations to invest in a high level of technical security. One of the most basic goals is to find incentives for companies to undertake proper risk assessments. At the moment the only motivating factor is the need to avoid bad publicity and this is clearly inadequate.

4. Actions

There is the need to clarify the definition of the terms 'event' and 'incident' in IT security-related context. If there is confusion about what precisely an event or incident is and whether these should get notified, it can slow down the progress of resolving the issue and mitigating the damage. It is therefore essential to develop a clear and commonly-held understanding of what should be reported. This is also of importance because events or incidents for one company might not necessarily generate the same problems for another company; that depends on their business and whether it can lead to compromised systems, either their own or those belonging to third parties. There is a problem if the responsibility of an event/incident handler or the management is to make a decision on whether a particular event or incident needs to be reported. The consequence of this is that there will be a tendency to under-report, in order to avoid any potential liability or negative publicity.

4.1. Actions for organisations

4.1.1. Data minimisation

Gathering of personal data can be very valuable for companies, but companies need to address whether the gathering of data has any legitimate need for operations of the organisation. The absence of such an assessment creates an unnecessary risk for leakage of personal data – data which should never should have been stored in the first place. Even when this data is collected with informed consent and processed in full respect with the needs for operations of the organisations, the data can be stored beyond the necessary period. This too generates unnecessary risks for the leakage of personal data – one of which the individuals concerned have not been informed, to which they have not consented and which generates no benefit for them.

There are currently no incentives for companies to apply the principle of data minimisation, beyond unevenly implemented data protection legislation. But the more personal data an organisation gathers and stores, the higher the risk and the damage for the persons whose information is leaked in case of incidents.

Considering this, data-minimisation should be actively stimulated by the European Union. One way to achieve this would be a stronger position of the Article 29 Working Party on data minimisation. When a DPA investigates a (personal) data leak, the principle of data-minimisation should be a separate factor of the investigation and to be taken into account in order to establish whether the organisation has acted illegally or recklessly. Another way could be to stimulate transparency with regard to how and which data is collected. This could be by promoting the ´best practice´ of publishing precisely which and how data is collected, e.g. that GPS coordinates are checked every five seconds, or the calendar is checked every month. It should be possible for the customer to disable any data collection if it is not essential for the main purpose of the application

4.1.2. Dealing with breaches

Organisations need to properly address any breach of their IT infrastructure. First of all, they need to notify their users and other relevant stakeholders. In order to increase the incentives to do so, the consequences of not reporting incidents need to be increased. A leak of personal data can be of great significance for an individual and may generate a greater risk of further leaks, e.g. in the case of password or other information leaks that might lead to accounts being compromised. An immediate notification to the users of the system is of paramount importance, as it allows users to take appropriate action to prevent further damage. Also, if a breach of the system occurs, without leakage of personal data, a notification might nonetheless be of vital importance to other organisations and their security, especially if the leakage is caused by widely used software components. A significant amount of unnecessary damage can be prevented if the public is to be alerted to incidents in time. It is crucial to increase the consequences for not reporting leaks and incidents, not least because the responsible party will be more motivated to invest in a robust system, as a means of having adequate protection, thereby avoiding problems that need to be reported. In the long run, organisations will also be motivated to report leaks as showing the effectiveness of its countermeasures, thereby minimising possible liability. The incentive to increase the willingness to report can be increased by ´naming and shaming´ and by increasing the accountability of the organisation where the leak has occurred. To increase the consequence of not reporting an incident, a ´black list´ could be introduced. This list will be used to register to companies that have failed to reported leaks (in time). This will obviously create damage to the reputation of companies which do not follow the mandatory duty to report leaks. There's also the need to distinguish between the user who uses a system an

d the customer whose data gets collected. The user of a system may not be impacted by a data leakage, but the customer is. The customer should get informed since his data is involved in leak and could be available in the wild. Organisations should encourage users to report a possible breach of the system. Therefore, the European Union should take the following measures:

1. Make sure that every organisation offers users of their system(s) an easy way to contact them, e.g. via e-mail – to report incidents.

2. The work of IT security researchers should be stimulated, promoted and protected. Their work can be helpful in finding vulnerabilities in a system.

3. Knowledge of social engineering needs to be shared in a broader way, so people can be alerted in time to prevent damage from such tactics.

4. Create incentives to make exploits and discussions about vulnerabilities public. In this way, IT security will be increased, as known vulnerabilities can be patched while unknown or hidden vulnerabilities can not.

4.1.3. Disaster recovery measures

Even when all necessary actions are taken, disasters are not entirely avoidable. The main reason for this is that IT is complex and interconnected, both inside and outside of organisations. In order to be able to respond quickly, measures need to be in place to recover quickly.

> A good example of this is the case of Hetzner, a German hosting provider. The company had a data breach and notified their users within 24 hours, before subsequently informing the general public. Hetzner had processes in place to identify and recover from disaster very quickly and drastically lowered the risks for a large number of their customers.

Disaster recovery includes, for example, regular backups, ways of finding out what actually happened by assuring easy implmentation of forensic analysis, notification of users to change passwords and procedures to fix technical issues. Such an approach is beneficial for all stakeholders, as it elevates trust in services, because there it will be demonstrable that good safeguards were implemented in the aftermath of an incident. Rules for disaster recovery procedures for IT companies are not only in the best interest of customers and their data but also for Europe as a market for trustworthy services, which results in more capital for meaningful general protection measures.

4.1.4. Increasing accountability

In order to create an incentive for organisations to create adequate safeguards, accountability needs to be increased. The situation sometimes arises where the individual responsible for the security of the system does not recognise the damage but the people are aware of it. For example: if leaks in patient-register systems occur, only the patients might recognize the problem, because the personal information of patients becomes available to attackers.

It is especially crucial to increase the accountability if the soft- or hardware is closed-source. If it is closed-source, proper accountability is vital for the user to gain more confidence in the service or equipment and to get the right protection. A consumer cannot alter the software if it is flawed, so s/he is obliged to depend on the willingness of the vendor to address the problem. It is a risk which the customer cannot minimise. In open source soft- or hardware, it is not only the vendor, but also a third parties or the customer him- or herself that can fix problems, so liability rules ca not and should not actually apply to open source in the same way.

One way to get better accountability is to increase the liability for the manufacturer of the soft- and hardware. It starts simply with the obligation to provide the possibility to contact a responsible security officer of an organisation and it the obligation to respond to an incident within a certain period of time. In case of out-sourcing of IT-security, this should not limit the accountability of the organisation that has out-sourced its activities. Also, when the life cycle of a product ends, there should be a reasonable timespan for consumers to adapt their technological infrastructure.

On the other hand there must be a liability for users to update their software regularly in order to have the right to take legal actions against vendors which don't follow the rules. For example: if an airline using Windows XP after the life circle has ended, they should be held fully responsible for incidents due to their extended use of an insecure IT infrastructure.

4.1.5. Dealing with high risk data

Biometric, genetic and health data in general is the most sensitive data as it can't be altered as easily as other personal data. At the moment, this type of data is often being processed the same way as other similar personal data. There is a great danger that protection of biometric and genetic data will be not be commensurate with its high level of sensitivity.

Once this data is generated and collected, it creates a high risks for all people affected by it. These risks in include:

- The re-personalisation of data that was partially anonymised (as full anonymisation is virtually impossible).
- That the data could also be used for other purposes in the future which can lead to an tremendous disadvantage for people affected by breaches. For example, breaches might make it easy for example to put fake evidence in real life crime scenes.

There is also a strong need for research regarding the protection of genetic, biometric and health data. As processing this data can't be avoided completely, there should be specific legislation regulating its processing, enabling the implementation of a higher level of security. For example, biometric data should be treated as the most sensitive personal data, instead of ´normal´ personal data. There is a need to have strong safeguards to prevent any kind of extended use, misuse or abuse of this data. Another way could be to have high fines in case of breaches or leakage of this type of data, to punish companies who fail to put in place adequate security procedures.

Cross-border flow of this data should be discouraged or prohibited.

4.2. Actions for governments and on EU level

Human rights infringing regulation needs to be proportionate and necessary. The mere fact that new technology has provided us with almost limitless opportunities to spy on civilians, monitor their behaviour and control their access to knowledge do not justify the use of technology to do so. In other words: The existence of a technology does not constitute the need for its use.

4.2.1. Fact-driven policies only

There is no such thing as absolute security or safety. It is important to accept this fact.

Policies should not be based on the assumption that a ´success-rate´ of absolute safety can be achieved. There is a need for policies based on facts, rather than on fear, uncertainty and doubt. Unfortunately, this is exactly the basis for much European policy and legislation.

For example, Europol issued a report on the ´criminalisation´ of the Internet and focusing especially on the use of encryption by criminals. The increased use of encryption on the Internet by criminals is idenified as a risk. However, the report fails to point out that this encryption also keeps innocent individuals safe from the criminals in question.

Another example is the report on the ´use of the Internet for terrorism purposes´ by the United Nations Office on Drugs and Crime. In this report, the UN suggested the storage of communications data of innocent individuals, in the absence of any evidence of effectiveness or proportionality.

Both reports point in the same direction: creating fear and suggesting the implementation of draconian ´safety´ measures, such as the Data Retention Directive, without evidence for the necessity, effectiveness or proportionality of these measures.

Any proposal that risks undermining human rights should at least be based on facts and on the legal obligation for such measures to be necessary and proportionate. This will contribute to the democratic process, as both legislators and the public can discuss such a proposal for its merits rather than fear.

4.2.2. Effective legislation

A proposal constituting human rights infringing measures needs to be necessary, effective and proportionate in solving the issues the proposal aims to solve. This means that both the existence of the problem and the effectiveness of the proposed measure needs to be addressed. We do not need focus on incidents when creating policy, because this does not necessarily create proportionate policy. Instead, policy based on facts requires proper research and defining of the ´real´ problems at hand. The fact that the legislation or countermeasure has a legitimate aim, does not mean that it is necessary or proportionate

There are – at least – two current definitions of cybercrime and when creating policy. We need to be clear about whether we are talking about the use of the internet as a means to a commit a criminal act or if we are talking targeting the internet or the infrastructure itself.

One of the ways of generating effective legislation might be to harmonise certain regulations; but only if it leads to a race to the top. Considerations about legislation should also take into account that the internet is truly global space. Efforts to improve security in the EU should not lead to, and should not promote, a European Wide Web or European intranet, even if that network would be more secure than the current global internet.

4.2.3. Dealing with NIS

An example of the need for effective legislation is the proposed Network and Information

Security Directive (NIS Directive). The proposed NIS directive is flawed, as it is too narrow to improve the general level of IT security. With all due respect of the value of the stated goals of the Directive, it will fail. In order to repair the flaws of the NIS directive proposals, there should be a revision into a "NIS4ALL Directive" in which the following three points below are covered.

- Organisations in the public sector seem not to have to comply with the NIS Directive. This is strange, especially if considered that organisations in the public sector should give a good example in maintaining high levels of security. Forcing organisations in the public sector to comply with the NIS Directive will increase the general level of the security of IT infrastructure.
- Producers, such as app-designers or technology providers can – basically – disregard the NIS Directive. The producers of soft- and hardware used for the processing of data enjoy have a responsibility for the security of their produced equipment / software. They should also comply with the NIS Directive.
- Small business are excluded from the NIS-directive. This is remarkable, as there are a lot of critical small organisations that need to be included into the directive and have a certain liabilities as well. The size of the company should be of no importance when assessing risk, responsibility and liability.

4.2.4. Create better oversight

The EU should take measures to ensure an expedient and effective oversight on the security of IT infrastructure. There is a need to invest in the knowledge and capacity of the oversight bodies. Data protection authorities (DPAs) and sectoral regulators should issue transparency reports on the number of leaks and data breaches, should frequently investigate whether organisations have a proper risk assessments and whether incidents occurred. They also need to cooperate with other regulators and provide assistance to organisations.

Oversight bodies should be civilian authorities subject to EU data protection laws. A couple of member states (for example, the United Kingdom and Denmark) have created IT security agencies which are part of the defence intelligence services, and hence (they claim, although this can be disputed) exempted from EU data protection laws[2].

Procedures for protection of IT systems and analysis of possible intrusions into IT systems may involve processing of personal data. It is important that personal data is only processed to the extent that it is strictly necessary and proportionate for the purpose of protecting IT systems and investigating intrusions. Personal data from log files and intrusion detection systems should be deleted or effecttively anonymised as soon as possible. Information sharing about adverse IT security events is an important aspect of protecting the general IT security infrastructure, but fundamental rights about data protection should always be

[2] http://edri.org/danish-government-plans-create-center-cybersecurity-privacy-invasive-powers/

respected. In particular, of information information containing personal data should be limited to what is absolutely strictly necessary and proportionate for handling the specific IT security event. Security must not be allowed to become a standard excuse for evading data protection laws.

4.2.4.1. A framework for cooperation between regulators

A central approach to incidents is not always appropriate, as many IT infrastructure problems are sector-specific. At the same time, these problems are often interconnected; as a leak in an operational system might also affects other sectors. Hence, there should be strong cooperation between sectoral regulators, DPAs and CERTS, in order to assess and address threats and incidents. Regulators need to have a good framework for cooperation, especially between national CERTs. In general CERTs should not be tied to Europol, military or national law enforcement agencies as these latter organisations do not have protecting civil IT infrastructure as their main objective. Furthermore, having this type of entity in critical civil processes undermines trust.

4.2.4.2. Regulators need to inform, provide and assist

Regulators need to offer easy ways to notify them of incidents. The process of notification should be as simple as possible and should be connected to existing procedures, insofar as this is feasible.

Regulators should issue best practice guidelines and be clear about the assistance they can offer in order to prevent incidents or for disaster recovery and what happens with the information the organisations share with regulators. The regulators should also have follow up procedures for after an incident. Even if other organisations are informed of an incident, there is no way to be sure that the organisations understand what they need to know and need to do, other than staying in contact with them.

In short, organisations need to be able to:

- beprovided with information about incident and the follow-up;
- be provided with information on how to get meaningful protection;
- have the possibility to speak to an independent expert or trusted government official.

4.3. Forbid LEAs to break into computers

Another example of how policy fails to achieve its goals lies in proposals regarding how to tackle computer crimes. There is no real territorial boundary on the internet. The lack of such a boundary is a risk, as law enforcement agencies are increasingly acting across national borders. One of the proposed measures is allowing law enforcement agencies to remotely break into computers. While this measure aims to improve the security of the IT infrastructure and the safety of the citizens, it will lead to the exact opposite result.

Several member-states have introduced the authority to hack into computers – even if the computers are located in the territory of another country. Several member-states are pushing for European regulation to create harmonisation on the field of the hacking of computers. It is easy – or should be - to see why the EU should restrain from encouraging this authority for law enforcement.

It does not solve the problem. It does not improve the security of the IT infrastructure, because LEAs have an incentive to profit from weak IT security, as they need insecurities in IT systems to catch the criminals who also profit from weak IT infrastructure. So instead of tackling the problem at the core (which is the insecurity of IT infrastructure), LEAs will tend to abuse the same vulnerabilities. It is also a disproportionate violation of privacy, as it allows LEAs to monitor citizens in every way possible. This paradox should be avoided.

Acting beyond the judicial competence of the member-state threatens the sovereignty of the other state. This should also be avoided. Cross-border crime in the European Union should be addressed by cooperation between member-states, e.g. by mutual legal assistance. If governments see a need to act for themselves because of failing assistance – e.g. due to lengthy procedures – the core issue should be tackled. One of the justifications put forward in 2005/2006 for the adoption of the failed Data Retention Directive was the slowness of mutual legal assistance procedures. It is absurd that, nearly ten years later, further disproportionate measures are being proposed, due to the same unsolved problem. The core issue is in this case obviously improving mutual legal assistance.

A special approach to crimes related to botnets also needs to be developed, to prevent unnecessary violations of the privacy.

To create an incentive to be effective and up to date, all human right infringing measures should have a sunset clause. This means that human rights infringing measures shall cease to exist after a certain period, unless legislators extend the law. This will force policymakers to evaluate and re-evaluate the necessity and effectiveness of these measures.

5. Conclusion

The future of Europe relies on the functioning and security of information technology in order to maintain political stability and economic growth. Currently, our strategies for dealing with technical vulnerabilities and errors has led to a culture that generates unnecessary risks and vulnerabilities. Some of these risks can be tackled by meaningful assessments and actions taken by organisations, such as dealing with breaches and disasters or increased liabilities and effective legislation such as stronger liabilities. But it's crucial that decisions are made on the basis of facts raher than on fear, uncertainty and doubt.

A strong internal security strategy is built from within organisations, building a culture of security by design and by default. This culture should be enhanced and supported by a coherent, security-enhancing legal framework of a standard that is far higher than we see in the proposed NIS Directive. The legal framework is also nothing without both the carrot of support and the stick of enforcement offered by technically, legally and administratively competent regulatory authorities.