KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

CDT COMMENTS ON THE PROPOSED DIRECTIVE CONCERNING MEASURES TO ENSURE A HIGH COMMON LEVEL OF NETWORK AND INFORMATION SECURITY ACROSS THE UNION

May 2013

The Center for Democracy & Technology ("CDT") is a non-governmental organization dedicated to keeping the Internet open, innovative and free. We have offices in Washington, D.C., Brussels, and San Francisco, California. CDT's extensive work on cybersecurity has focused on advocating measures that increase the security of Internet communications without compromising human rights or innovation. We submit these comments on the proposed European Commission's proposed directive on cyber security.

CDT agrees with the European Commission's motives for proposing EU legislation on cybersecurity – to ensure a high common level of network and information security (NIS). We support the objective of enhancing the level of cybersecurity cooperation and collaboration across the EU. Cybersecurity is clearly a matter that impacts the Single Market, and therefore EU-level action is warranted.

Issues and concerns

With the above in mind, CDT raises a number of issues regarding the proposed Directive, which we believe need to be addressed by the European Parliament, the Council of Ministers, and the Commission in their further deliberations on this important piece of legislation.

I. National competent authorities: ensuring civilian control and democratic oversight

Article 6 requires each Member State to designate a 'competent authority on the security of network and information systems.' Competent authorities are charged with monitoring the application of the Directive, receiving notifications of incidents, cooperating with other Member States' competent authorities, and other responsibilities. As drafted, the Directive leaves full flexibility for Member States to establish or designate the competent authority. CDT believes it would be well-advised to introduce a set of conditions stipulating that competent authorities must be under civilian control with full democratic oversight and transparency in their operations.[1] The vast majority of the networks and systems covered by the proposed Directive are civilian in nature or are owned and operated by the private sector. From a human rights perspective, it would be undesirable if Member States were to designate military or intelligence agencies as competent authorities.

[1] We note that the U.S. House of Representatives voted in April 2013 to reaffirm civilian leadership of cybersecurity programs affecting civilian government agencies and private sector networks and systems. The Administration and the Senate have likewise favored civilian control.

II. Data minimization: ensuring that only strictly relevant data are collected and processed for cyber security purposes

Information sharing is a major theme of the proposed Directive. Article 9 requires the creation of a secure information-sharing system. Article 10 requires the Commission, in a Union NIS cooperation plan, to define the format and procedures for the collection and sharing of information on risks and incidents. Article 10 also requires the competent authorities or the Commission to provide early warnings of risks and incidents. Article 14 requires covered entities to notify competent authorities of security incidents. .

The information to be shared under these and other provisions of the proposed Directive may contain personal data, raising concerns about minimization, retention, use and disclosure. This issue is addressed to some extent in Article 1, paras. 5 and 6. These provisions state that the proposed Directive shall be without prejudice to current data protection directive (the 1995 Directive) and future (the GDPR) Data Protection legislation. Despite this, CDT recommends that the cybersecurity Directive include a clear and unambiguous definition of the types of data that can be considered relevant for collection and processing for cybersecurity purposes, and clearly stated obligations on authorities to delete and dispose of such data once they are no longer required to manage cybersecurity risks and threats.

One solution to this problem would be to develop an Annex with an exhaustive list of the types of data that can and should be collected for cybersecurity purposes and, conversely, listing types of data that would normally not be considered relevant or would be considered relevant only in exceptional circumstances.

As currently drafted, we fear that authorities would be encouraged to collect, store and process excessive amounts of data, among them personal data, without sufficient safeguards against use of these data for purposes not related to cybersecurity risks and threats.

III. Range of market operators subject to the obligations of the Directive

In the same vein, CDT has concerns about the range of private sector companies ('market operators') covered by the Directive. Article 3, para. 8 (supplemented by Annex II) broadly defines market operators to include two distinct sets of entities: information society providers, and operators of critical infrastructure essential for maintenance of vital economic and societal activities. It should be noted that the lists provided in Annex II are specified as 'non-exhaustive', and we can thus expect the list to be expanded with additional types of companies in some Member States. This will most likely mean broader sourcing of more types and categories of data. Annex II currently includes: e-commerce operators, Internet payment gateways, social networks, search engines, cloud computing services, and application stores. Annex II also mentions transport, energy and infrastructure companies. The range of market operators encompassed in Article 3, para. 8 seems overly broad, and we would recommend that the list be narrowed, or alternatively that different market operators should be subject to different types of obligations, based on the importance of their activities to society at large.

IV. Obligations and incentives of market operators and public administrations

Article 14 imposes obligations on public administrations and market operators to notify competent authorities about security incidents (para. 2). Article 14, para. 4 authorizes competent authorities to publish incident information or require market operators and public authorities to publish incident information. An "incident" that must be reported is "any circumstance or event having an actual, adverse effect on security" (Article 3 para. 4) that has "a significant impact on the security of the core services" provided by a market operator or public administration (Article 14 para 2). The Article does not, however, seem to address sharing of information about cybersecurity threat information that may be tied to an incident or an attempt to cause an incident.

This raises the very important question of what information would be most valuable to report and share – incident information, threat information, or other categories of information? Threat information is not currently defined in the proposed directive. It consists of information that describes an attack that results in an incident or an attempt to cause an incident. Threat information includes cyber attack signatures. Market operators and public authorities might consider threat information more valuable than incident information because it can be used to prevent incidents, , whereas incident reporting would merely record attacks that have already occurred. The Directive should encourage Member States to incent, but not mandate, market operators and public administrations to share threat information.

It is debatable whether an incident reporting obligation combined with the possibility of publication of incidents would provide market operators with the right incentives. In addition, it must be recognized that reporting of either incidents or threat information may well involve disclosure of highly confidential and sensitive information. Market operators may well be concerned that such confidential information could end up in the wrong hands or could raise questions about liability for security incidents, resulting in litigation. Market operators would probably need guarantees and safeguards against unintended uses of their reported information.

A more precise and narrow drafting of Article 14 could address such concerns and provide the right incentives for market operators to share relevant information, under appropriately controlled conditions, about incidents, threats, and/or the current and future threat landscape.

While it is important to ensure that reporting of incidents and/or threat information is carefully defined and that information shared is properly protected, CDT has always favored notification to consumers when there is a breach of their personal data. While it is necessary to carefully define the circumstances under which notice must be given (to ensure that consumers are not unnecessarily notified), CDT believes that the experience in the U.S. has overall been highly positive under laws requiring notice to consumers when their personal data is lost, stolen or otherwise compromised. We note that issue is properly addressed in the proposed data protection regulation.

V. Standards and technology mandates

Article 16 of the Directive directs Member States to encourage the use of standards and/or specifications relevant to NIS. Given the global nature of information and communications networks and services, it is essential to ensure that any decisions and recommendations regarding technical standards and specifications refer to globally recognised and deployed technologies. In general, Member States and the Commission should avoid favoring certain standards over others, because it is doubtful whether competent authorities would be able to take decisions and make recommendations rapidly enough to match day-to-day developments in the cybersecurity threat landscape. Market operators and the companies developing and deploying security tools and software are probably better placed to make rapid decisions to counter cybersecurity risks.

For further information, contact

Jens-Henrik Jeppesen, Director for European Affairs, jjeppesen@cdt.org
Gregory T. Nojeim, Director of CDT's Project on Freedom, Security and Technology, gnojeim@cdt.org.