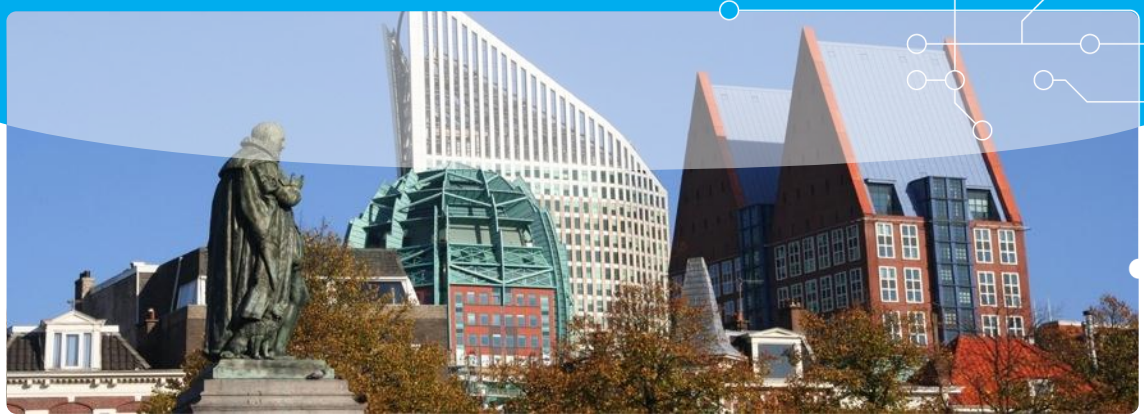

# European Cyber Security Strategy

On February, 7th 2013, the European Union presented its European Cyber Security Strategy and accompanying Directive. This factsheet summarises HSD's first reactions.

## Cooperation between public and private sectors

The EU requires both public authorities and the private sector to develop capabilities and to co-operate effectively in order to promote cyber resilience in the EU: "Since the large majority of network and information systems are privately owned and operated, improving engagement with the private sector to foster cyber security is crucial. The private sector should develop, at technical level, its own cyber resilience capacities and share best practices across sectors. The tools developed by industry to respond to incidents, identify causes and conduct forensic investigations should also benefit the public sector". One of the initiatives of the EU in this field is the launch of an EU-funded pilot project, early in 2013, on fighting botnets and malware. The pilot is meant to provide a framework for coordination and cooperation between EU Member States, private sector organisations such as Internet Service Providers and international partners.

HSD recognises the importance of public-private partnerships. As continuously growing network of businesses, governments and knowledge institutions in the security sector we join forces to realise innovative security solutions and economic development.

In addition, the EU asks the industry to take leadership in investing in a high level of cyber security and to develop best practices and information sharing at sector level and with public authorities.

The EU Cyber Security Strategy describes responsibilities for regulators, and national and local authorities as cyber user. HSD would like to see that (local) governments are not only pointed at their responsibilities, but that they, as heavy users of ICT, are provided with obligations.

We would like to see that governments and public authorities (are stimulated to) act as launching customer for innovative security solutions. That, in turn, will stimulate the private sector to invest in innovative technologies to develop new and more secure solutions.

The EU Cyber Security Strategy mentions public-private cooperation with respect to information sharing at the technical level. The strategy promotes also cross-border public-private cooperation in the field of CIIP (Critical Information Infrastructure Protection). It remains unclear, however, if the strategy only promotes technical cooperation (e.g., sector-specific CERTs), or that it also aims to foster public-private cooperation at tactical and operational levels (e.g., by Information Sharing and Analysis Centres).

## Awareness and education

An important part of the EU Cyber Security Strategy is about raising awareness: “Ensuring cyber security is a common responsibility. End users play a crucial role in ensuring the security of networks and information systems: they need to be made aware of the risks they face online and be empowered to take simple steps to guard against them”. Practically, the EU asks ENISA to propose in 2013 a roadmap for a voluntary certification program to promote enhanced skills and competence of ICT professionals (e.g. website administrators) and requests Member States to step up national efforts on network and information education and training.

The Hague Security Delta supports the need for raising awareness on cyber security. However, we feel that the proposed initiatives are not sufficient. Member States do have roadmaps to move to an international harmonised, and in the long run mandatory, certification program for ICT professionals. What is required is support by the EU for implementation of these roadmaps.

Other EU initiatives for raising awareness include the organisation, with the support of ENISA, of a cyber-security championship in 2014, where university students will compete in proposing NIS solutions. Moreover, the EU invites Member States to organise a yearly cyber security month, with the support of ENISA and the involvement of the private sector from 2013 onwards, with the goal to raise awareness among end users. A synchronised EU-US cyber security month will be organised starting in 2014.

In The Hague Security Delta, businesses, knowledge institutions and governments have an urgent and permanent need for more and better trained experts and graduates in cyber security.

Mainstream education in The Netherlands (and Europe) however, still offers (too) little training and research in the field of cyber security. Although there is a great demand for cyber specialists, there is also a need for experts at the strategic level and for employees who can make the connection between technology and business-related topics such as management, legislation, privacy and international relations.

The EU strategy does not pay a lot of attention to the design and promotion of cyber security education (both in width - conscious citizens in all age categories- and in depth - the technological, the risk and the organisational aspects). We also regret that there’s little attention in the strategy to step up for C-level awareness and C-level education. We feel that especially top management engagement with cyber security and risk management is of major importance.

**To satisfy the existing and future need for cyber security experts, The Hague Security Delta is taking the initiative to start a Cyber Security Academy: a communal place, a ‘campus’, where professionals, researchers and students meet for education, research and sharing expertise in the field of cyber security. Governments, businesses, educational and knowledge institutions are working together on the business case.**

## Proposed Directive

Together with the European Cyber Security Strategy, The European Commission has issued a proposal for a Directive on a common high level of Network and Information Security (NIS) across the Union, addressing national capabilities and preparedness, EU-level cooperation, take up of risk management practices, and information sharing on NIS.

According to The Hague Security Delta, the scope of the Directive (notably 'Network and Information Security') is too small.

The focus is on gathering information about incidents, without the support of a thorough risk management vision. Therefore it is likely that organisations are obliged to collect and share irrelevant information.

We regret that the scope of the Directive is limited to NIS, while the main problem lies in the awareness and risk management skills of top management and administrators.

Incident reporting actually distracts from a larger problem, namely the lack of risk management capabilities of top management in both the public as the private sector. As mentioned in the impact assessment of the EU: "..that users of information and systems are unaware of the existing NIS threats and incidents (82.8% of respondents) and that businesses, governments and consumers in the EU are not sufficiently aware of the behaviour to be adopted to minimise the impact of the NIS risks they face (84%)." Nevertheless, measures to address the lack of risk management capacity in the boardroom are not mentioned in the Directive. And the proposed incident-driven approach does not resolve this issue.

Moreover, we expect additional pressure on organisations by the mandatory reporting of incidents, without substantial proof that the proposed Directive will be effective in making the digital world a safer place.

The introduction of the draft Directive ignores the context in which various stakeholders (with varying risk profiles) are responsible for different parts of the NIS. A distinction between societal risk and business risks is also missing. In our opinion, it is not fair to ask companies to figure out themselves which societal risk they are supposed to manage. However, in many cases the government is not able to specify the risk. That makes it difficult or even impossible to manage, for both the government and the industry.

Given the increasing use and dependence on ICT, The Hague Security Delta thinks that the effect of the proposed Directive would be stronger if it is accompanied by policies for the development of business and social resilience in the event of ICT failure.

**In The Hague Security Delta partners are in the process of establishing a Cyber Incident Experience Centre. This is a setting where operational experience of contemporary threats and incidents are turned into insights, so that lessons can be learned in a few weeks' time. The issue of the 'DigiNotar hack' would have been a typical case to analyse in this centre, providing insight into both the technical details as the organisational aspects, for a select group of (C-level) people directly involved.**

## Scope and Definitions

Despite the fact that the European Cyber Security Strategy mentions "the Internet and more broadly cyberspace" in its introduction, the focus of EU cyber security strategy is mainly restricted to internet services and infrastructure. The scope of the Directive is even limited to internet services and infrastructure.

That means that a big part of cyberspace (namely the part not (directly) connected to internet, is out of scope. Including mobile telecommunications, process control systems, medical equipment such as pace-makers and insulin pumps, digital TV's, point-of-sale terminals, ICT in vehicles, etcetera. These are all areas where a large and growing cyber security risk is present. The EU strategy overlooks that most Mem-ber States look at cyber security from a broader perspective.

The EU cyber security strategy does not define the terms used and the directive defines only a limited number of terms. Also there is no international consensus on the definition of terms such as cyber security, cybercrime and other cyber-related terms (Luiijf, 2013; ENISA, 2012; Klimburg, 2012). Interpretation differences may therefore occur between Member States and in the interaction between the EU and the Member State functions, which will have an negative impact on (international) cooperation.

The same comments hold for the definition of critical infrastructures in the Strategy. The list of critical infrastructures in the Strategy is different from the list in the Directive and is non-exhaustive. It is unclear if for exam-ple the cyber risk to drinking water systems and prisons is covered by the Directive or not.

Rightly, the EU strategy mentions an all-hazards approach to resilience. Unfortunately this is not being elaborated further in the strategy, which is confined to vulnerabilities of process control systems and exercises. Resilience-enhancing activities, such as the activation of the C-level and performing stress tests are not addressed by the EU strategy.

## Conflicting roles and mandates

It should be noted that the EU strategy and the Directive take insufficient account of existing mandates and organisational structures within the Member States.

The Strategy actually prescribes in detail how Member States have to implement organisational structures. For example, the national cyber security authority has to perform a list of tasks which may conflict with existing mandates and information flows within Member States. Another example is the task to inform the legal authorities after receiving a security breach notification caused by cybercrime. Due to that, the notifying infrastructure operator is confronted with two or even three conflicting mandates which causes uncertainty in the consequences of the notification. A security breach and near miss notification approach alike the one globally adopted in the air transport sector would have supported the objectives of the Strategy much better.

In this factsheet, experts of HSD's Innovation House Cyber Security have touched upon a number of topics where we relate (positively or negatively) to the new European Cyber Security Strategy and proposed Directive. This is not a complete study. For more information please contact: info@thehaguesecuritydelta.com. We will connect you with experts in our network.