FIC 2014 DIGITAL IDENTITY AND TRUST

6th International Forum on Cybersecurity

FIC Observatory

EU Cybersecurity: Ensuring Trust in the European Digital Economy

Synthesis of the FIC Breakfast-Debate
15 October 2013, Brussels

With the participation of

Tunne Kelam
Member of the European Parliament'
Foreign Affairs Committee

&

Dr. Gustav Kalbe
Deputy Head of Unit "Trust & Security", DG "Communications Networks, Content and Technology", European Commission

Debate moderated by
Axel Dyèvre
Managing Director at CEIS European Office

This report is transmitted for information purpose only.
It does not necessarily reflect the opinions and views of CEIS, nor is it bound by its conclusions/assertions.

Boulevard Charlemagne 42 – 1000 Bruxelles – Tél. +32 2 646 70 43 – Fax : +32 2 646 70 22
Email : bruxelles@ceis.eu - Site web : http://www.ceis.eu

Recent initiatives of the European institutions related to cybersecurity highlight the increasing need for a stronger involvement of the European Union in the digital world. The EU intends to exploit all the opportunities provided by the digital revolution to further develop the digital European economy. Between economic necessity and strategic opportunity, the cyberspace has become a new field for commitment at the EU level.

However, the development of Internet related activities is conditional upon total confidence in networks and information systems. Building digital trust and ensuring confidence require security, confidentiality and protection of data. Recent international events have increased user demand for greater security, protection and transparency in the digital world. This is the reason why the EU started a modernisation process of its existing legislation on network security. Digital confidence and data protection were given an important place. Flagship measures such as the European Cybersecurity Strategy and the NIS Directive are in addition to recent initiatives undertaken by the EU to develop relevant cyber security policies, to accompany the development of an integrated and safe digital market and to foster R&D investments.

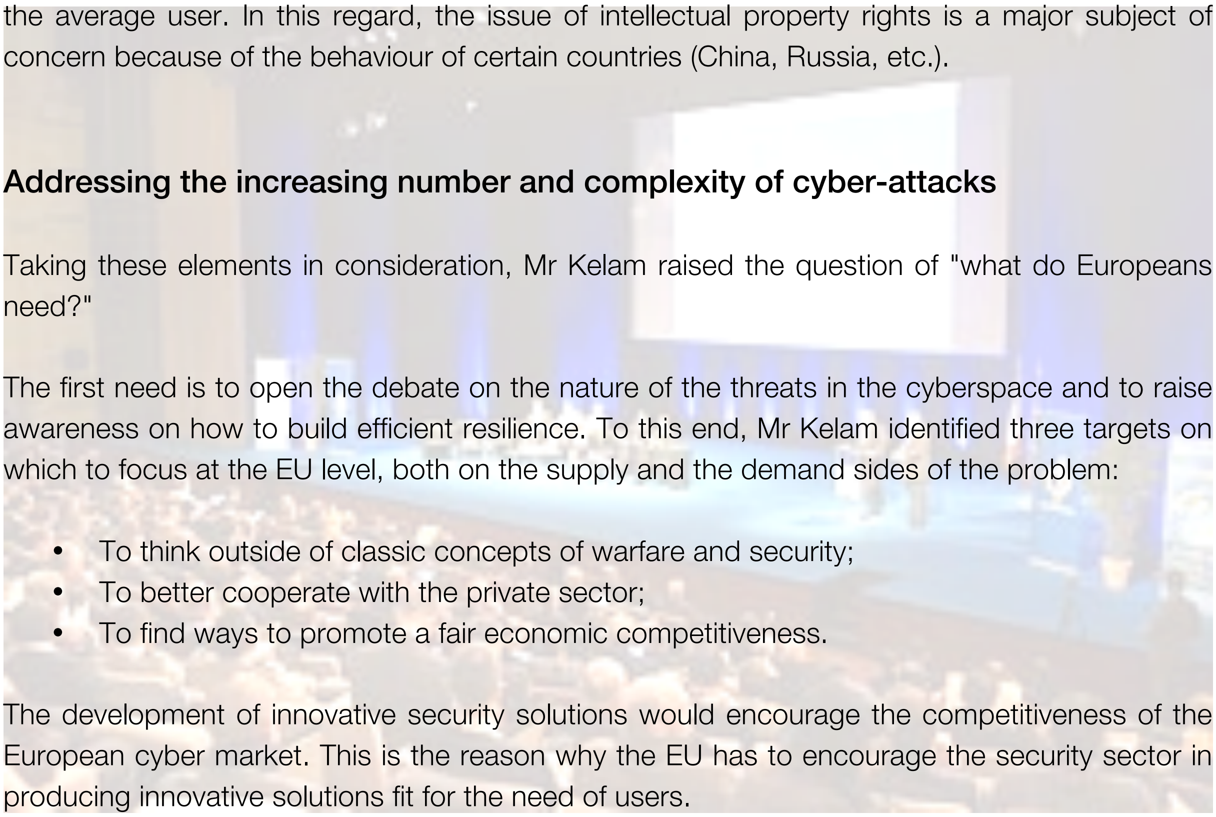
The dialectic between protecting privacy, promoting economic growth and ensuring security is at the heart of the topics to be addressed at the 2014 International Cybersecurity Forum (FIC) dedicated to "Digital Identity and Trust" (http://www.forum-fic.com).

Therefore, the FIC Observatory organised a round table in Brussels on 15 October 2013 to further integrate the perspective of the European Union into the discussions of the next Forum to be held on the 21 & 22 January 2014. This event aimed to question the follow-up of the recent initiatives undertaken by the European institutions. The objective was also to analyse the policy rationale behind the increasing involvement of the EU.

The views expressed in this report are personal opinions of the speakers and not necessarily those of the organisations they represent, nor of the International Forum on Cybersecurity (FIC) organiser board, its members or partners.

Reproduction in whole or in part is permitted, providing that full attribution is made to the International Forum on Cybersecurity and to the sources in question, and provided that any such reproduction, whether in full or in part, is not sold unless incorporated in other works.

MEP Tunne Kelam - presenting himself rather as an interested amateur than an expert on cybersecurity - described the cybersecurity challenge as twofold for European policy-makers: they have to be aware of the danger and then promote greater communication between different stakeholders. As recent examples demonstrated, cyber-attacks have intensified, and their level of complexity increased over the last years. In the same time, the number of users is expanding. Unfortunately, these users – who are most of the time unaware of the consequences of their behaviours - are increasingly unprotected from cyber threats. In such a context, the situation is becoming increasingly concerning. Mr Kelam estimates that cyber attacks cost a huge economic cost for the public and private sector stakeholders as well as for the average user. In this regard, the issue of intellectual property rights is a major subject of concern because of the behaviour of certain countries (China, Russia, etc.).



Addressing the increasing number and complexity of cyber-attacks

Taking these elements in consideration, Mr Kelam raised the question of "what do Europeans need?"

The first need is to open the debate on the nature of the threats in the cyberspace and to raise awareness on how to build efficient resilience. To this end, Mr Kelam identified three targets on which to focus at the EU level, both on the supply and the demand sides of the problem:

- To think outside of classic concepts of warfare and security;
- To better cooperate with the private sector;
- To find ways to promote a fair economic competitiveness.

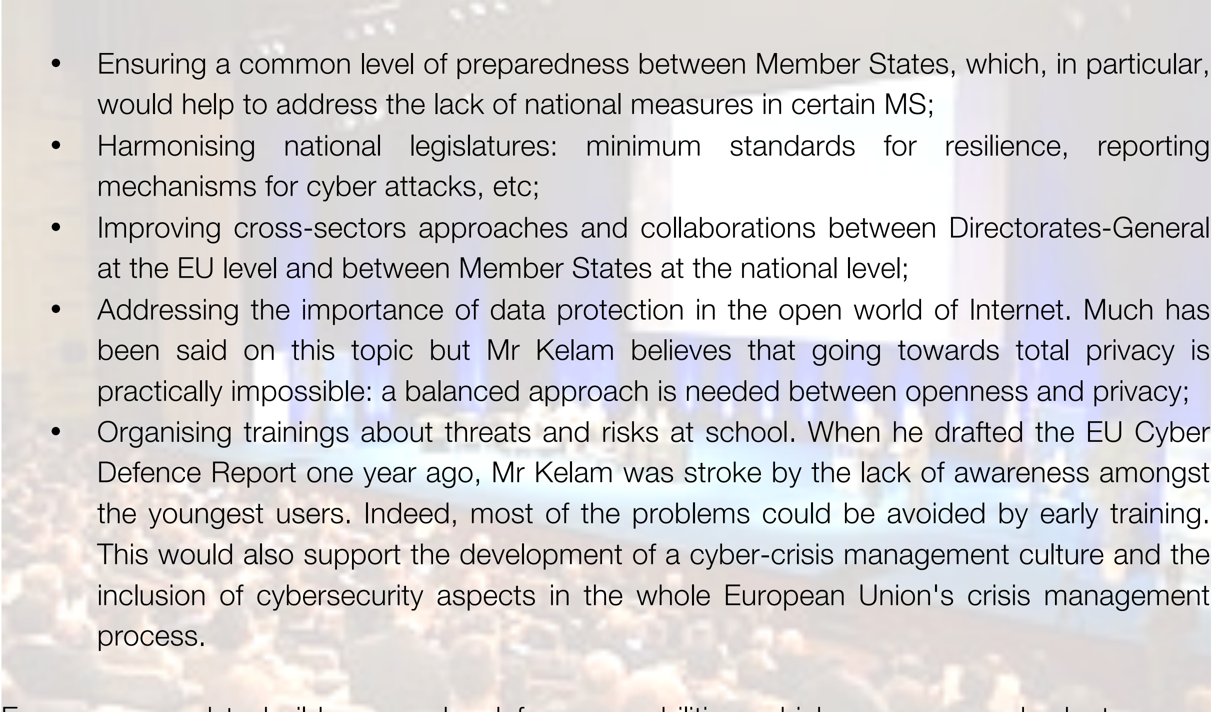
The development of innovative security solutions would encourage the competitiveness of the European cyber market. This is the reason why the EU has to encourage the security sector in producing innovative solutions fit for the need of users.

Mr Kelam also underscored the problem of identifying cyber-attacks' perpetrators. According to him, the challenge is to identify who they are, and then to implement relevant measures to pursue them. The Tallinn Manual on the International Law Applicable to Cyber Warfare produced in 2013 is one very positive response that can be used as a basis. It addresses several key issues among which the nature of the risks, the way states should answer, etc. The Tallinn Manual - which second updated version is currently being prepared - also insists on the need for deeper cooperation between the states.

> *"Key changes are needed at the EU level to address the challenges of the cyber-age"*
>
> Tunne Kelam, Member of the European Parliament

The European Union's response to the cybersecurity challenges

Mr Kelam highlighted the following key changes needed at the EU level:



- Ensuring a common level of preparedness between Member States, which, in particular, would help to address the lack of national measures in certain MS;
- Harmonising national legislatures: minimum standards for resilience, reporting mechanisms for cyber attacks, etc;
- Improving cross-sectors approaches and collaborations between Directorates-General at the EU level and between Member States at the national level;
- Addressing the importance of data protection in the open world of Internet. Much has been said on this topic but Mr Kelam believes that going towards total privacy is practically impossible: a balanced approach is needed between openness and privacy;
- Organising trainings about threats and risks at school. When he drafted the EU Cyber Defence Report one year ago, Mr Kelam was stroke by the lack of awareness amongst the youngest users. Indeed, most of the problems could be avoided by early training. This would also support the development of a cyber-crisis management culture and the inclusion of cybersecurity aspects in the whole European Union's crisis management process.

Europeans need to build more cyberdefence capabilities, which means more budgets, more qualified personnel, more investments in R&D, etc. The European Defence Agency (EDA) would be the right arena to put in place such actions. Mr Kelam also stressed that cyber military units are needed in Member States. The December 2013 European Council on defence issues will give to cybersecurity and cyberdefence a prominent place. This council will provide a unique opportunity to address these huge challenges.

MEP Kelam eventually addressed the international dimension of EU cybersecurity policies by calling for an improvement of EU cooperation's tools. Several existing arenas can be used in a complementary way to address these issues: the Organisation for Security and Cooperation in Europe (OSCE), NATO, the Council of Europe, or the European Union. Within the EU, one major obstacle to cooperation seems to be the unwillingness of Member States to ratify common international texts such as the Budapest Convention on cybercrime. On the international stage, cyber-dialogue must be engaged with BRICS, and the EU and NATO have to continue to cooperate for training and capacity building. Despite the recent surveillance scandals, the "United States of America remain our first ally" Mr Kelam added, in particular on cybersecurity issues. Indeed, the EU-US Working Group on Cyber Security and Cybercrime is one of the most active elements of the transatlantic relation. Because they share common political objectives and values, the US and the EU should work together to be at the forefront of cybersecurity and put in place their rules on the international stage.

> *"Despite the recent PRISM scandal, the USA remain our first ally to set up rules and standards at the international level"*
>
> Tunne Kelam, Member of the European Parliament

Translating the European Cyber Security strategy into effective actions

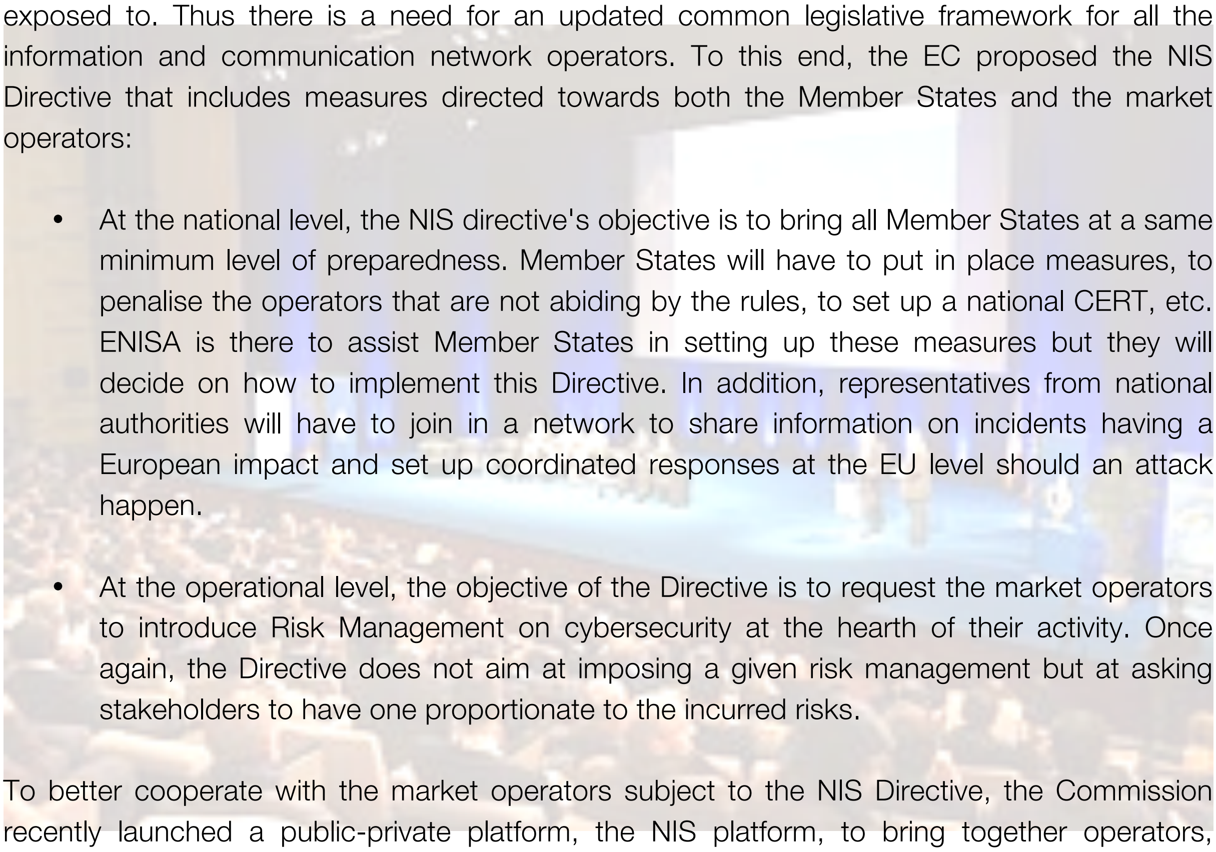
The presentation given by Dr. Gustav Kalbe - Deputy Head of Unit at the DG Connect - provided the audience with an overview of how the EU is currently implementing its comprehensive approach to cybersecurity and digital issues. Whereas for about three years cybersecurity has emerged as a major global issue, the EU has a longstanding experience in this field: creation of the ENISA in 2004, adoption of the "telecoms package" in 2009, etc. What is now really different is that the European Commission has its flagship Digital Agenda for EU in which one pillar is dealing with Trust and Security.

However, Dr Kalbe stressed the need for the European institutions to intensify their efforts to reach its objectives. Indeed, the risks and issues related to cybersecurity are dramatically growing. This is the reason why the EU drafted the recently published Cyber Security Strategy of the EU to present a comprehensive approach. The Strategy is based on four pillars: international dimension which is actively followed by the EEAS; combatting cybercrime mainly followed by DG HOME (EC3's launch, Europol's action against pornography on the Internet, etc.); the Network and Information Security (NIS) Directive; and the technological and industrial dimensions.

The two last pillars of the European Cybersecurity Strategy fall under the responsibility of DG Connect.

The Directive on network and information security (NIS)

The action of DG Connect aims to increase the resilience of information networks and to make sure that all stakeholders take responsibility and ensure efficient protection of our networks. Dr Kalbe justified the legitimacy of the EC to act on such issues by underscoring the need to address a failure in the internal market: while companies providing communication services such as Orange or France Telecom are covered by common European legislation on telecommunication, new communication providers (such as social networks) escape the obligations of this legislation. In the same way, electricity grids and critical infrastructures' operators should also take appropriate measures to address the cyber threat they could be exposed to. Thus there is a need for an updated common legislative framework for all the information and communication network operators. To this end, the EC proposed the NIS Directive that includes measures directed towards both the Member States and the market operators:



- At the national level, the NIS directive's objective is to bring all Member States at a same minimum level of preparedness. Member States will have to put in place measures, to penalise the operators that are not abiding by the rules, to set up a national CERT, etc. ENISA is there to assist Member States in setting up these measures but they will decide on how to implement this Directive. In addition, representatives from national authorities will have to join in a network to share information on incidents having a European impact and set up coordinated responses at the EU level should an attack happen.

- At the operational level, the objective of the Directive is to request the market operators to introduce Risk Management on cybersecurity at the hearth of their activity. Once again, the Directive does not aim at imposing a given risk management but at asking stakeholders to have one proportionate to the incurred risks.

To better cooperate with the market operators subject to the NIS Directive, the Commission recently launched a public-private platform, the NIS platform, to bring together operators, national authorities and EU institutions and to discuss best practises. The NIS platform will come with first concrete recommendations in the spring of 2014.

Industrial and technological dimensions

The upcoming European Framework Programme for Research and Innovation - Horizon 2020 - is defined in collaboration with all stakeholders identifying which topics will be addressed. This could be for example the development of the cybersecurity risk management process mentioned above.

Two general trends guided the elaboration of this programme to be launched in 2014:

- To work on concrete support to business. In this regard, DG Connect proposes to launch in 2014 a work programme for market operators. The objective is to look for concrete solutions in the fields of information sharing, RM, privacy, etc.

- To introduce security from the start of the manufacturing process. Manufacturers do not give enough consideration to security. The business model has to change in order to make security a top priority for the ICT sector.

Such an approach, rather than imposing additional constraints, would support a strong European industrial strategy insisted Dr Kalbe. Europe has the fundamental values of privacy and protection at its core, and international partners know European technologies can be trusted. Thus, integrating security by design would be an additional asset for the European industry.

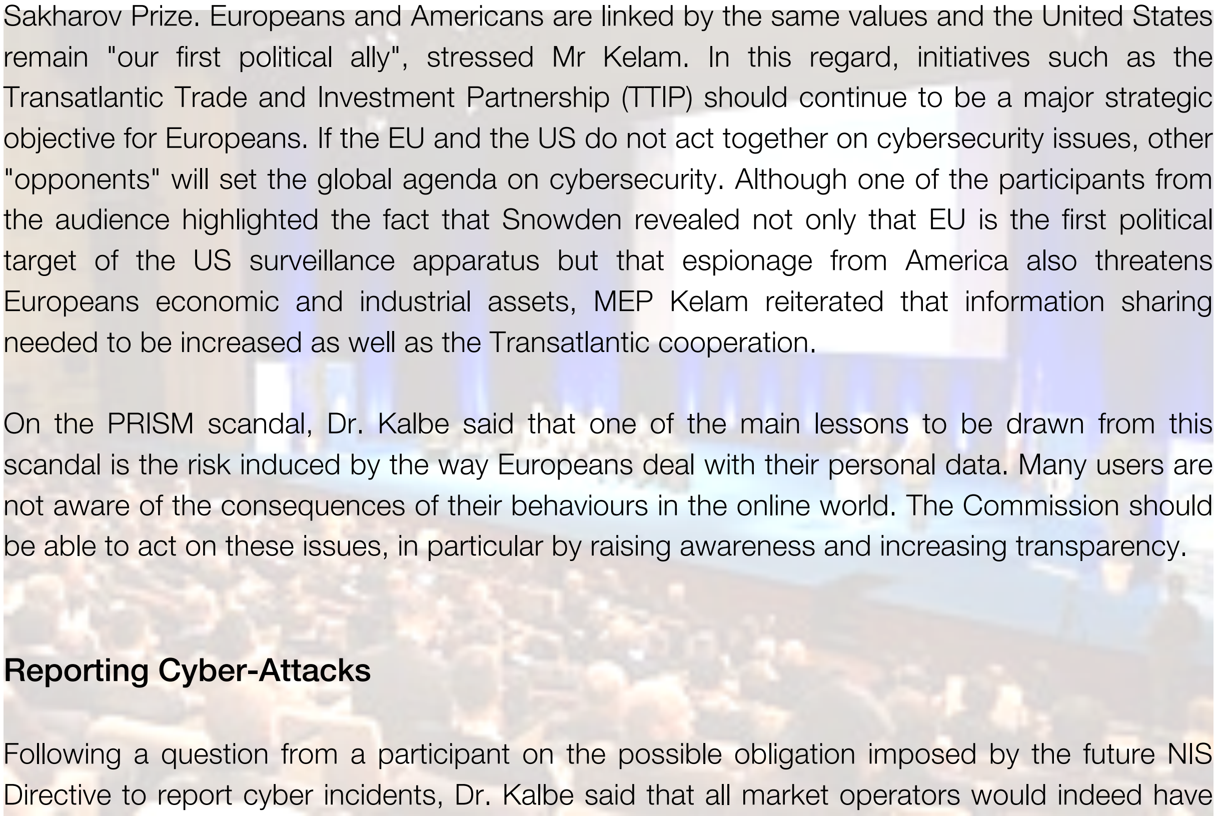
"Integrating security by design for our information networks would support the development of a strong European ICT industry trusted by our consumers"

Dr Kalbe, Deputy Head of Unit "Trust and Security",
DG Connect, European Commission

Discussion

The PRISM scandal and its consequences on the transatlantic relation

Panellists were asked several questions about the impact of the PRISM mass surveillance scandal on the transatlantic relation. According to MEP Kelam, to be fully understood, the PRISM scandal must be placed into a broader context. Indeed, this scandal is too emotional, as evidenced by the recent European Parliament's proposition to award Edward Snowden the Sakharov Prize. Europeans and Americans are linked by the same values and the United States remain "our first political ally", stressed Mr Kelam. In this regard, initiatives such as the Transatlantic Trade and Investment Partnership (TTIP) should continue to be a major strategic objective for Europeans. If the EU and the US do not act together on cybersecurity issues, other "opponents" will set the global agenda on cybersecurity. Although one of the participants from the audience highlighted the fact that Snowden revealed not only that EU is the first political target of the US surveillance apparatus but that espionage from America also threatens Europeans economic and industrial assets, MEP Kelam reiterated that information sharing needed to be increased as well as the Transatlantic cooperation.



On the PRISM scandal, Dr. Kalbe said that one of the main lessons to be drawn from this scandal is the risk induced by the way Europeans deal with their personal data. Many users are not aware of the consequences of their behaviours in the online world. The Commission should be able to act on these issues, in particular by raising awareness and increasing transparency.

Reporting Cyber-Attacks

Following a question from a participant on the possible obligation imposed by the future NIS Directive to report cyber incidents, Dr. Kalbe said that all market operators would indeed have to report incidents. The relevant level to which attacks would have to be reported - national or European level - still needs to be defined. The NIS Directive will establish a cooperation framework via a "network of national NIS competent authorities" to which cyber attacks and incidents would be reported. At this stage the question of the relevant body - ENISA or the European Commission - to coordinate the attack reporting process is still under discussion.

One of the questions raised by the audience on cyber-attack reporting was whether it would be possible to make the public sector more accountable. Indeed, much is expected from the private sector but how to make the public sector more accountable also? Dr Kalbe replied the first elements of response are in the NIS Directive, which also targets public authorities. The public sector is increasingly relying on ICT to support their daily missions: smart grids, smart cities, etc. Public institutions need to be supported in order to adapt their behaviours and build resilience.

The question was also asked of whether it seemed important from the Commission's point of view that Europe generates its own standards on cybersecurity. The EC is indeed working on the development of standards but the international community is the right level to address this issue. It is a major concern but the EC is looking at the existing standards rather than trying to create European ones.

Human factors vs. Technological Solutions

Digital identity also questions the development of appropriate solutions to mitigate risks caused by our dependence on digital assets. Youngest users seem to be more vulnerable to cyber threats because they lack a basic technical knowledge of digital tools they are daily using. In this regard, Mr Dyèvre, Director of CEIS-European Office and moderator, asked if solutions should be found at a human level or if we should rely on technological progress to better protect ourselves. "Human factors came first, and it is a good thing", stated MEP Kelam. Training and awareness-raising initiatives play a key role in the European Cybersecurity Strategy, through initiatives such as the European Cyber Security Month (ECSM). The technological dimension also needs to be addressed because most of the users do not know the technology supporting the devices they depend on. This is the reason why security by design is very important and why security must be introduced at the manufacturing level.

Taking up the question of whether the EU is the relevant level to address the overall question of Digital Identity, Dr Kalbe announced that another piece of legislative measures including the point of digital identity was under discussion in the European institutions. Dr Kalbe added that users do not have to necessarily disclose personal information or data to enjoy the benefits granted by the digital society. One possibility to address the challenges of digital identity would be to further develop such solutions not requiring personal information. There are a lot of examples in that sense and it is an interesting additional field of engagement for the EU.

"The technological dimension must be addressed because average users do not know the technology supporting the devices they depend on. This is the reason why security by design is very important and why security must be introduced at the manufacturing level"

Dr Kalbe, Deputy Head of Unit "Trust and Security",
DG Connect, European Commission

Next challenges to be addressed

"*On the EU level, the most important is now to bring all our MS on-board with the same level of technical preparedness*", concluded MEP Kelam who called for the creation of a common European framework on cybersecurity, both legislative and operational. The NIS Directive will improve the situation in this respect, and the European Parliament intends to bring a constructive contribution to the debate.

Dr Kalbe concluded that the adoption of the Directive could of course be considered as the main short-term objective of the European Commission. From a long-term perspective, the main objective would be to capitalize on the investment of Europe in this area to support the effort to get out of the economic crisis. This would only be possible by building a robust European competence for digital security. Now that everyone has realised that cybersecurity and digital economy really matter, it is time to build a strong European ICT industry.

This breakfast debate was held in partnership with the European Cyber Security Month 2013 (cybersecuritymonth.eu) an EU campaign to promote cybersecurity.