Support by

Hosted by:

Cyber Security – Risks and Opportunities for Europe's Economy

21 May 2014, Brussels

Final report

This debate was organised by Digital Enlightenment Forum (DEF) and hosted by Deloitte. The president of DEF**, George Metakides** opened the meeting by recalling the impact of the Snowden revelations in mid-2013 which raised serious concerns for citizens and generated strong political debate, including at the European Commission (EC) and amongst Member States (MSs). It figured prominently at the DEF 2013 Forum in Brussels (September 2013) where a first call was made for a new covenant for the digital society between governments, industry and citizens. Parties, including individual citizens, in the EU are asking how their cyberspace can be secured particularly if in the global economy so much data is being collected and managed by global companies not based in the EU.

He invited the participants to examine Europe's real options to protect itself against the dangers in cyberspace, taking account of the reality of the global power balance and the need for free trade. What is the impact of current EU initiatives and do we need to do more?

Erik van Zuuren, on behalf of the host Deloitte, welcomed all. He noted Deloitte's interest in Information Security and referred to the meeting on *Cyber security (State of Play)* hosted by Deloitte and organised by EEMA on 15 May, which particularly addressed the related technical and tactical issues, complementary to this DEF meeting that aimed at the longer term policy and strategy level. He referred to the changes in society due to digitisation, and also recalled Echelon, the affair of 20 years ago in which the US with some of its partners were alleged to be spying on EU nations, for political as well as industrial purposes. His conclusion was that cybersecurity problems have already been with us for a long time, is clearly growing, but is still not adequately addressed. There is an urgent need for a coherent EU strategy.

Raffaele Di Giovanni Bezzi (EC/CNECT, Unit Trust and Security) presented the EU policy on cybersecurity. He noted the need for a comprehensive EU vision and co-ordinated action because of the economic and social benefits of digitisation that are jeopardised by cybercrime and other social risks (privacy), and the need to address cross-border and global cybercrime. He mentioned three strands of EU policy/action:

1. NIS Directive (EP voted in March 2014, expected final agreement with Council at the end of 2014):
    a. Strengthening capabilities of Member States (MS) for strategy, competent authorities and CERTs.
    b. EU-level cooperation of MS authorities, co-ordination of early warning and response, capacity building, EU exercises and ENISA support
    c. Risk management and incident reporting for six specific sectors: energy, financial, transport, health, Internet enablers, public administrations.

2. Public-Private NIS Platform, an inclusive, multi-stakeholder platform (>200 organisations) consisting of three working groups:
    a. WG1 – Risk Management
    b. WG2 – Information exchange and incident coordination
    c. WG3 - ICT R&I strategic agenda.
3. Awareness activities: Cyber Security Month and Championship, NIS education and training, driving licence, self-assessment pilots.

Vangelis Ouzounis (ENISA, Head of Unit Secure Infrastructure & Services) presented ENISA's activities. The main focus of ENISA is to:

- Mobilise communities, including CERTS, InterPol, EuroPol, CePol and thematic groups of industry, Member State representatives and policy makers for cybersecurity.
- Advise on policy implementation for Member States and the European Commission.
- Recommend on actual problem solving for (and in discussion with) the stakeholders
- Hands-on activities for assistance and training (e.g. for CERTs) as well as cyber-exercises (Cyber Europe, EU-US cyber exercises).

After these introductions to EU cybersecurity policy other speakers presented views from practice.

Eric Blot-Lefevre (Director Association Forum ATENA) gave, after an introduction to his organisation, his ideas for a new trust architecture model and regulatory framework to ensure cybersecurity in the current migration wave from packaged software (stand-alone) to SAAS and IAAS in the Cloud. An adequate trust architecture would require regulation of e-ID, authentication and document signature validation (currently foreseen in the e-IDAS regulation), protection of the individual and their privacy (new data protection regulation (DPR)) and attention for cybersecurity of legacy systems (NIS Regulation). He proposed a cybersecurity ecosystem architecture consisting of three groups of parties: (1) cybersecurity software providers, (2) trust service providers and (3) digital validation parties (including certification authorities).

Troels Oerting Joergensen (Head EC3) presented the work of the European Cybercrime Centre (EC3). He underlined the benefits of cyber space for the economy, but law enforcement must be all the more effective and evidence gathering is the basis for that. In cyberspace the law enforcement landscape has changed completely. With a criminal no longer physically linked to the scene of a crime (or even in the same jurisdiction), the problems of attribution and jurisdiction have become technically and legally extremely difficult. We see the strong development of organised crime making use of global darknets, as well as problems of distinguishing between activities that are state-sponsored, coming from intelligence services, or being terror and/or crime-related. All four stages of addressing cybersecurity: prevention, protection, disruption and recovering need rethinking and we need governments, enterprises and citizens to work together on a trusted worldwide cyberspace. Steps need to be made at the EU level, but international agreements are needed to be fully effective.

Gillian Youngs (Professor Digital Economy, University of Brighton) sees an important change in the geo-political environment due to globalisation and the effects of ICT systems and applications.

The political space extends beyond the liberal paradigm, including for example China, Russia and others signalling the need for new geo-spatial understandings. New forms of diplomacy might be needed in recognition of socio-spatial (virtual) as much as geo-spatial (physical) interests. Societies, legal systems and states are adjusting to digital realities. States remain the major socio-political players in the international relations arena.

The EU is a vital and natural "middle-actor". It has a strong research capacity that could be directed to researching new rules of virtual diplomacy. This should take into account the technologically-mediated dimensions of state security, identity and economic growth. This search for a new digital political economy would work to balance the positive economic, political and social forces of ICT with any negative threats in the new digital conditions of international relations. Citizens, less constrained by state boundaries than ever before due to the Internet, are facing the limits of state protection and this situation is raising challenges to historic forms of social contract between state and citizen. As such the voice of citizens, acting at global, national and regional levels, need to be fully heard in the debate.

The discussion that followed touched on many points from the presentations given. Only a selection can be given here.

- We see many positive activities in the EU concerning cybersecurity. However, there is clear doubt whether they are timely enough and sufficient to address the immense problems we are facing. The regulatory process is slow, and sometimes seen as inconsistently implemented, particularly at the local (MS) level. Nevertheless, details are dependent on culture and national jurisdiction and must be implemented at national level which can be very difficult.
- The knowledge and awareness of citizens on cybersecurity problems and threats is rather low and needs more attention.
- There seems to be an underlying assumption that transparency, openness and accountability is essential for cybersecurity. However at the state security level this creates vulnerabilities and secrecy might be needed in certain situations. These problems may have arisen due to the conflation of security for the citizen (for protection against crime and to protect their privacy) and security of the society and state against terrorism and geo-political action of other states. The latest debates on state-supported intelligence gathering and citizen surveillance strengthen this conflation and therefore undermine citizens' trust in the digital society.
- We need to build trust in our digital environment through stronger and enforced regulation, as well as through ways of intelligence gathering and surveillance on the Internet that are comparable with what was considered normal and commonly accepted before, hence with guarantees of legal warrants based on reasonable suspicion only and no unspecified mass surveillance on individuals.
- Important questions at the level of nations states are:
  - Can we build trust in jointly fighting cybercrime?
  - Is it realistic in the existing international political space with increasing ideological challenges to find common ground?

  - Can emphasis on the benefits of global connectivity help create new forms of diplomatic understanding and process across ideological boundaries among states?
  - What can be done if another nation is not willing to cooperate in rolling up a cybercrime network?
  - Moreover, the attribution of criminal activity and the difficulty of properly distinguishing it from state-supported activities may aggravate these problems.
- It was strongly suggested that the EU should focus on cyber-diplomacy in conjunction with its attention to cybersecurity. Nation states were always reluctant having too many international contacts in this context. The time has come however to develop a new framework of international and national policies for governance and diplomacy in the digital age. The EU has a large body of experience in this at the practical as well as the scholarly level that should now be put to good use. Moreover, the increased opportunities of citizens to build their cross-border networks must be taken into account for its positive and negative effects. The changes will eventually be felt at the individual level and it will therefore not be sufficient to work at the level of nations, companies and international organisations only.
- The EU could ,at the more practical level, also give attention to:
  - The possibility of building a Cloud infrastructure under its own control.
  - Give more attention to strengthening awareness and best practice on cybersecurity.
  - Investigate the possibility for the EU to develop use its own procurement policy for the improvement of cybersecurity
  - Further development of EU regulation based on e-IDAS, the new DPR and NIS directive, to stimulate the development of a cybersecurity eco-system architecture including cybersecurity (software) providers, trusted service providers and validation/certification parties.

The debate could not, of course, be conclusive on all the complex issues involved. There are many and different facets to be taken into account and many longer term uncertainties. However a few **recommendations** emerged and can be formulated:

1. The EU needs to bring together experts from government, business, technology and social and economic sciences to formulate and implement an agenda for research and action to develop a new EU and international (including all global political powers) framing of policy and diplomacy in the digital age, ensuring cyber-diplomacy is consistent with cybersecurity implementation, given the international dependencies and cross-border community activities of citizens.
2. Develop a broad public-private partnership, including proper representation of citizens, for a joint action against cybercrime, including awareness activities and development of knowledge for enterprises and citizens to play their own roles in the improvement of cybersecurity.
3. Bring Member States together in a truly joint EU action, using all the MSs relevant assets, for EU cybersecurity improvement whilst ensuring an open mind for truly global cooperation and free trade.