Openforum Academy

'Improving Cyber Security in Europe, the way forward'

Report

Breakfast Briefing: 'Improving Cyber Security in Europe, the way forward'

24 April 2013, European Parliament, Brussels

Disclaimer:
This report is prepared by the rapporteur, Dr. Alea Fairchild, for OpenForum Academy (OFA). The summaries of the speaker presentations and panel discussions in this report are based on the rapporteur's notes and they are not in any way binding or necessarily complete. All effort has been given to reflect and convey objectively the essence of the speakers' presentations and the discussion.
The views expressed in the report do not necessarily reflect those of the rapporteur or OFA. Neither the rapporteur, nor OFA should be held accountable for any claimed deviation from the original speeches.

Foreword

The European Commission presented a package on Cyber Security in Europe in February 2013, consisting of a Commission Communication (COM / 2013 048) Cyber Security Strategy for Europe and a draft Directive (COM 2013 / 027) concerning measures to ensure a high common level of network and information security across the EU. The latter is now in the legal decision making process with the European Parliament and the Council.

The cyber security strategy recently addresses the most important themes in cyber security and is to be welcomed. Main points made in the strategy are the need for improved information sharing between the public and private sector to improve cyber security and the need for open standards and interoperability.

The Network and Information Security (NIS) Directive proposes significant changes to the status quo in that it mandates security breach notification to a government agency, not only for critical infrastructure providers, but also for a range of internet services such as search engine and social network providers.

Our briefing session speakers will address this topic by examining several issues. What role should the Commission play? Is mandating breach notification from “key providers of information society services” such as search engines and social networks to Government agencies as is proposed in Article 14 of the Directive going to make these services more resilient against cyber-attacks? What are the risks and benefits of this approach? What about cyber security standards and certification?

Speakers

Tunne Kelam – MEP EPP
Nick Coleman – Global Head Cyber Security Intelligence, IBM
Andrew Updegrove – Partner, Gesmer Updegrove LLP
Paul Timmers – Director, Sustainable and Secure Society, DG CONNECT

Moderator: Graham Taylor, CEO of OpenForum Europe.
Rapporteur: Dr. Alea Fairchild, Director, The Constantia Institute and Docent, HUB.

Graham Taylor opened the event by welcoming everyone to the OpenForum Academy (OFA) and explained the purpose of the OFA and its participation in the open standards community. He introduced the concept of the OFA with its approximately 40 Research Fellows from industry and academia, with its purpose of creating new thought leadership and debates. He pointed out they had provided the First OFA conference proceedings on the table for each participant. He introduced the breakfast briefing topic ***'Improving Cyber Security in Europe, the way forward'***, then used the example of the Twitter hack on the @AP account and the fake report of an injury to U.S. President Obama as an example of some of the issues in cyber security today.

Graham started by stating that the width of the topic was broad, as there is no clear cut definition of cyber security. With the Internet, a major discontinuity occurs with access and use of data, impact of cloud computing and the emphasis on a core public network. The Internet needs to remain 'open' and 'free', but there also needs to be a balance between this and the safety and security of the public infrastructure and networks. Today's discussion will focus on how to achieve that balance.

The four speakers invited to frame this discussion were:

Tunne Kelam – MEP EPP
Nick Coleman – Global Head Cyber Security Intelligence, IBM
Andrew Updegrove – Partner, Gesmer Updegrove LLP
Paul Timmers – Director, Sustainable and Secure Society, DG CONNECT

Questions to be addressed include:

- What is the impact of cross-border collaboration, specifically with other regions such as the U.S. and China?

- What is the validity of the EU role in this in relation to national security?

Graham then introduced the concept of the breakfast briefing panel, and that Chatham House Rules will apply, in that the speakers could be quoted, but no other participant in the debates would be quoted in their contributions.

Tunne Kelam opened his presentation with a welcome on behalf of the European Parliament (EP), and agreed that this was a hot topic, with an active interest in what could or should be done. He stated that the EP welcomed the draft directive of the European Commission (EC), and it was a long-awaited response to initiatives by the EP. Ninety per cent of SMB/ large companies have been targeted by cyber-attacks in the last 3 years, and losses due to cyber-attacks have tripled in this period. Sharing of information on cyber-attacks is based on trust and this trust needs to reciprocal on every level. The basis for trust is to demonstrate political will and ensure fulfilment of common minimum requirements to protect networks. Whereas all Member States have CERTs, only 13 of 27 Member States have a cyber national security strategy.

In terms of the cross-borders aspects of cyberspace, a difference across borders in terms of preparation causes challenges and there needs to be a minimum of requirements to build trust and share best practices. But there are different kinds of challenges to be solved. He used the analogue of sharing of information across border guards in a physical boundary.

He welcomed that the directive builds on a single market, pointing out that vulnerabilities in NIS can be damaging to single market.

He also welcomed that the directive aims to build a culture of risk assessment. One of the problems is the training of staff working in public entities, but also in private sector; in order to ensure full awareness and ability to act safely and securely in their respective cyber environment.

However, this implies a switch from a low level of preparedness to a higher level in the short term. It is nice to have a directive, but there are many directives. Implementation, however, takes decades to achieve both practical and political use.

Having national CERTS that can take over responsibilities is good, but how fast can they do this? He raised this question in regards to information sharing, infrastructure design, controls, costs and timings. These national CERTs should react quickly for immediate action, but how fast needs to be defined, as does the definition of severe impact and the definition of compliance assurance. He also discussed the subsidiarity principle; Sweden has for example already voiced its opinion.

He also questions what cooperative networks mean practically (Article 8), and if the differences in laws in different Member States would be handled. A further point is how to articulate to the private sector the benefits of information sharing, overcoming concerns on business secrecy and confidentiality.

The EP is preparing its response, with several committees involved (ECON, LIBE, ITRE, JUS, FA) and IMCO as the core committee. The EP is looking for the best outcome, producing more efficiency in the process.

Graham thanked **Tunne** for his contribution, and then started a discussion on how collaboration between governments, and between the private and public sector might work, leading to the contribution of **Nick** to the discussion.

Nick Coleman then presented the views of organisations active in running cyber security programmes in the context of this draft legislation. The environment for cyber security is becoming more challenging with more threat actors using cyber actions for their targeted activities.

His concerns about increasing attacks are in regards to critical infrastructures with malicious intent, potentially impacting services to citizens. One point Nick focused on was the need for risk management and the appropriate security for the environments that are critical, with a focus on priorities for protection.

He also discussed how to share information with organisations with a focus on the people and training aspects necessary for this to occur. The global nature of cyber securtiy challenges and of crossing country boundaries and the associated cross-jurisdictional issues.

In Europe forums like ENISA can help define best practices. Specifically referring to the draft EU Directive, he commented that at present the scope is wider than the critical national infrastructure. That the directive did not comment yet on creating information sharing and two way information sharing process.

Nick then stated that the communication was welcome, but if it focuses on governmental collaboration and two way information sharing. He believes that risk sharing environments need to be stimulated. He also shared that is was important to think through the issues of liability. For example, who is disclosing to whom? Are there liabilities for sharing that information further and how is that dealt with?

Another point to be discussed is the issue of liability, as this is crucial in the commercial environment. For example, who is disclosing to whom? What is the value chain of liability? What is the cost impact to businesses in the value chain?

Nick then closed his portion of the discussion with a summary of the key points he was making on risk management, critical infrastructure protection, and enabling intelligence and information sharing to create cyber security capacities. A focus on risk management, voluntary exchange and building cyber security capabilities can help drive forward. Because the threat levels are increasing, the impact of these attacks are rising, and they are increasingly more sophisticated in their nature.

Andrew Updegrove then opened his contribution to the discussion by applauding the EC on their work in this area. He stated that the U.S. was ineffective on this at present, and it has been problematic. He agreed with Nick that things could only get worse with asymmetric military threats. Cyber-attacks can be seen as cost effective but one still needs to protect the physical location. History tells us that all kinds of threats will repeat.

As he focuses on standards, Andrew commented on the standards aspect of the draft Directive. He stated that standards are crucial and that the challenges for this are environmental with many vulnerable areas and can give a false sense of security. He gave examples of what view could work in this regard by discussing electronic payment standards that do not specify specific standards but designates the whole payment value chain including process, environmental approach, actors and roles in the environment. Standards are achieved within this environment at a macro level, with macro level requirements that isolate goals and areas of concern, not micro level approach.

It is better to use a problem solving approach on the points of vulnerability. More innovation needs to take place within the marketplace to address needs. Standards need to be held out as best practices plus additional points beyond that. He would hope that what security should like would be described and then the necessary actions and elements of security environments would be defined and then a pool of market actors would produce actions to achieve it. This would allow public private cooperation plus the flexibility to achieve it.

He also addressed the concept of a global focus in order to facilitate global competition. If standards vary from region to region, businesses will have to undertake significant additional expense to comply with local requirements.

To summarise, Andrew gave an overview of his message on flexibility and macro focus on standards, brought up the lack of governance and comments on the lack of discussion in the draft Directive on information sharing, and questioned why that was the case. Was it because of potentials for anti-trust, or was it that information sharing mechanisms already exist in industry? Industry cares about loss, and avoidance, therefore the focus on risk management.

Graham then made an introduction to **Paul Timmers** and the work of the EC on the draft Directive and Cyber Security Strategy.

Paul opened his remarks with some clarification on the process of the strategy. He started with the comment that the EC's text is correct, but not complete in its approach. The EC is aware of the urgency to address this issue, and no one wants to be responsible for not acting. He is happy that the EP and Council have reacted quickly, and that the processes are in place for pursuing the strategy and adopting the Directive.

The goal is for the Directive to be adopted before the end of the legislative period. The approach allows a focus on the NIS directive, plus other elements of strategy. This includes public private cooperation necessary for best practice, risk management and information sharing.

There is a Call for Expressions of Interest for the NIS platform coming out in the next few weeks, and a mid-June meeting on this as well. They wish to keep the focus on public private cooperation, proper risk management procedures, best practices and the need to act together with industry.

He felt it was very positive that the EP approved the new ENISA mandate, therefore supporting the strategy and tools to make the process move forward.

He then brought up his concerns, specifically how to act at an European level on this subject. The EC believes that it should not be centralized, but existing cooperation need to be encouraged then increasing cooperation where it is needed. National CERTS demonstrate cooperation within their environment at implementing standards. Not sharing impacts their ability towards national resilience.

The EC had reflected quite a while whether to choose a regulation or a directive, and felt that the directive promoted better practices of cooperation and supports current practices. In respecting current practices, there is not a focus on centralization of power at the European level, but touching on other competence methods that are so sensitive to this.

He agreed that Tunne had raised points to consider that were not fully dealt with in the strategy, including completeness and bi-directional sharing between public and private sectors. The point on scope as to who is obligated by this directive is also a point to consider, as not all sectors are included. He gave an example that chemical and hardware and software companies are not included, not are users in general. The question is if this scope is not proportional or related to the problem at hand. They include key internet enablers, but not all on the Internet.

The scope on sectors concerned is up for debate, but key internet enablers are in the scope, which they believe is the right way to go about it. He also agrees about Tunne’s point about the skill side not being addressed, and he joked it was a tactic to get it more attention. This attention is for awareness, but it needs more in the strategy, or skill, side which includes inviting industry to help address with their skills and best practices.

Paul felt that the comments made with the previous speakers were relevant on the risk of false incentives of compliance-based approach and standards basis. He also agrees with best practice sharing on risk management, and Article 16 of the draft Directive encourages standards, although not specifically which ones. He is also looking for a convergence of standards and best practices. He is not convinced that standards and risk management lead to "tick boxing", and the sectors in the scope of this Directive are major, and not seen as "tick boxers". Paul has found relatively little opposition from industry on this Directive to-date. He appreciated the informed and sensible debate at this Breakfast meeting. He believes that the NIS platform being on the table sets up a wider basis for incentives. He agrees that the debate on standards in this area is crucial, and that the actions taken so far are on the right path. He gave examples of governmental alignment in particular countries (UK, Germany, U.S.), including joint approaches with NIST, heading toward more global standards.

His colleague Alessandra added a few points regarding participation of critical infrastructure providers (e.g. energy, banking) and the relation to the impact on economic development vs. the more rigid rules based approach of telecom directives. They both continued the discussion on the NIS platform as a vehicle to define the 'seriousness' of incidents in cyber security. Paul continued with a discussion on why industry should share with the public sector, and how sharing does not breach confidentiality and how these are networked industries, therefore impact has a domino effect. He also discussed trust and the impact of trust on networked industries, but within sectors, there is a large differential between computing facilities.

At this point, **Nick** added a comment about social media. Is social media a fundamental piece of society? We can agree that banking is a critical infrastructure, but then there is the question of liability - is hacking a social media account considered an incident? Nick then referred to Annex 4 of the draft Directive, where reporting on wrong password would be required. He encouraged a discussion on the practicality of reporting. Too much information is not always necessary, too much of a reporting obligation then allocated resources aware from other critical tasks.

Discussion

Disclaimer: These comments were taken from the general part of the meeting and do not necessarily represent any of the speakers' views or those of their organisations.

The first comment was regarding the scope of the draft Directive, and the exercise itself in reporting. One participant was part of a large MNE that under the scope is not obligated to report, but certain portions of its business do fall into internet enablement.

The next audience comment was in regards to the national competency area, and asked: "What is in this for the Member States?" What is the benefit (carrot)? The answer was that the Member States are supportive and realize they are as weak as the weakest networked Member. Not all Member States have sufficient resources; can be of concern to the other Member States. International market effect is larger than we think, and they should be concerned if they can react quickly enough.

Graham asked: Why do only 10 Member States have a centralised resource? He also asked a question regarding collaboration and common goals; do Member States buy-in?

Paul responded that they need a willingness to cooperate, as the CERTS cooperate and share capability experiences. Not all Member States have national plans or strategies, and this is moving up the priority lists of Member States.

Another audience member stated they were surprised by the comment regarding little industry resistance, as they are aware of large resistance in the ICT industry. It boils down to scope, and they believe the scope needs to be narrowed to solve some of the resistance problems. Others continued this line of questioning as to who should be included in the scope, and how this compares to the U.S. Executive Order, which has a different scope.

Paul commented on this to say that larger Internet providers are focused on providing trust, so no concern there. Smaller providers have the potential to be hampered by this, and they are sensitive to this argument.

Graham comment that the key message is that definitions are so important, and there are fundamental is scoping that the definitions are articulated well. He suggested that definitions could be addressed with industry groups.

Nick added that MNEs can also have bits of their business that are and are not involved.

Graham also brought up that this topic is interconnected to ICT, cloud and networking, all which have standards issues.

Andrew suggested instead of picking standards we try to evolve standards. Standards are a quasi-governmental process, with companies voluntarily following the regulation created. He discussed participation, incentives, no enforcement, and spontaneous compliance as some of the issues. He mentioned a comparison with EU standards development, and if industry leads development of standards or if government does.

The discussion ended with **Tunne** summarizing the EP viewpoint about concerns about the preparedness of Europe on cyber security and the concern of having certain Member States needing incentives as it may be considered a burden on their resources.

Graham Taylor closed the proceedings with the next steps to be taken in this discussion, including perhaps some follow-on sessions.