“The new legislative initiatives of the Commission on cyber security – how protected the Union will be?”

***Ivailo KALFIN**, Member of the High Level Group on Own Resources, EP Rapporteur on critical information infrastructure protection – achievements and next steps: towards global cyber-security.*

Mr President,

Mr Commissioner,

Dear colleagues,

Ladies and Gentlemen,

Thank you for the invitation and for choosing the topic of security and cyber security in particular for the Annual Seminar.

Few years ago cybersecurity was a very interesting issue but of almost no practical relevance. I was among the few first raising the issue in the EP and commuting between Washington and Brussels with the idea to help establish a transatlantic cooperation on these issues.

Now cybersecurity is very high on the agenda and still, there is a long way to go to establish a viable mechanism for assurance on the global web.

I shall not speak about the importance of the digital technologies and the speed they are entering our lives. I would rather focus on the vulnerabilities this phenomenon creates. Actually cyber security is not about a total protection - this is not possible. A reasonable protection instead is feasible, having in mind that the digital systems and technologies are very dynamic. There are few basics to deal with cybersecurity:

- The protection from cyber risks cannot be a one off event – it is a continuous effort;
- Cybersecurity is about resilience – the systems cannot be 100% protected but any attack should have a limited effect and the systems should resume working as soon as possible;
- Cybersecurity is a global issue. Still the lack of global cooperation should not be a reason not to cooperate in other geometries;

- Cybersecurity is a field where public and private interact with much more active role of the private players so far. No need to make it a government only issue – the multi-stakeholder approach has to be preserved.

A major obstacle for advancing the cybersecurity cooperation in the EU are the different levels and intensities of the national cybersecurity policies. Some MS fear that cooperation will not enhance security but rather create leakages and loopholes that malicious actors can use. They rightly point that the strength of a chain is determined by the weakest link. Nevertheless a huge progress is made over the last few years. At the same time risks increase exponentially – personal data, critical networks, security, terrorism – digital networks make us vulnerable.

Achievements to date – the Network Information Security directive (2016).

The NIS was adopted in 2016. It has to be translated in the national legislations by April 2018, then - 6 months to identify the companies – subject to compliance.

The NIS Directive sets a number of network and information security requirements which apply to operators of essential services and digital service providers (DSPs). The "operators of essential services" referred to in the legislation include enterprises in the energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution as well as digital infrastructure sectors. These are services of a high, even critical public interest.

The Directive defines a digital service as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services." The specific types of DSPs outlined in the Directive include cloud service providers, online marketplaces, and search engines. Still each MS has to determine the scope of the DSPs at national level. DSPs are, however, subject to less stringent requirements than the "operators of essential services" outlined in the Directive.

The NIS Directive includes a number of requirements around incident response and the implementation of technical security measures based on risk. The requirements are designed to improve cross-border cooperation in information and network security and foster a culture of risk management.

- **EU Security Network:** To improve cross-border cooperation, the Directive will create a network of Computer Security Incident Response Teams (CSIRTs) in each Member State. Member States are also required to designate National Competent Authorities (NCAs) and Single Points of Contact (SPoC) for cybersecurity monitoring, reporting, incident response, and other cross-border coordination. The CSIRTs from each Member State will have a range of tasks, including monitoring national security incidents, disseminating

early warnings, alerts, and announcements about cybersecurity, providing dynamic risk analysis, and coordinating with CSIRTs from other Member States.

- **Member State Strategies:** Every EU Member States has to implement a national cybersecurity strategy defining security goals as well as relevant policy and regulations needed to enforce the strategy. The Directive requires that any strategy should include issues like governance frameworks, response and recovery measures, public and private sector security cooperation planning, security awareness education programs, risk assessment plans, and lists of people and organizations involved in the strategy. Member States are also required to designate a NCA to monitor the impact and implementation of the NIS Directive at national level. National arrangements are to be open for coordinatyion and exchange of information with their counterparts across the EU.
- **Cooperation Group:** In addition to the other bodies established by the NIS Directive, there is a further requirement to create a Cooperation Group whose purpose is to facilitate collaboration around cybersecurity between Member States. The Cooperation Group is made up of representatives from Member States and the European Union Agency for Network and Information Security (ENISA) with a member of the European Commission acting as secretariat.
- **Incident Reporting:** Those organizations who qualify as DSPs under the Directive's criteria must implement a range of risk management measures both technical and operational. DSP organizations must comply with the Directive's incident reporting protocol, which requires that organizations notify "without undue delay" CSIRTs and other relevant bodies about any significant security incidents encountered. The timing for reporting incidents was one of the most difficult issues to agree upon during the negotiations for the NIS Directive. As we recently see with the case with personal data leakage from Uber, incident reporting might gain more and more importance.
- **Penalties:** the NIS Directive states that the responsibility to determine penalties for non-compliance lies with the individual Member States and not the EU. The Directive does, however, state that penalties must be "effective, proportionate, and dissuasive."
- **Best practices:** there are a number of steps organizations should take to ensure they remain in compliance with the NIS Directive
    - **Contact NCAs:** Organizations within the scope of the Directive should contact their Member State's NCA to find out to which authority they have to communicate in the event of a security incident and also to figure out which body can sanction them in the event of non-compliance.
    - **Liaise with CSIRTs:** Organizations should contact CSIRTs to obtain information about current security threats and get further clarity on cybersecurity issues.
    - **Implement technical and organizational security measures:** The Directive requires organizations to implement a range of security measures in areas like system security, incident management, testing, and compliance with international standards. While the Directive is short on specifics, organizations

should follow all industry cybersecurity best practices and look to meet other compliance regulations such as the GDPR, many of which have overlapping requirements. Organizations should also conduct risk assessments regularly and implement measures to mitigate identified risks.

- **Implement an effective security incident response process:** Incident reporting is a key part of the Directive. Organisations should have your own incident reporting process including criteria like number of users affected, duration of incident, geography, economic impact, and service disruption.

ENISA Regulation and Cybersecurity Act

These are the new draft proposals by the Commission. From the beginning of 2018 the co-legislators will start working on them. This package is building upon the NIS Directive and has more ambitious goals.

What are the changes proposed in relation to the European Union Agency for Network and Information Security's (ENISA) work?

- The current mandate will expire in June 2020 – the proposal is to renew it and have reviews but not an end date of a mandate;
- So far ENISA's role has mainly been to provide expertise and advice rather than dealing operationally with cybersecurity. This has already started to change. The Directive on the Security of Network and Information Systems (NIS) has formally created a network of Member State Computer Security Incident Response Teams (CSIRTs) and the secretariat for this network is provided by ENISA.
- reform ENISA into a stronger **EU Cybersecurity Agency** with a permanent mandate, greater operational resources and a stable footing for the future. The main aim of the Agency is to assist Member States in implementing the NIS Directive.
- New tasks and resources will be given to the Agency in areas such as operational cooperation and Information and Communication Technologies (ICT) security certification in order to reflect the new reality and needs in cybersecurity. ENISA will therefore play an important role in the field of EU cybersecurity certification policy by preparing, in cooperation with Member States' certification authorities, candidate European cybersecurity certification schemes. The new Agency's mandate, objectives and tasks will be subject to regular reviews.

But there is a number of issues that will require difficult negotiations:

- Subsidiarity and proportionality principle - who responds to a cyber attack?
    - To whom to report
    - Legal issues – access to sensitive information

    - Media policy
- Member states consider to a large extend cybersecurity as part of defense – that makes cooperation more difficult. This might be an issue to be included in the Defense Union talks
- Insufficient capacity in some MS, which might compromise the entire system
- EU CSIRT will need access to the necessary information, including sensitive one
- Cybersecurity crisis management – for some MS it is best done at national level, the EU level would create feeling of caveats
- ENISA should help exchanging information and experience – ENISA has to strengthen national abilities and not to replace the national mechanisms
- Cyber Europe exercises – a very good tool that has to be expanded and upgraded

To be successful, the co-legislators will need to see the big picture, not the details of the proposed legislation. The main goal has to be the increase of the cyber resilience of the MS and the EU as a whole.

The developments in the defense cooperation will largely influence the cooperation in cybersecurity.

ENISA should work upon request of the MSs and not replacing the national CSIRTS.

The Cybersecurity Act

Why is the Commission proposing an EU cybersecurity certification framework for ICT products and services?

- ICT security certification plays an important role in increasing trust and security in products and services that are crucial for the smooth functioning of the Digital Single Market. At the moment, a number of different security certification schemes for ICT products exist in the EU (e.g. Certification Sécuritaire de Premier Niveau in France, Commercial Product Assurance in the UK). While these initiatives confirm the importance of certification, there is a risk that multiple certification initiatives will lead to barriers and the fragmentation of the single market. For example, smart meters currently have to undergo separate certification processes in France, the UK and Germany. EU Certification has to **smoothen and facilitate the process**, without duplicating it.

- On the other hand, a "one size fits all" approach to cybersecurity certification will not work across the large variety of ICT products and services. The Commission is therefore proposing the creation of a **European cybersecurity certification framework** which is expected to deliver numerous individual European cybersecurity certification schemes, i.e. clear descriptions of security requirements to be met by covered products, systems or services. Resulting certificates confirming compliance with such requirements should be recognised in all Member States making it easier for businesses to trade across borders and for purchasers to understand the security features of products or services.
- The use of the certification schemes will be on a **voluntary basis** for market players. High cybersecurity standards – attested through such a certification scheme – could evolve into a competitive advantage for companies that aim at assuring consumers that their products and services pocess a certain level of cybersecurity. Such a scheme will thus encourage "cybersecurity by design".

Who will benefit from the certification framework and how?

- **Citizens and end-users** (e.g. operators of essential services), who will be able to make more informed purchase decisions related to ICT products and services they rely on day-to-day**.**
- **Vendors and providers** of ICT products and services (including SMEs and new businesses). They will have to go through one single process in order to obtain a European certificate valid in all Member States. For the German BSI "Smart Meter Gateway" certificate, for example, the cost is more than €1 million (highest level of test and assurance, concerns not only one product but the whole infrastructure around it as well), while the cost for smart meter certification in the UK and France is about €150,000.

- **Governments**, too, will be able to make more informed purchase decisions and will at the same time be equipped with an institutional framework that enables them to identify and express priority areas that need ICT security certification.

But there are also major concerns that are to be cleared during the negotiations:

- Voluntary vs. compulsory – how the EU voluntary certification scheme would match national compulsory certificates;
- Standartization b/f certification – in order to issue certificates, an EU wide standardization needs to be in place. Whose standards will be adopted? How the new standards will be drafted, how the level playing field will be assured?
- Standard – weakest or strongest? In case the EU adapts a weaker standardization than the MSs, the aims of the EU certification will not be achieved.

- To provide resilience, the producers of digital products – both software and hardware adopt dynamic systems of upgrading and patching. How certification will cope with this dynamism?
- Standards have to be recognized both by providers and users – sometimes the interests differ substantially;
- In case fines are imposed at national level, then how the regulatory arbitrage will be avoided?
- Risk to duplicate EU certification and national validations
- What to certify – i.e. IoT is a primary hacking target but differs substantially from PC protection – thousands of protocols – so the cloud, the gateways and the information exchanged are to be protected. How can this be standardized and certified?

Despite the difficulties, the EU needs to climb the next level of cybersecurity with more stringent rules, unification and powers to the supranational level. If designed properly, this can be successfully combined with the principle of subsidiarity.

There are several anchors that have to be observed though:

Certification needs to be voluntary, market driven and harmonized, technology neutral, ENISA should be in lead and the multistakeholder approach has to be observed. No additional bureaucracy should be created.

Certification should be clearly based on risk assessment.

There should be a clear distinction between labeling (awareness) and certification (assurance).

Legislation like the GDPR should not create competitive advantages to companies working in cybersecurity – it has to be completely neutral.

The convergence of national standards into EU and international ones is possible, though difficult.

The legislation proposed is certainly ambitious, mostly with the attempt to transfer the cybersecurity policy setting and management at EU level. This will not be at the expense of the national policies, but they have to be an integral part of the EU cybersecurity policy. This is a big effort and needs a massive political courage but it is worth.

Thank you for your attention.