Hong Kong Model European Union 2014

Working agenda

Meeting of the Heads of State or Government

April 25 and 26, 2014

1. Topic: EU Cyber Security Strategy

   a. Adoption of NIS (Network and Information Security) strategy and designation a national NIS competent authority with adequate financial and human resources to prevent, handle and respond to NIS risks and incidents;

   b. Create a cooperation mechanism among Member States and the Commission to share early warnings on risks and incidents through a secure infrastructure, cooperate and organize regular peer reviews;

2. A new Cyber Security Strategy by the High Representative Catherine Ashton and the European Commission is the first comprehensive policy document that the European Union has produced in this area. It comprises internal market, justice and home affairs and Foreign Policy angles of cyberspace issues.

3. The Strategy is accompanied by the technical legislative proposal by the European Commission's Directorate General Connect to strengthen the security of information systems in the EU. This will encourage economic growth as people's confidence in buying things online and using the Internet will be strengthened.

This project is co-funded by the European Union

4. The Strategy is offering clear principles for the EU international cyberspace policy:

    - Freedom and openness: The strategy will outline the vision and principles on applying the EU core values and fundamental rights in cyberspace.
    - The laws, norms and EU's core values apply as much in the cyberspace as in the physical world: The responsibility for a more secure cyberspace lies with all players of the global information society, from citizens to governments.
    - Developing cyber security capacity building: The EU will engage with international partners and organizations, the private sector and civil society to support global capacity building in third countries. It will include improving access to information and to an open Internet, and preventing cyber threats.
    - Fostering international cooperation in cyberspace issues: To preserve open, free and secure cyberspace is a global challenge, which the EU will address together with the relevant international partners and organizations, the private sector and civil society.

5. Cyber-security incidents are increasing in frequency and magnitude, becoming more complex and know no borders. These incidents can cause major damage to safety and the economy. Efforts to prevent, cooperate and be more transparent about cyber incidents must improve. Previous efforts by the European Commission and individual Member States have been too fragmented to deal with this growing challenge.

    - There are an estimated 150,000 computer viruses in circulation every day and 148,000 computers compromised daily.

This project is co-funded by the European Union

- According to the World Economic Forum, there is an estimated 10% likelihood of a major critical information infrastructure breakdown in the coming decade, which could cause damages of $250 billion.

- Cybercrime causes a good share of cyber-security incidents, Symantec estimates that cybercrime victims worldwide lose around €290 billion each year, while a McAfee study put cybercrime profits at €750 billion a year.
- The 2012 Eurobarometer poll on cyber security found that 38 % of EU internet users have changed their behaviour because of these cyber-security concerns: 18 % are less likely to buy goods online and 15 % are less likely to use online banking. It also shows that 74% of the respondents agreed that the risk of becoming a victim has increased, 12% have already experienced online fraud and 89% avoid disclosing personal information.
- According to the public consultation on NIS, 56.8% of respondents had experienced over the past year NIS incidents with a serious impact on their activities.
- Meanwhile, Eurostat figures show that, by January 2012, only 26% of enterprises in the EU had a formally defined ICT security policy.

6. The cybersecurity strategy – "An Open, Safe and Secure Cyberspace" - represents the EU's comprehensive vision on how best to prevent and respond to cyber disruptions and attacks. This is to further European values of freedom and democracy and ensure the digital economy can safely grow. Specific actions are aimed at enhancing cyber resilience of information systems, reducing cybercrime and strengthening EU international cyber-security policy and cyber defense.

7. The strategy articulates the EU's vision of cyber-security in terms of five priorities:

- Achieving cyber resilience

This project is co-funded by the European Union

- Drastically reducing cybercrime
- Developing cyber defense policy and capabilities related to the Common Security and Defense Policy (CSDP)
- Developing the industrial and technological resources for cyber-security
- Establishing a coherent international cyberspace policy for the European Union and promoting core EU values

8. The EU international cyberspace policy promotes the respect of EU core values, defines norms for responsible behavior, advocates the application of existing international laws in cyberspace, while assisting countries outside the EU with cyber-security capacity-building, and promoting international cooperation in cyber issues.
9. The EU has made key advances in better protecting citizens from online crimes, including establishing a European Cybercrime Centre (IP/13/13), proposing legislation on attacks against information systems (IP/10/1239) and the launch of a Global Alliance to fight child sexual abuse online (IP/12/1308). The Strategy also aims at developing and funding a network of national Cybercrime Centers of Excellence to facilitate training and capacity building.

10. The proposed NIS (Network and Information Security) Directive is a key component of the overall cyber security strategy and would require all Member States, key internet enablers and critical infrastructure operators such as e-commerce platforms and social networks and operators in energy, transport, banking and healthcare services to ensure a secure and trustworthy digital environment throughout the EU. The proposed Directive lays down measures including:

    (a) Member State must adopt a NIS (network and Information Security) strategy and designate a national NIS competent authority with adequate financial and human resources to prevent, handle and respond to NIS risks and incidents;

This project is co-funded by the European Union

(b) Creating a cooperation mechanism among Member States and the Commission to share early warnings on risks and incidents through a secure infrastructure, cooperate and organize regular peer reviews;

(c) Operators of critical infrastructures in some sectors (financial services, transport, energy, health), enablers of information society services (notably: app stores e-commerce platforms, Internet payment, cloud computing, search engines, social networks) and public administrations must adopt risk management practices and report major security incidents on their core services.

This project is co-funded by the European Union