Cyber Security Mechanism in European Union

Dr. Sanghamitra Sarma *

The very structure of the European Union's (EU) institutional arrangement and policy-making process reveals that it is a collective actor in an interconnected world seeking to establish itself as a strategic actor. However, a globalised world consisting of numerous other actors, each wanting to change the course of world affairs, faces a number of security-related threats that demand advanced and progressive measures so as to check their presence and adopt counter measures. Among the security-related threats, ensuring cyber security has become a growing need with increasing number of attacks on the internet. The hostile invasion into the virtual cyber space today varies in terms of its nature and frequency.[1] As such, it becomes imperative to look into the mechanisms or arrangements that the EU, collectively and individually has put in place to respond to cyber attacks.

The current trends of cyber attacks in EU:

The current trends in the cyber space that have been identified in the EU and member countries can be mentioned here to comprehend the types and variety of attacks. The analysis of cyber threats, which were encountered between December 2014 and December 2015 by the European Network and Information Security Agency (ENISA), the centre of network and information security for the EU and its member states, indicates that the prime threat during this period was malware. Installation of malicious information in the firmware of hard discs and mobile malware were identified as topics of concern. Among the top five countries providing online malware resources, three are EU member countries, namely Netherlands (ca.[2] 8 per cent),

Germany (ca. 5 per cent) and France (ca. 3 per cent). Web-based attacks like clicking on malicious URLs lead to infection of end-user devices. Portugal has the third most number of malicious URLs (ca. 3 per cent) followed by Netherlands (ca. 2 per cent). The ENISA Report, which gave an overview of geographic locations with high botnet density shows that among the top ten countries, from where such attacks originate, the Netherlands, Germany, France, UK and Romania are also included.[3] Related threats include phishing, spam, botnet, ransomware, data breaches, identity thefts, denial of services and information leakage.

The scale of threats that the EU currently faces, hence, necessitates the examination of the collective framework of the EU and individual responses that member states have adopted over the years to deal with cyber offences.

The collective framework:

Every European country has an agency, which is entrusted with the task of improving its cyber defence capabilities. Within EU, member countries are given training and research and development assistance. However, cyber threats do not respect borders and hence the EU must act together and not in isolation. Collectively, cyber security issues are addressed under the Digital Single Market, Home Affairs Policy and Foreign Affairs and Security Policy. An inter-service group coordinates across the European Commission. It is chaired by the Directorate General for Communications Networks, Content and Technology (DG CNECT), Home Affairs (DG HOME) and the European External Action Service (EEAS). While DG HOME is responsible for the fight against cyber crime and protecting critical infrastructures from attacks, DG CNECT is responsible for cyber security.

Recognising the expanding scope of cyber threats, the EU published a Cyber Security Strategy in 2013 and a proposal for a Network and Information Security Directive (NIS) accompanied it. The European Network and Information Security Agency (ENISA) formed in 2004 works to develop a cyber resilience mechanism, whereas the European Defence Agency (EDA), also founded in 2004, works to support capability development required to implement the 2013 Strategy. The European Cybercrime Centre (EC3) helps to protect European citizens and businesses by aiding criminal investigations, raising awareness against emerging trends of cyber attack activities and by pooling expertise and information regarding cybercrime issues. ENISA has been engaged as a facilitator for member states that supports the exchange of practices in the area

of **cyber crime policies.** It also acts as a chief force behind the series of pan-European cyber exercises, Cyber Europe as well as the joint EU-US cyber exercise called the Cyber Atlantic. Besides, the European Parliament and the Luxembourg Presidency of the EU Council of Ministers recently reached an agreement on the rules, agreeing to improve cyber security capabilities among member states on 8 December 2015. Another latest development in this regard has been the approval of the new data protection rules to strengthen online privacy and streamline legislation between the member countries. The General Data Protection Regulation (GDPR) proposed in 2012 was passed by the European Parliament with amendments in 2015. The new regulations includes stringent provisions like fines up to four per cent of companies' annual turnover for data breaches and strict requirements regarding collecting and using data for marketing purposes. This is expected to ensure the security of customer information in EU countries.

To step up cyber defence cooperation, the EU's Computer Emergency Response Team (CERT-EU) recently concluded a Technical Arrangement on Cyber Defence with the NATO (North Atlantic Treaty Organisation) Computer Incident Response Capability (NCIRC) on 10 February, 2016. This agreement provided a framework for exchanging information and sharing best practices between emergency response teams of both the organisations, keeping into account their decision-making autonomy and procedures. In fact, EU and NATO collaboration began in 2010 with consultations and annual meetings that have since become an essential feature of their cyber defence mechanism.

A number of cyber security conferences are held in Europe which aims to sensitise individuals, businesses and organisations about new emerging threats in the cyber space and effective tools and mechanisms to deal with the same. In this connection, the United Kingdom (UK) is the harbinger of advancing knowledge and raising awareness against cyber threats. The Cyber Security Summits held in London annually aim to bring together networking experts, penetration testers, senior government officials and policy makers from all sectors and industries to provide an update on UK's cyber security policy. Other events like the InfoSecurity Europe held in London and CyberSec held in Poland offer constructive and innovative solutions for making the cyber space safe for users.

Individual arrangements:

The BSA EU Cyber Security Dashboard (Business Software Alliance now known as BSA - The Software Alliance is a major leader in the global software industry before governments and the international marketplace) surveys national cyber security laws and policies across the EU. The purpose of this report is to provide government officials in each of the EU Member States with an opportunity to evaluate their country's cyber security policies as regards their legal and policy frameworks and the required infrastructure to implement laws and policies. It states that only a few countries like UK, Germany and Estonia have strong legal cyber security frameworks, whereas other countries have much work to do in this regard.[4] As such, it is necessary to examine the cyber security arrangements in these countries at first and then proceed to explain the mechanisms in other countries.

Among the European countries, the UK faces the most number of threats in the cyber space. The latest Internet Security Threat Report from cyber security firm Symantec ranked the UK second globally, for targeted attacks in 2014, and placed it on top in Europe.[5] Two-thirds of the targeted attacks were aimed at small and medium sized businesses. The latest figures from the Government Security Breaches Survey say that nearly three-quarters (74%) of small organisations reported a security breach in 2015.[6]

To counter the gravity of cyber security threats, the UK government has acted by investing 1.9 billion Euros by 2020 in cyber security. The government has allocated 860 million Euros until 2016 to establish a National Cyber Security Programme. The vision of the government is to ensure a strong and secure cyberspace that can enhance the UK's prosperity, national security and society.[7] This vision is set out in the UK Cyber Security Strategy, published in November 2011. The strategy has four objectives:

- Making the UK one of the most secure places in the world to do business online.
- Making the UK more resilient to cyber attacks.
- Helping to shape an open, vibrant and stable cyberspace that supports open societies.
- Building cyber skills, knowledge and capability, which the UK needs.[8]

The Minister for Cabinet Office, Matt Hancock spoke on cyber security recently to highlight the measures required to be taken by the government to ensure cyber security for it as well as businesses in an increasingly interconnected world. He remarked that this task concerns three imperatives – recognition, response and reward. "We need to recognize the scale of the challenge. We need to respond to it. And we need to reap the rewards of the digital revolution".[9] He also announced that a new National Cyber Centre will be established, which will cater to providing support, advice and intelligence industry needs. All these steps, as he said, will help to expand the Cyber First Programme, which was initiated in 2015 to enhance UK's cyber security skills.

Germany's Cyber Security Strategy was adopted on 23 February 2011. This strategy called for establishing the National Cyber Response Centre and the National Cyber Security Council. In view of the growing number of cyber attacks, Germany had passed a strict law on 10 July, 2015, ordering over 2,000 essential service providers to implement new minimum information security standards or face penalties if they fail to do so within two years. It gives companies two years to introduce cyber security measures or face fines of up to 100,000 Euros. Regulatory bodies like the Federal Office for the Protection of the Constitution (BfV) and the Federal Office of Information Security (BSI) work together in cooperation to gauge and measure the possible impact of cyber attacks on infrastructure facilities, while the Office of Criminal Investigation (BKA) undertakes the responsibility to probe cyber crimes, such as data spying, intercepting or manipulating.

Estonia was one of the first countries in the EU to adopt a National Cyber Security Strategy in 2008 resulting in a strong legal cyber security framework since then. The basic document, which was updated to form a part of Estonia's broader security strategy, is the Cyber Security Strategy 2014-2017. The general objective of the Strategy for 2017 is to increase cyber security capabilities and raise the population's awareness of cyber threats.

Besides, there are five sub goals like ensuring the protection of information systems, enhancing the fight against cyber crimes, development of cyber defence capabilities, adoption of independent cyber security solutions and development of cross sectoral activities.[10] The strategy also highlights important developments, examines threats to cyber space and suggests measures to tackle these threats. Public-private partnerships have been operational in the country as well. The creation of the Estonian Defence League's Cyber Unit (EDL CU) is an example of such

collaboration. Through the functioning of EDL CU, efforts are made to improve the security of Estonian state agencies and company's information systems through coordinated exercises, testing of solutions, training, etc. Training and sensitising the infrastructures about emerging cyber threats is the responsibility of the Information Technology Foundation for Education (HITSA). Estonia has cooperated with other countries like USA (Raytheon – an American defence contractor and industrial corporation) in the field of cyber security. It has been one of the leading countries in promoting initiatives to bolster efforts towards reducing the vulnerability of cyber attacks in North Atlantic Treaty Organisation (NATO), EU, United Nations, Council of Europe, Organization for Security and Cooperation in Europe (OSCE) and International Telecommunication Union (ITU).

Along with UK, Germany and Estonia, France also has a considerably mentionable cyber defence mechanism. Its national cyber security strategy was adopted in 2011. In France's national security agenda, cyber attack prevention and response have been given high priority. The French Network and Information Security Agency was created in July 2009 to improve the security of cyber space. The National Strategy for the defence and security of information systems was published in 2011. **A White Paper was designed to identify and protect critical infrastructure from cyber attacks in 2013.** The Cyber Defence Pact of 2014, a Ministry of Defence initiative, aims to develop cyber defence capabilities and make them accessible to the French society. It aims to lift up the resource base and operation research in safeguards against cyber attacks. It also aims to build a network of foreign partners within Europe and North Atlantic Treaty Organization (NATO). France participates actively in the work of the United Nations Group of Governmental Experts and the Organization for Security and Cooperation in Europe (OSCE) to establish an international normative framework based on current international law, as well as confidence-building measures and specific standards of conduct in cyberspace. France is also involved in implementing the objective of international cyber security capacity-building through specific programmes through the EU and NATO. USA and France have also been working in collaboration to "improve network defense, cooperate in responding to cyber incidents, and build upon existing diplomatic and military cooperation on cyber issues".[11]

The BSA Cyber Security Dashboard reports that though a consensus exists among member states about strengthening cyber security policies; however discrepancies exist in policies, legal frameworks and operational capabilities leading to 'notable cyber security gaps across Europe'.[12]

In this context, it will be purposeful to mention that not all member countries of the EU have a working National Cyber Security Strategy. This comprehensive strategy contributes towards increasing cyber security capabilities to address and respond to cyber attacks. The countries, which have established a National Cyber Security Strategy to define key guidelines to respond to threats of cyber crimes are Austria (established in 2013), the UK (2011), Cyprus (2013), Belgium (2012), Czech Republic (2011), Finland (2013), France (2011), Hungary (2013), Latvia (2014), Lithuania (2011), Luxembourg (2013), Netherlands (2013), Poland (2013), Romania (2013), Slovakia (2009) and Spain (2013). On the other hand, not all member countries of the EU together have a functioning Computer Emergency Response Team (CERT) as well as public-private partnerships working in cooperation to strengthen cyber security. Only Austria, Belgium, Croatia, Czech Republic, Estonia, Germany, Spain and UK have both CERTs and public-private partnership ventures which are an indication of the presence of a vigilant cyber security network. However, the BSA Cyber Security Dashboard points out that though 27 member states have established CERTs, "the mission and experience of those entities vary greatly".[13]

The EU Cyber Security Strategy is also comparatively nascent in its formation. Compared to the United States, which released its National Strategy to Secure Cyberspace in 2003 and Russia which approved its Information Security Doctrine in 2000, the EU adopted its Cyber Security Strategy in 2013. Moreover, member states across the EU decipher the nomenclature of cyber security in their own contexts "leading to a fragmented understanding and the lack of a reliable international definition of the term".[14] To ensure rapid identification and intelligence exchange, member states need to move beyond their rationale that cyber security is a part of the national agenda. Cyber attacks cannot be dealt in isolation as it does not respect any territorial boundaries.

As the ENISA Report says, "Internet of Things is here to stay, so is the cyber threat exposure that it represents."[15] The magnitude of the challenges that is constantly unfolding in the cyber space calls for a multi pronged approach to counter the complexities in a globalised world. The emerging cyber threats that continue to pose danger to individuals, businesses and organisations require the actors to be vigilant and involved in a consistent attempt to anticipate the nature and dimension of the threats, respond to these threats promptly, minimize damage and increase the possibility of retrieval of data that are crucial to critical infrastructures linked to national security, economic security, defence and national public health or safety. National cyber security strategies should be continuously updated to include focus on improving information

collection, reducing threats and vulnerabilities, encouraging research and development of new software technologies to counter attacks, conducting awareness and training camps and securing government information systems. A quintessential requisite is the consolidation of different agencies, public and private, to harness the best practices which can be consolidated to check cyber crime. The EU must utilize its collective strength to create a secure digital environment for its citizens. At the same time, developing a system of international cooperation can contribute towards incorporating the best practices which can be selected carefully as per their applicability to the EU cyber security strategy.

***

** Dr. Sanghamitra Sarma is Research Fellow, Indian Council of World Affairs, New Delhi.*

The views expressed are that of the Researcher and not of the Council.

Endnotes:

[1] As the European Union Agency for Network and Information Sharing (ENISA) Threat Landscape 2015 states, "Cyber threats have evolved while following two extremes. Effective simplicity, achieved with a series of 'low-tech' highly efficient infection methods. And effective complexity, achieved with next generation malware and attack vectors". January 2016. https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015 accessed on 30 March, 2016.

[2] ca. means Certificate Authority which is a trusted authority that issues electronic documents that verify a digital entity's identity on the internet.

[3] Marinos, Louis, Adrian Belmonte & Evangelos Rekleitis (2016). '*ENISA Threat Landscape Report 2015'*. January. https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015 accessed on 30 March, 2016.

[4] Boue, Thomas (2015). "Closing the Gaps in EU Cyber Security". *Computer Weekly.com*, June 2015. http://www.computerweekly.com/opinion/Closing-the-gaps-in-EU-cyber-security accessed on 21 March, 2016.

[5] Curtis, Sophie (2015). "British companies bombarded with cyber attacks". *The Telegraph*, 14 April 2015. http://www.telegraph.co.uk/technology/internet-security/11534709/British-companies-bombarded-with-cyber-attacks.html accessed on 18 March, 2016.

[6] Ibid.

[7] *2010 to 2015 Government Policy: Cyber Security* (2015). Policy Paper, 8 May, 2015. https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security accessed on 18 March, 2016.

[8] Ibid.

[9] *Expanding the Cyber First Programme: Speech by Matt Hancock* (2016). Cabinet Office, The Rt. Hon. Matt Hancock MP and Government Communications Headquarters. 3 March, 2016. https://www.gov.uk/government/speeches/expanding-the-cyber-first-programme-speech-by-matt-hancock accessed on 18 March, 2016.

[10] Cyber Security Strategy 2014-2017. Ministry of Economic Affairs and Communication, 2014. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Estonia_Cyber_security_Strategy.pdf accessed on 21 March, 2016.

[11] The White House, Office of the Press Secretary (2014). "*Fact Sheet: US-France Security Cooperation*". February 11, 2014. https://www.whitehouse.gov/the-press-office/2014/02/11/fact-sheet-us-france-security-cooperation accessed on 22 March, 2016.

[12] www.bsa.org "EU Cyber Security Dashboard". http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf accessed on 21 March, 2016.

[13] Ibid

[14] Csernatoni, Raluca (2016). "Time to Catch Up: The EU's Cyber Security Strategy". *European Public Affairs.eu*. http://www.europeanpublicaffairs.eu/time-to-catch-up-the-eus-cyber-security-strategy/ accessed on 5 April, 2016.

[15] Marinos, Loius (2016). "*Seven Messages to the Edge of Cyber Space*". Greece: ENISA https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015/cyber-7-seven-messages-to-the-edge-of-cyber-space accessed on 30 March, 2016.