DE JURE NEXUS LAW JOURNAL

Author:

Vatsal Agarwal

Symbiosis Law School, Noida

1st Year, BA LL.B.

INTERNATIONAL LAWS ON CYBER CRIMES- A COMPARATIVE STUDY

Abstract-

This paper is on the evolving and emerging role of cyber security in international laws. This paper is trying to discern whether cyber-crime has the qualification of being an international concern. It discusses the importance and relevance of cyber security in the international platform. And also, try to find out whether cyber-attack can be seen as an act of war on a nation. And what kind of legal action for cyber defense is being taken by different nations to protect their cyber data and cyber platforms from cyber-attacks.

Keywords- *Cyber-security, international laws, Cyber-crime, cyber-attack, Act of war, cyber defense.*

Introduction-

Cybersecurity is the state or process of preventing and recovering from cyber-attacks on computer systems, networks, devices, and applications. Assailants are employing new approaches driven by social engineering and artificial intelligence (AI) to evade standard data security protections, cyber-attacks are becoming a more sophisticated and developing threat to one's sensitive data.

Our world is more technologically dependent than ever before, and this trend shows no signs of abating. Data breaches that potentially lead to identity theft are now being shared openly on social media sites.

To safeguard the cyber space of one's nations, many countries are trying to build up a legal framework for cyber-crimes. This legal framework can be important as a measure to cybercrime can be a constructive tool in the normalization of the cyber domain as a safe environment for individuals to operate within.

European Union-

European union is a political and economic union of 27 member nations located in Europe. A standardized system of laws has been constructed to create an internal single market that applies to all member states in those, and only those, areas where the states have consented to function as one. EU policies strive to ensure free movement of people, goods, services, and money inside the internal market, pass justice and home affairs laws, and preserve common trade, agricultural, fishing, and regional development policies.

Cyber-security Act-

On June 27, 2019, the EU Cybersecurity Act (Regulation (EU) 2019/881) went into effect. It was notable since it was the first set of guidelines addressing cybersecurity certification for all European Union countries.

The purpose of this act was to accomplish two things:

1- **Establishment of the EU Cybersecurity Agency-**

The European Union Agency for Cybersecurity, ENISA, was set up as the permanent regulatory agency. It was established in 2004 and was strengthened by the EU Cybersecurity Act.

The European Union Agency for Cybersecurity supports EU cyber policy, improves the trustworthiness of ICT goods, services, and processes by cybersecurity certification schemes, collaborates with Member States and EU agencies, and assists Europe in preparing for future cyber problems. The Agency collaborates with its major stakeholders to promote confidence in the connected economy, increase the resilience of the Union's infrastructure, and, ultimately, keep Europe's society and citizens digitally secure through information sharing, capacity building, and awareness raising.

2- **Creation of a cybersecurity certification framework-**

The Regulation (EU) 2019/881 establishes and maintains the EU cybersecurity certification framework's goal of establishing and maintaining confidence and security in cybersecurity goods, services, and procedures. The goal of developing cybersecurity certification schemes at the EU level is to provide criteria for conducting conformity assessments to determine how closely products, services, and processes adhere to certain requirements. Users and service providers alike must be able to assess the security of the items, services, and procedures they purchase, make available, or use.

NIS2 Directive-

The Network and Information Security (NIS) Directive is the first piece of EU-wide legislation on cybersecurity, and its specific aim was to achieve a high common level of cybersecurity across the Member States. The Commission has submitted a proposal to replace the NIS Directive in order to strengthen security requirements, address supply chain security, streamline reporting

obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonized sanctions across the EU, in response to the growing threats posed by digitalization and the surge in cyber-attacks. The proposed expansion of the scope of the NIS2 will help to raise the level of cybersecurity in Europe in the long run by effectively requiring additional organizations and industries to adopt precautions. The subject has been assigned to the Committee on Industry, Research, and Energy in the European Parliament. On October 28, 2021, the committee adopted its report, as well as a mandate to enter into interinstitutional negotiations.

NIS2 establishes requirements for national cybersecurity capabilities among EU member states, as well as rules for cross-border cooperation and regulations for essential service providers. The provisions for business regulation in the proposed NIS2 include:

- Baseline cyber risk management measures.
- Reporting obligations.
- Remedies and sanctions for enforcement.
- An updated list of sectors and activities covered.
- Expanded coverage of midsize as well as large companies.

United States of America-

Statutory provisions-

The federal computer fraud and abuse act ("CFAA"), 18 U.S.C. 1030, is the primary statute in the United States for prosecuting cybercrime, including hacking, as well as other associated extortionate crimes, such as ransomware. Both civil and criminal punishments are included in this statute. This law makes it illegal to access a computer without permission or in excess of permission.

The electronic communications protection act ("ECPA") is another important law that applies to cybercrime. The ECPA, as amended, safeguards wire, oral, and electronic communications while they are in use, in transit, and when they are stored on computers. Email, phone chats, and data saved electronically are all covered by the Act.

State legislature-

In addition to federal laws, many states have implemented laws against hacking and other forms of cybercrime, several of which are more comprehensive than the federal laws. For example, The California Consumer Privacy Act ("CCPA") (expanded by the California Consumer Privacy Rights Act beginning in 2023) creates a data breach right of action for Californian residents with statutory penalties of $100 to $750 per consumer and per Incident if plaintiffs prove that the impacted business failed to implement reasonable security procedures to protect the personal information.

There are many other state laws regarding cybersecurity in United States like New York's SHIELD Act, requires reasonable security for personal information and specifies measures that may satisfy

that standard. Virginia and Colorado have recently passed data protection laws that require "appropriate security measures," and Massachusetts regulations have long imposed specific security requirements for personal information, such as the implementation of a written security program and the encryption of certain data.

Conclusion-

So, after briefly analyzing the cybersecurity legislature and measures of both the USA and European Union, we can see the difference between the approach and steps taken by both of them.

In the European Union case, legislation is more focused on prevention by using the best practices and certification of organizations to safeguard the data handled by them. This approach is more of a safeguard approach, where the legislation concerns itself more on prevention of harm from cybercrimes. It is also focused on the compliance of all the member states of the EU to create a secured service network across all the member states. EU Is mainly concerned with the data protection aspect of the cyber security, rather than punishment for breaches, cybercrime like cyber bullying, doxing, or another prevalent cybercrime.

On the other hand, USA's federal legislation on cybersecurity is more based on the punishment aspect of the cybercrimes. Where there are many federal laws mentioning civil and criminal liability for cybercrimes. And many of the prevention legislation which needs more elaboration and consideration of procedures are handled by the specific state's legislations, which helps in creating more protected and secured cyberspace for themselves.

So, in comparison USA cybersecurity legislation is more developed than EU in holistic manner and approach. But EU's cybersecurity law is developing with proposed legislation focusing more on securing their cyberspace from cyber-attacks and cybercrimes.