Law Journals
A Treasure Trove of Legal Knowledge.

National Journal of Cyber Security Law
Volume 1, Issue 1
www.stmjournals.com

Significance of Ever-evolving Cybersecurity Landscape: Challenges and Possible Pathways

Md. Mamun-Ur-Rashid Askari
Deputy Chief (International Cooperation Division), Bangladesh Tariff Commission, Bangladesh

Abstract

There is a growing significance of protecting cyber-threat both legally and intellectually across the globe as a consequence of everchanging science, technology and innovation world which gains urgency in cyber-security landscape. Some overarching issues like, e-commerce, Big Data Databases, Internet of Things (IoT), cyber-threat, cloud computing, cyber-crime, cyber heist, Software as a Service (SaaS), Distributed Denial of Service (DDoS), Block-chain etc., have not been properly addressed globally due to its everchanging nature and lack of global consensus. In this context, this paper seeks to find some possible pathways of ensuring cyber-security under legal and intellectual landscape. Moreover, the paper examines how different countries ensure their cybersecurity under various frameworks and strategies with a view to learning lessons from their own experiences. It also tries to examine the pros and cons of the cyber-security laws and the use of Artificial Intelligence (AI) as fight-back tool under the future cybersecurity perspective.

Keywords: *e-commerce, Big Data Databases, Internet of Things (IoT), cyberthreat, cloud computing, cybercrime, cyber heist, Software as a Service (SaaS), Distributed Denial of Service (DDoS), blockchain*

****Author for Correspondence*** E-mail: mamoon_askari@yahoo.com

INTRODUCTION

From the pen I hold, the paper I write on; to the dawning of the plane over head, everything proclaims the glorious achievements of ever-evolving science and technology. In this era of science and technology, every day we have been introduced with novel buzzwords like Internet of Things(IoT), Big Data, Artificial Intelligence (AI), cybersecurity, cybercrime, cyber heist, Software as a Service (SaaS), blockchain etc. With the ever-changing nature of technological advancement, new dimensions have been added with the existing thinking. One of such dimensions is cybersecurity which attracted greater attention to the global community due to its direct association with the downfall of different businesses and organizations. Whenever technology has increased interconnectedness with the world, the associated risks have also been multiplied manifold. It was predicted in 2016 in the 'Cybersecurity report 2017' prepared by Cybersecurity Ventures that "cybercrime will cost the world in excess of $6 trillion annually by 2021' [1]. They have also revealed that "Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades" [2]. In this context, it is crucial to explore the possible pathways though answering to the following questions:

- How does a country can handle this critical challenge?
- Is the legal framework sufficient enough to handle this issue?
- How AI can contribute ensuring future Cybersecurity?
- What are the other possible pathways to tackle Cyberattack?

In this paper it was tried to analyze the above-mentioned issues including associated facts to reduce the risk of cybersecurity which will help contribute the ease of doing business in different countries.

SIGNIFICANCE OF CYBERSECURITY

The issue of cybersecurity could be viewed from different angles such as cybercrime perspective, national and personal data security perspective, threat to human lives and vehicles

perspective, international trade perspective and above all, world peace perspective. In this paper, the security perspective and the international trade perspective have been highlighted as these two issues have been associated with the context of this paper and most of the industries, especially the financial and banking industries are directly associated with such threat of cybersecurity. 'Bangladesh Bank cyber heist' happened in February 2016, is one of the world's biggest cyber-heists that could be a good example to realize the significance of the cybersecurity in today's world. Bangladesh Bank(BB) is the central Bank of the Govt. of the People's Republic of Bangladesh. The chronological steps of the heist can be viewed as follows:

- On Feb 4, 2016, hackers attempted to draw $1.94b thru' 70 fake payment orders;
- Of the $101m transferred, $81 million sent to RCBC, Manila, $20m to Sri Lanka;
- Sri Lanka returned $20m immediately after the heist; Philippines sent back $14.54m in Nov 2016;
- Efforts are on to get back remaining $66.46m from Philippines;
- CID collecting info about 40 suspects from 8–9 countries including Philippines, Sri Lanka, China [3].

This incident has been interpreted from different viewpoints in different write-ups considering the best information available. From the investigation conducted by SWIFT, a global secure financial messaging system which was announced on 13 May 2016, it was found that:

Attackers first exploited vulnerabilities in the bank's funds transfer initiation environments. This may not have been too challenging as the Bangladesh Bank were using "cheap security devices", and "their firewalls were not functioning at full capacity as they did not have proper licenses" [4].

In accordance with the forensic experts of SWIFT:

The attackers showed sophisticated knowledge of specific operational controls within the Bangladesh Bank. Such information could have been provided by malicious insiders or gained from previous cyber-attacks that the central bank was not aware of, or a combination of both [5].

On the other hand, Bangladesh Banks did not accept SWIFT's claim rather their probe "report shows an analysis of how SWIFT was responsible for the cash flowing out of the BB's account with the Federal Reserve Bank of New York" [6]. Moreover, this report also claims that "SWIFT will never be able to evade its responsibility. But we have to solve our future problems with the help of SWIFT" [7].

A careful analysis reveals that there was lacuna both in case of the system of Bangladesh Bank as well as in the SWIFT system. Besides lack of appropriate knowledge and efficiency including legal loopholes might be some of the focus points for the attackers. Truly speaking, no organisation in today's world is safe from such cyberattacks. It was revealed in the 'Cybersecurity report 2017' as, "Cybercrime is the greatest threat to every company in the world, and one of the biggest problems with mankind; the impact on society is reflected in the numbers" [8].In this context, Shihab Uddin Khan, associate professor at the Bangladesh Institute of Bank Management(BIBM) conducted a research study titled 'Review of IT Operations of Banks in Bangladesh 2016' expressed that "Some 16% banks mentioned that the current situation of cyber security is not enough to prevent any virtual or physical damage to information management system, perceiving the highest risk" [9, 10].In this study, it was also opined that "A total of 52% banks in the country are at high risk of cyber security" [11].He has also viewed that "Of the banks, 16% are at a very high risk and 36% at high risk" [12]. But this is not only the scenario of only Bangladesh but also most of the developing and least developed countries are prone to such kind of cyber-attack as we have seen in the 'Cybersecurity report 2017'. But, it is wise to accept the fact and try to find best possible existing solutions under both domestic and international legal perspective as well as security policy and strategic perspective. Realizing the fact SWIFT enters a new cybersecurity framework that must have to be complied by the users of SWIFT from 1 January 2018 [13]. SWIFT has taken some security control measures for instance "incident response, security awareness training, multi-factor authentication and anomalous behaviour detection" [14]. They

have also realized the fact that loopholes in a single bank under SWIFT could be disruptive for the whole SWIFT system which may lessen their global image. Steven Grossman, Bay Dynamics VP of Strategy highlighted:
"SWIFT has a responsibility to establish the standard for transacting on its network. Just one bank having lax security controls in place lowers the bar and elevates cyber risk for everyone else who uses the platform. The framework affects banks of all sizes that vary in cyber maturity levels in developed and underdeveloped countries" [15].

After the heist, Bangladesh Bank also took some initiatives as security measures and Govt. of Bangladesh placed the 'The Digital Security Bill, 2018'in parliament on April 2018 after cabinet's approval [16]. According to the proposed law, "If anyone illegally enters any critical information infrastructure, he or she will be sentenced to maximum 7 years' imprisonment or be fined by Tk 25 lakh or by both" [17]. This is just the beginning this law may need future amendment to tackle new issues of cyberspace.

Trade Perspective

Cybersecurity is causing extra burden for the business sectors, especially the financial and banking sectors, but other organizations like health, energy and transports are also not safe from cyberattacks in recent days. A recent forecast by Gartner can be seen where it was predicted "Cybersecurity spending will grow from $86.4 billion in 2017 to $93 billion in 2018" [18].It can be assumed from the forecast that cyberattack will become a great concern for all in the near future as it may change its patterns of attack like the Hydra, a mythological character about which the myth goes that if one of the heads of a hydra is cut off then two or more grow back immediately. Chief Security Scientist of Thycotic, Joseph Carson agrees with this estimate of Gartner:
I believe that the actual number will be much higher given that many aggressive regulations will come into enforcement in 2018, including the EU General Data Protection Regulation (GDPR). This will force many companies to increase spending on information security and response to avoid becoming either victims or receiving massive financial fines for failure to protect and secure [19].

In favour of his argument, Carson mentioned two recent Cyberattacks: *Not Petya* and *Wanna Cry* [20]. He agrees with the fact that these attacks are occurring huge financial losses. It is interesting to note that in case of international trade, people are rushing to reduce the cost of doing business while cyberattacks are causing extra cost burden which is directly affecting international trade. Another impact is that in case of least developed and developing countries which have recently flourishing their e-commerce may have become the victim of such cyberthreat. This is also a threat for the consumers of such countries as they have just started trusting online transaction which affects e-commerce business negatively. As the threat landscape is changing its forms and patterns, the need for ensuring cybersecurity is also essential. Chief Security Strategist at AsTech, Nathan Wenzler emphasized,

If we watch how the trend of attacks has gone over the past several years, we see more and more criminals moving away from targeting servers and workstations, and toward applications and people. As an industry, we have gotten better and better about protecting devices, but now the focus has to turn to other assets, and thus, the increase in spending Gartner is forecasting in DevOps and services. Essentially, wherever the criminals go, corporate spending is soon to follow [21].

Security Perspective

The cyber threat landscape is changing every day as if every morning we are listening to the story of novel forms of cyberattack. In this situation, for security reasons, no organization should depend only on the same trusted techniques years after years for ensuring protection against newer threat as the hackers can explore new ways in every attack. In the recent years, the sophistication of different attacks has been increasing alarmingly which is a cause of greater concern for industry security as well as private data and national security. In this context, Digital Manager at *Atlantic.Net* Brady Keller states:
The multi-million dollar ransomware industry has grown and will continue to grow with amazing speed in the years to come, … the spread of untraceable cryptocurrency such as Bitcoins and the proliferation of ransomware

kits on the dark web, which allow anybody, even script kiddies with no programming skills, to put together and reap the financial rewards of ransomware attacks.

Ransomware is increasingly targeting organizations in the financial and healthcare industries. These organizations often have thousands or even tens of thousands of gigabytes of customer/patient data they cannot afford to lose, which makes them all the more willing to pay handsomely to get their data back at any cost [22].

In this context, remarks of Carl Herberger, VP of security at *Radware* can be cited as:
The top challenge for cybersecurity isn't preventing data breaches, stamping out ransomware, or preventing ever-more-massive DDoS attacks, it is securing our digital privacy. 2017 and the years to come will dictate the future of cybersecurity, and most importantly human privacy. Digital threats have evolved quickly and can wreak havoc on our lives, endangering our personal privacy and the privacy of those around us [23].

We need to tackle this significant issue by any means. The national government can take initiatives to protect people's digital privacy. But is it easy to protect private data? In recent times, people have become interconnected with so many sites. Which site is violating their rights, and which are not? Can private data protection be treated as a human right? These questions are not easy to answer, and these issues are not easy to handle specially for developing and LDCs. Carl Herberger agrees with the fact that "It needs to protect each and every citizen and hold those who might put our privacy in jeopardy accountable for their actions. This will be the most important cybersecurity decision in the next year and it will shape the security landscape for years to come" [24].

THE LEGAL LANDSCAPE OF CYBERSECURITY

3.1 Developed countries enacted cybersecurity legal framework many years back. For instance, "The United States' privacy system is arguably the oldest, most robust and effective in the world" [25]. Inspite of having robust regulatory framework,

The number of data breaches in the US increased from 157 million in 2005 to 781 million in 2015, while the number of exposed records jumped from around 67 million to 169 million during the same time frame. In 2016, the number of data breaches in the United States amounted to 1093 with close to 36.6 million records exposed [26].

But due to the nature of recent cyberattacks, some of the countries are updating their legal frameworks. But developing countries including least developed countries are lagging as they have just started facing newer challenges and enacting new laws to fight against those cyberattacks. As an example, recent initiative of Bangladesh to enact the Digital Security Bill, 2018 can be mentioned.

Legal Landscapes in Some Selected Countries

To give an overview of the legal landscapes of some selected countries we have considered three countries: Australia(Developed), India(Developing) and Bangladesh (Least Developed).Under the framework of the Global Cybersecurity Agenda, ITU provides its 193 Member States' 'Cyberwellness profiles' with a view to giving an indication of the member states' [27],levels of cybersecurity progress built on the five pillars of the cybersecurity agenda namely: legal measures, technical measures, organisation measures, capacity building and cooperation including child online protection [28].It was also expected by the ITU that these profiles will help tackling cybersecurity challenges as well as opportunities. Information of these three countries has been retrieved from ITU's 'Cyberwellness Profiles' which have been analysed in Table 1. From the table it is evident that Australia as a developed nation has already progressed a lot to fight back cyberattacks while India as a developing nation has progressed less and Bangladesh is running at a slower pace. It is also evident from the profile that the data used in these profiles are not updated. In the meantime, these countries' cybersecurity profile might have changed a lot. It is also evidenced that there is less interaction of the member states of the ITU regarding the data updates. Australia has progressed developing an integrated

approach while India and Bangladesh are lagging in this context [29].

In case of technical measure like Standard, Australia has its own cyber security standard whereas India uses Information Security Management System (ISMS) Standard ISO 27001 and Bangladesh does not follow any officially recognised standard [30]. Regarding Certification, Australia follows 'The Emanation Security Program' accountable for 'certification and accreditation of national agencies and public-sector professionals' [31], while India and Bangladesh "do not have any officially approved national or sector specific cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals [32]". In case of organizational measures, such as policy perspective, Australia has "officially recognized the National Plan to Combat Cybercrime and the Cyber Security Strategy as the national strategy" whereas India has 'Officially recognized National Cyber Security Policy (NCSP)' [33] and Bangladesh does not have an officially recognized national cybersecurity strategy. Regarding roadmap for governance, Australia and India have the national governance roadmap for cybersecurity while Bangladesh does not have any roadmap, but initiatives were taken for the roadmap by the competent authority.

Table 1: *Cyberwellness Profiles of Australia, India and Bangladesh.*

S. No.	Type of Measures	Measures Name	Country		
			Australia	**Bangladesh**	**India**
1.	Legal Measures		• Cybercrime Legislation Amendment Act 2012; • National Plan to Combat Cybercrime; • Australian Communications and Media; • Authority (ACMA) enforces the Spam Act; • Australian Cybercrime Online; • Reporting Network; • Data breach notification.	• Information and Communication Technology Act; • Bangladesh Telecommunication Regulation Act; • Bangladesh Penal Code.	• The Indian Penal Code; • Information Technology Act;
2.	Technical Measures	CIRT (Computer Incident Response Team)	• Computer Emergency Response Team(CERT) Australia; • Cyber Security Operations Centre (CSOC);	• BDCERT	• CERT-IN
		Standard	• The Australian Signals Directorate (ASD); • Australian Government Information Security Manual;	• Does not have any officially recognized national (and sector specific) cyber-security frameworks for implementing internationally recognized cybersecurity standards.	• Implementation of Security policy in accordance with the Information Security Management System (ISMS) Standard ISO 27001. • The Five-Year Plan on Information Security also states guides on standards.
		Certification	• The Emanation Security Program is responsible for the framework for certification and accreditation of national agencies and public - sector professionals.	• Bangladesh does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public-sector professionals.	• India does not have any officially approved national or sector specific cybersecurity frameworks for the certification and accreditation of national agencies and public - sector professionals.

3.	Organization Measures	Policy	• Australia has officially recognized the National Plan to Combat Cybercrime and the Cyber Security Strategy as the national strategy.	• Bangladesh does not have an officially recognized national cybersecurity strategy.	• India has an officially recognized National Cyber Security Policy (NCSP).
		Roadmap for Governance	• Tahe national governance roadmap for cybersecurity is elaborated in the National Security Information Environment Roadmap: 2020 Vision.	• Bangladesh does not have a national governance roadmap for cybersecurity in Bangladesh. However, there are efforts from the Honorable Prime Minister's office, Bangladesh Computer Council and the Telecommunication Regulatory Commission (BTRC) to finalize a roadmap to ensure cybersecurity.	• India has a national governance roadmap for cybersecurity through the Five-Year Plan on Information Security.
		Responsible Agency	• The following are the officially recognized agencies responsible for cybersecurity in Australia: - The Cyber Policy and Intelligence Division - The Attorney-General's Department - The Department of Prime Minister and Cabinet - The Australian Signals Directorate.	• Bangladesh does have an officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.	• The Department of Electronics and Information Technology and Ministry of Communications and Information Technology are the officially recognized agencies responsible for implementing a national cybersecurity strategy, policy and roadmap.
		National Benchmarking	• Federal Government entities subject to the Public Governance, Performance and Accountability Act2013 participate in annual benchmarking of their ICT activities	• Bangladesh does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.	• As a means of benchmarking and referential to measure cybersecurity development, security auditors have been empanelled to conduct security audits including vulnerability assessment, penetration testing of computer systems and networks of various organizations of the government, critical infrastructure organizations and those in other sectors of the Indian economy.

Source: *Author's Compilation from ITU's Cyberwellness Profiles*

AI AS A TOOL FOR ENSURING CYBERSECURITY

If the experts were asked: What would be the future of cybersecurity landscape? the answer would obviously be AI-based cyber-security. Nick Hastreiter shows in his article titled "How AI and Blockchain Will Shape the Future of Cybersecurity", that the question is not easy to answer as we are entering an entirely new kind of cyber threat regularly [34]. In this connection, he tries to present some experts opinions in his article. Of those, the forecast of Ondrej Vlcek, CTO and GM (Consumer) of Avast, a Czech multinational cybersecurity software company could be mentionable:

In 10–15 years, we will be deep in a 'war of the machines' era with advances in artificial intelligence bringing fast and sophisticated execution of security defence and cybercrime. This will be a battle of AI vs. AI [35].

He is also of the view that due to the availability of lower cost computer equipment as well as 'off-the-shelf machine learning algorithms', 'AI code and open AI platforms' will increase the possibility both for good and bad guys in the realm of AI [36]. The conflicts will start here which might start sophisticated attacks in a quicker and intelligent manner with a few human interventions [37] He also predicted that:
Cybercriminals will create fully autonomous, AI-based attacks that will operate completely independently, adapt, make decisions on their own and more. Security companies will counter this by developing and deploying AI-based defensive systems. Humans will simply supervise the process [38].

Another novel issue is the blockchain which is interconnected with the future cybersecurity. A continuously growing list of records is called blocks creates a blockchain which are linked and secured through using cryptography [39] For an example, the Bitcoin system is considered as the first blockchain. Konstantinos Karagianni, CTO of BT states that:
Blockchains are moving from the realm of just fuelling cryptocurrencies like Bitcoin to providing smart contracts, identity management, and multiple ways of proving integrity of data. They may also hold the key to defending against IoT attacks.AI will be used to identify hacking flaws and patch them to stay ahead of malicious attackers [40].

AI is the simulation of human intelligence by machines through intelligent computer programs. It seems like the world of science fiction. AI's relevance today lies in the interesting trends included in it like machine vision, cognitive prostheses, and robotic scientists which are also relevant to futurist goals. 'The Policeman's Beard is Half Constructed' is the first book (a collection of prose and poetry) published in 1984 which is written by Racter, an AI based computer program that is capable of generating English language prose randomly. AIs are not only producing patentable products, they have also started producing potential copyrightable and cryptographic works like newspaper articles, songs, poems and books, remotely piloted vehicle which are obviously creative and artistic in nature. 'Flow Machines' developed by a Sony researcher is capable of composing music, even some other machines like 'Mubert' which has been claimed as the world's first online music composer that can continuously produce music in real time [41].

Not only that, automobile industries have started using AI and using the concept 'driverless cars'. According to a research from analysts IHS:
In 2015, the install rate of AI based systems in new vehicles was just 8%; this number is expected to soar to 109% in 2025. This is because different kinds of AI systems will be installed in vehicles [42].

IHS believes that the use of AI is likely to be increased dramatically in operating different applications operating vehicles over the next decades and beyond [43] This analysis also suggested that "unit shipments of AI systems for infotainment and advanced driver assisted systems (ADAS) are expected to rise from seven million in 2015 to 122 million by 2025" [44]. With this rise of AI some tech giants and automobile leaders such as Tesla and Google started spending huge amount of money for research study towards finding technological solution for the 'commercial autonomous cars' [45]. Recent advancement shows that "Ford Motor Company made an investment of one billion dollars in Argo AI, a new AI company to bring forth a virtual driver system in the future, possibly by 2021" [46].

Researchers and scientists are optimistic enough that AI will redesign the global future healthcare system. With the immense potential of AI, the future healthcare system will become a better one where it would be possible to prepare overall treatment plan, finding best suited method of treatment for the patients. Considering this potential of AI in healthcare, tech giants such as IBM or Google have invested in the field of patient data mining. Some other good examples include *Google Deepmind Health*, 'used to mine medical records in order to provide better and faster health services' [47], *IBM Watson Paths*, 'expected to help physicians make more informed and accurate decisions faster and to

cull new insights from electronic medical records (EMR)' [48], and *Careskore*, 'A cloud-based predictive analytics platform for health systems and physician organizations' [49].

REGIONAL EXPERIENCE

EU Cybersecurity Initiatives

With a view to ensuring a more secure online environment, the EU cybersecurity strategy was adopted in 2013 [50]. In addition, they have adopted some legislative proposals especially in connection with the network and information security through taking cybersecurity projects worth €600 million during 2014–2020 [51]. They have also strengthened their approach through including cybersecurity at the centre of their political priorities. Trust and security became the heart of the 'Digital Single Market Strategy' which was presented in May 2015 [52]. Fighting against the cybercrimes is one of the important pillars of the agenda on security. Another important milestone is 'the Directive on security of network and information systems (NIS Directive) adopted in July 2016boostingcybersecurity and tackling cyberthreats [53]. In the EU, the cybersecurity is significant for many reasons. Digital technologies created the backbone of the EU's economy over the past years. EU's business services have been interconnected by different network services which provide the 'uninterrupted availability of the internet and the smooth functioning of information systems' [54]. In this context, any cybersecurity incident whether it be accidental or intentional could disrupt the whole system. They have assumed that "By completing the Digital Single Market, the EU could boost its economy by almost €415 billion per year and create hundreds of thousands of new jobs" [55].

Ensuring cybersecurity, the key objectives of the commission are as follows:

a) Increasing cybersecurity capabilities and cooperation;
b) Making the EU a strong player in cyber-security; and
c) Mainstreaming cybersecurity in EU policies [56].

With these three objectives, the EU tries 'to bring cybersecurity capabilities at the same level of development in all the EU Member States', 'nurturing its competitive advantage' and 'to embed cybersecurity in the future EU policy initiatives' [57].

Measures Taken to Strengthen Cybersecurity

The key measures taken by the commission are as follows:

EU Cybersecurity Strategy (2013)

This strategy has been taken by the Commission and the European External Action Service in 2013, with a view to guiding the EU actions such as fundamental online rights, internet access, online protection etc. under this domain. With this aim five priority areas have been set [58]:

a. Increasing cyber resilience;
b. Drastically reducing cybercrime;
c. Developing EU cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP);
d. Developing the industrial and technological resources for cybersecurity;
e. Establishing a coherent international cyberspace policy for the EU and promote core EU values;

European Agenda on Security (2015)

Effectively fighting against cybercrime is one of the three priority areas under 'the new European Agenda on Security 2015–2020' adopted in April 2015. It was felt by the commission that a coordinated response is required to fight against at European level. In this connection, the agenda on security, the following actions have been set [59]:

i. Giving renewed emphasis to implementation of existing policies on cybersecurity, attacks against information systems, and combating child sexual exploitation;
ii. Reviewing and possibly extending legislation on combating fraud and counterfeiting of non-cash means of payments to take account of newer forms of crime and counterfeiting in financial instruments, with proposals in 2016;
iii. Reviewing obstacles to criminal investigations on cybercrime, notably on issues of competent jurisdiction and rules on access to evidence and information; and

iv. Enhancing cyber capacity building action under external assistance instruments.

Digital Single Market Strategy (2015)

Keeping in mind that trust and security are vital for making digital economy beneficial, the Digital Single Market Strategy was presented in May 2015 that includes a Public Private Partnership (PPP) on cybersecurity which was officially signed on 5 July 2016 by the Commission and the European Cyber Security Organization (ECSO) [60].

EU Legislation Directive on Network and Information Security

A directive on security of network and information systems commonly known as 'NIS Directive' was proposed in 2013 by the Commission which aims at ensuring 'a high common level of cybersecurity in the EU' [61]. On 6 July 2016, this directive was adopted by the European Parliament which entered into force in August 2016. The three key pillars on which the directive was built are as follows [62]:

a) Ensuring Member States preparedness by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority;
b) Ensuring cooperation among all the Member States, by setting up a 'Cooperation Group', in order to support and facilitate strategic cooperation and the exchange of information among Member States, and a 'CSIRT Network', in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks;
c) Ensuring a culture of security across sectors which are vital for our economy and society, and moreover, rely heavily on information and communications technologies (ICT). Businesses with an important role for society and economy that are identified by the Member States as operators of essential services under the NIS Directive will have to take appropriate security measures and to notify serious incidents to the relevant national authority. These sectors include energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Also, key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive. Similar requirements already apply to telecom operators and internet service providers through the EU telecoms regulatory framework.

Legislative Actions to Fight Cybercrime

There are some EU legislative actions in place towards fighting against cybercrimes in the EU including [63]:

a) 2013: A Directive on attacks against information systems, which aims to tackle large-scale cyber-attacks by requiring Member States to strengthen national cybercrime laws and introduce tougher criminal sanctions. This Directive had to be implemented by Member States by September 2015 and the Commission is currently checking implementation. Five infringement procedures for partial or noncommunication have been launched in December 2015. An implementation report will be published in 2017.
b) 2011: A Directive on combating the sexual exploitation of children online and child pornography, which better addresses new developments in the online environment, such as grooming (offenders posing as children to lure minors for the purpose of sexual abuse). This legislation had to be transposed by 2013, and the Commission is currently verifying implementation. Two reports on implementation were issued at the end of 2016.
c) 2001: Framework decision on combating fraud and counterfeiting of non-cash means of payment, which defines the fraudulent behaviours that EU States need to consider as punishable criminal offences. The Commission is assessing the need to revise this framework decision to cover new forms of money transmissions like virtual currencies and other aspects, with a plan to come forward with any new initiative for the first quarter of 2017.

Networks/Organisations

The European Union Agency for Network and Information Security (ENISA) was set up in 2004 to contribute to the overall goal of ensuring a high level of network and information security within the EU.ENISA helps the Commission, the Member States and the business community to address, respond and especially to prevent NIS problems. The main activities run by ENISA include [64]:

a) Collecting and analysing data on security incidents in Europe and emerging risks;
b) Promoting risk assessment and risk management methods to enhance capability to deal with information security threats;
c) Running of pan-European cyber exercises;
d) Supporting Computer Emergency Response Teams (CERTs) cooperation in the Member States; and
e) Awareness-raising and cooperation between different actors in the information security field. In order to boost the overall level of online security in Europe, the agency organises each October the Cybersecurity Month awareness campaign, with the support of NIS contact points in all Member States.

The EU Computer Emergency Response Team

The EU Computer Emergency Response Team (CERT-EU) was established in 2012, aiming to deliver effective response to the incidents related to information security and cyber threats for all the organisations in the EU. This team was composed of the 'security experts in the core team of CERT-EU, together with experts from the General Secretariat of the Council, the European Parliament, the Committee of the Regions and the Economic and Social Committee' [65].

The Europol's Cybercrime Centre (EC3)

In 2012, this centre was set up as an integral part of Europol. It acts as a focal point to combat and prevent cross-border cybercrime through:

a. Serving as the central hub for criminal information and intelligence;
b. Supporting Member States' operations and investigations by means of operational analysis, coordination and expertise;
c. Providing strategic analysis products;
d. Reaching out to cybercrime related law enforcement services, private sector, academia and other non-law enforcement partners (such as internet security companies, the financial sector, computer emergency response teams) to enhance cooperation amongst them;
e. Supporting training and capacity building in the Member States;
f. Providing highly specialised technical and digital forensic support capabilities to investigations and operations; and
g. Representing the EU law enforcement community in areas of common interest (R&D requirements, internet governance and policy development) [66].

EU Funding Research and Innovation

During the 2007–2013 period, the EU invested €334 million in cybersecurity and online privacy projects [67]. Topics such as trustworthy network and service infrastructures, cryptology and advanced biometrics were addressed under the 7th Framework Programme (FP7) and the Competitiveness and Innovation Programme (CIP) [68]. During the same period, the Security Research theme of FP7 invested €50 million in cybercrime projects addressing topics like the economy of cybercrime, risk analysis for infrastructure protection, money laundering and dedicated road mapping actions [69].

The African Union (AU)

The necessity for the promotion of cybersecurity in the AU was first found on a study on the harmonization of telecommunication, and information communication technology policies and regulation (2008) [70] which addressed the emerging questions "tracing and combating of cybercrime in all its forms (hacking, virus propagation, denial of service attacks, credit card fraud, etc.)" [71].This study also highlighted the necessity for establishing a harmonized regional policy and legal framework on cyber security. After that in 2011, a draft framework on cybersecurity 'Draft Convention for the Establishment of a Credible Legal Framework for Cybersecurity in Africa' was developed by the AU and the Nations Economic Commission for Africa (UNECA) [72] However, the draft convention

was not presented for the AU's adoption in January 2014 due to the opposition from the academia and the civil society claiming some concerns for 'the right to privacy and freedom of expression' [73]. After a long debate on the issues, the AU Convention on Cyber Security and Personal Data Protection, EX.CL/846(XXV) was adopted in the 23rd Ordinary Session of the Assembly of the African Union (Malabo, 27th June 2014) [74].Regarding the International Cooperation within AU Cybersecurity Framework Article 28 of the AU Cyber Security Convention provides with some provisions with a view to facilitate international cooperation on cyber security which has been stated in Article 28 as: "State parties shall ensure that the legislative measures and/or regulations adopted to fight against cyber-crime will strengthen the possibility of regional harmonization of these measures and respect the principle of double criminal liability" [75].

Economic Community of West African States (ECOWAS)

The directive of the ECOWAS on fighting cybercrime was adopted in August 2011by the ECOWAS Council of Ministers (C/DIR.1/08/11) at its 66th ordinary session at Abuja [76]. The directive obliged members to establish a framework for the facilitation of international cooperation regarding cybersecurity. In this context article 33(1) of this directive states:
Where Member States are informed by another Member State of the alleged commission of an offence as defined under the Directive, such Member States shall cooperate in the search for and establishment of that offence, as well as in the collection of evidence pertaining to the offence [77].

In addition to that the directive also provides that "such cooperation shall be carried out in line with relevant international instruments and mechanisms on international cooperation in criminal matters" [78]. Applicable ECOWAS instruments on international cooperation include: the ECOWAS Convention on Mutual Assistance in Criminal Matters and the ECOWAS Convention on Extradition [79] "The ECOWAS Convention on Mutual Assistance in Criminal Matters establishes a broad framework for the rendition of mutual assistance amongst ECOWAS States where there is an absence of applicable international agreement between them on the basis of a reciprocal legislation" [80]. Under the Convention, Member States are required to afford each other "the widest measure of mutual assistance in proceedings or investigations in respect of offences the punishments of which, at the time of the request for assistance, falls within the jurisdiction of the judicial authorities of the requesting Member State" [81].

The COMESA Model Cybercrime Bill

In October 2011, the COMESA established a Model Cybercrime Bill to provide a uniform framework that would serve as a guide for the development of cyber-crime laws in Member States, however, the Bill does not establish any binding obligations on Member States to criminalize cyber-crimes [82]. The Bill largely adopts the language and model of legal instruments such as the Council of Europe Convention on Cybercrime and the ITU Toolkit for Cybercrime Legislation. It also establishes an elaborate guide for the development of general framework to facilitate international cooperation, extradition, and mutual assistance [83] However, despite its framework on international cooperation, the Bill only serves as a mere guide or model for development of national cyber security laws in Member States. Thus, the Bill does not establish any international cooperation obligations on Member States and neither can it be used as a legal instrument for cooperation amongst Member States.

The SADC Model Law on Computer Crime and Cybercrime

The model law on computer crime and cybercrime was adopted in March 2012 by the Southern African Development Community (SADC)with a view to serve as the development guide of cyber security laws in the Member States [84]. However, no obligation was imposed on Members to set up cybercrime laws. It does not have any provision for establishing international cooperation among the Member States and nor it does have any international cooperation obligations on Member States. Rather, it was established that Member States may introduce

cyber security laws based on 'the SADC Protocol on Mutual Legal Assistance in Criminal Matters and the Protocol on Extradition' for obtaining international cooperation from other Member States. Within this SADC Protocol on Mutual Assistance, it is a requirement for the Member States to provide each other with "the widest possible measure of mutual legal assistance in criminal matters" [85].

GLOBAL INITIATIVES TO FIGHT-BACK CYBERTHREAT

Consensus on Cyber Security

- The need for global consensus was felt many years back to fight against cyberattacks. It was also felt by different experts that the significance of countries collaboration to counter cybercrime globally. The group president of the 'Information Technology and Services Group at Symantec' David Thompson, invited all to take part in International Multilateral Partnership against Cyber Threats (IMPACT), the first United Nations-backed cybersecurity alliance. He also felt the necessity of the public-private partnership towards combating global cyberterrorism [86].
- Based in Cyberjaya, Malaysia the International Multilateral Partnership against Cyber Threats (IMPACT) is acting as International Telecommunication Union's (ITU) cybersecurity executing arm. IMPACT delivers ITU's Members (193) to access technical know-how and resources including services towards effectively addressing cyberthreats. In Geneva, Switzerland during the World Summit of the Information Society (WSIS) on 20 May 2011, a historic agreement was signed between the ITU and the IMPACT. IMPACT's Global Response Centre (GRC) is a vital cyberthreat resource centre for the member states as well as for the global community that provides emergency responses for facilitating identification of cyber threats [87].
- To keep the cyber space ecosystem safe, a large number of standards organizations are playing vital role which includes: "the International Telecommunications Union (ITU), the International Criminal Police Organization (INTERPOL), the International Multilateral Partnership against Cyber Threats (IMPACT), the European Commission and the European Network and Information Security Agency (ENISA), and technical groups like the Internet Engineering Task Force (IETF)" [88].They should realize that this challenge is a global challenge and together everyone should come forward to fight back such cyberattacks through mutual consensus.

Challenges for Global Consensus

Analysing the facts and discussions mentioned in this paper, it can be assumed that there is no globally accepted effective cyber security strategy or mechanism or forum due to divergence of players in the field of cyber security who have different types of interest. Ensuring security is obviously a business, but at the same time, it is a global challenge as the attackers might be anonymous. Hence, it is difficult for a single country or a single business entity to fight back an array of hackers. The World Trade Organisation (WTO) has just taken consideration to discuss the issues of e-Commerce in the 11th Ministerial Conference held from 10 to 13 December 2017 in Buenos Aires, Argentina. There was no specific decision taken except the decision to continue discussions on 1998 work programme. In addition, a separate declaration by 45 members was taken to initiate pluri-lateral discussion on e-commerce. In this future discussion**,** the issue of cyber security could be addressed as this is a big forum of 162 members which is directly or indirectly related to e-commerce.

POSSIBLE PATHWAYS

Considering the above analysis and discussions, it reveals the fact that ensuring cybersecurity is a common global problem. It can and should be tackled both legally and intellectually. The possible pathways for the common global problem can be summarised as follows:

Legal Pathways

This is evident from the above facts and findings that every country should enact or update their legal framework for the protection of private and public data theft or hacked. Besides, coordinated policy should also be framed to fight against such attacks.

Regional Approach
As the nature of the cyberspace landscape, the challenges may be tackled through regional approach used by COMESA, SADC, AU or the EU. Considering the loopholes of these existing regional approach new regional approach could be framed that would be more effective. Bangladesh and India may consider such approach.

Multilateral Approach
The functionality of the existing multilateral framework under IMPACT could be revisited to make it more effective. Besides, multilateral framework under WTO could be an alternative option for future negotiations. In addition, WTO and IMPACT can sit together to address this issue under common platform.

AI Based Approach
This approach is good for fighting against future attack. But considering the huge cost of the usage of AI, developing countries and LDCs will be less attentive to this approach. But for obvious reasons there won't be any alternative for the developed country to avoid the use of AI to tackle future cyberattacks.

Public-Private Partnership
There is no alternative to public-private partnership towards combating global cyberterrorism. The global research organisations should come forward under the same umbrella to combat cyberterrorism globally under multilateral platform.

CONCLUDING REMARKS

Considering the nature and pattern of cyberattacks in recent times, it can be assumed that an effective cybersecurity mechanism requires the involvement of multiple stakeholders both at domestic and international level such as governments, private organisations, public organisations, think tanks, regional and multilateral forum etc. Existing multilateral forums like the WTO could incorporate these issues in its agenda. Moreover, the area of cooperation and effectiveness of IMPACT should be increased. Sometimes legal approach is fruitful, sometimes bilateral, regional or multilateral approaches are more effective to face the challenges of cyberthreat. But, there is no denying the fact that a coordinated approach is more effective than other approaches for mitigating those cyberthreats as the cyberspace is an interconnected arena which is beneficial for the individuals, institutions, organisations and nations. But it should be kept in mind that this space is also an anchorage for the criminals. So, if the countries with the common interests fail to understand the necessity of working together then they will place private data, national data and economic asset security at risk. Moreover, the future threat of cybersecurity could also be well-managed as AI has unimaginable potential which needs to be addressed both legally and intellectually. Researchers predicted that the AI may control the whole diaspora of human lives within a few couple of years. If machines become more intelligent than human being, there is growing apprehension that humans would be slaves to the machines. Thus, AI may pose an existential threat to humanity under cyberspace. If we fail to control it, someday it will control us, or even destroy us like the Frankenstein's monster. There is a growing need to integrate the philosophies of the East and those of the West and to seek answers to the fundamental questions of our existence here on this planet. Stephen Hawking puts it: "The short-term impact of AI depends on who controls it; the long-term impact depends on whether it can be controlled at all" [89]. Considering the importance of the new thinking on AI's creation and Hawking's prediction the world community should deeply ponder over the Cyberthreat issue as well as AI's involvement in it before it's too late. As AI becomes harder to distinguish from human creativity, the legal questions relating to the control of AI are bound to become more complicated in the years to come. Therefore, this new thinking on the war between AI vs. AI in the cyberspace reveals the fact that now is the ripe time to start a constructive dialogue on the cybersecurity with added AI's involvement to control unintended consequences through proper regulation. Prevention is better than cure. It can be summed up by saying that there is need for global consensus to effectively fight against cyberattacks across the globe.

REFERENCES

1. Steve Morgan, Menlo Park. Cybersecurity Ventures Official Annual Cybercrime Report. 2017. <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>.
2. Ibid.
3. Rejaul Karim Byron, Tuhin Shubhra Adhikary, Rafiul Islam.*BB Still Waits to Get Back $66m in Stolen Money*. Bangladesh:The Daily Star; 2018.<https://www.thedailystar.net/frontpage/bb-still-waits-66m-stolen-money-1529089>.
4. Md Nur Nurdianah.*Cybersecurity Lessons from the Bangladesh Bank Heist*. MIS Asia; 2017.<https://www.mis-asia.com/tech/industries/cybersecurity-lessons-from-the-bangladesh-bank-heist/>.
5. Ibid.
6. Staff Correspondent.*Govt Probe Hints at BB Officials' Links*. Bangladesh: The Daily Star; 2016. <https://www.thedailystar.net/backpage/govt-probe-hints-bb-officials-links-1232086>.
7. Staff Correspondent.*Govt Probe Hints at BB Officials' Links*.Bangladesh: The Daily Star; 2016. <https://www.thedailystar.net/backpage/govt-probe-hints-bb-officials-links-1232086>.
8. Morgan and Park.
9. Shariful Islam.*Most Banks at High Cyber Risks*. Dhaka: Tribune; 2017.<https://www.dhakatribune.com/business/banks/2017/05/05/banks-high-cyber-risks/>.
10. Ibid.
11. Ibid.
12. Ibid.
13. Madhvi Mavadiya.*SWIFT and the New Regulatory Environment of 2018*. Forbes; 2017. <https://www.forbes.com/sites/madhvimavadiya/2017/12/11/swift-new-regulation-2018/#19530a4578fd>.
14. Ibid.
15. Ibid.
16. Online Desk. Cabinet Okays Draft of 'Digital Security Act 2018. *2018-01-29, Daily-Sun.com.*Bangladesh: The Daily Sun; 2018.<http://www.daily-sun.com/post/285365/Cabinet-okays-draft-of-'Digital-Security-Act-2018'>.
17. Ibid.
18. Tony Bradley.*Gartner Predicts Information Security Spending to Reach $93 Billion in 2018*. Forbes; 2017. <https://www.forbes.com/sites/tonybradley/2017/08/17/gartner-predicts-information-security-spending-to-reach-93-billion-in-2018/#3edac2b3e7f1>.
19. Ibid.
20. Ibid.
21. Ibid.
22. Nick Hastreiter.*How AI and Blockchain will Shape the Future of Cybersecurity*. Future of Everything; 2018.<https://www.futureofeverything.io/future-of-cybersecurity/>.
23. Ibid.
24. Ibid.
25. *A Glance at the United States Cyber Security Laws - Appknox. Mobile App Security, Resources, Best Practices News*<https://blog.appknox.com/a-glance-at-the-united-states-cyber-security-laws/>.
26. Ibid.
27. *Cyberwellness Profiles*. ITU; 2018.<https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx>.
28. Ibid.
29. Ibid.
30. Ibid.
31. Ibid.
32. Ibid.
33. Ibid.
34. Hastreiter.
35. Ibid.
36. Ibid
37. Ibid.
38. Ibid.
39. Valentina Gatteschi,*et al*. Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough? *Future Internet*. 2018; <http://www.mdpi.com/1999-5903/10/2/20>.
40. Hastreiter.
41. *Flow Machines: AI Music-Making*. European Research Council <http://www.flow-machines.com/>.
42. Sunu Philip.*5 Ways Artificial Intelligence is Driving the Automobile Industry*. Crayon Data Resource; 2018.<http://bigdata-madesimple.com/5-ways-artificial-intelligence-is-driving-the-automobile-industry/>.
43. *Vehicles Using Artificial Intelligence Will Play an Increasing Role in the Future of Smart Cities*. Gemalto; 2016.<https://www.gemalto.com/review/Pages/109-the-amount-by-which-artificial-intelligence-in-new-vehicles-is-set-to-r.aspx>.
44. Ibid.

45. Philip.
46. Ibid.
47. *Top Artificial Intelligence Companies in Healthcare to Keep an Eye on the Medical Futurist.* The Medical Futurist[SM]<http://medicalfuturist.com/top-artificial-intelligence-companies-in-healthcare/>.
48. Ibid.
49. Ibid.
50. What Are the Key Objectives of the Commission in the Field of Cybersecurity? <http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf>.
51. Ibid.
52. Ibid.
53. Ibid.
54. Ibid.
55. Ibid.
56. Ibid.
57. Ibid.
58. Ibid.
59. Ibid.
60. Ibid.
61. Ibid.
62. Ibid.
63. Ibid.
64. Ibid.
65. Ibid.
66. Ibid.
67. Ibid.
68. Ibid.
69. Ibid.
70. Uchenna Jerome Orji. Multilateral Legal Responses to Cyber Security in Africa: Any Hope for Effective International Cooperation? <https://pdfs.semanticscholar.org/eb1c/59648805ae64bd6dca142e8aed70c79c6318.pdf>.
71. Ibid.
72. ButlerRobert J, Irving Lachow. Multilateral Approaches for Improving Global Security in Cyberspace.<https://www.mitre.org/sites/default/files/pdf/12_3718.pdf>.
73. Ibid.
74. Ibid.
75. Ibid.
76. Ibid.
77. Ibid.
78. Ibid.
79. Ibid.
80. Ibid.
81. Ibid.
82. Ibid.
83. Ibid.
84. Ibid.
85. Ibid.
86. Rita Boland. *Countries Collaborate To Counter Cybercrime*. *SIGNAL Magazine*; 2008. AFCEA <https://www.afcea.org/content/countries-collaborate-counter-cybercrime>.
87. Ibid.
88. Butler and Lachow.
89. Bill Snyder.*Bill Gates, Stephen Hawking Say Artificial Intelligence Represents Real Threat.*CIO,Consumer-Technology; 2015. <https://www.cio.com/article/2877482/consumer-technology/bill-gates-stephen-hawking-say-artificial-intelligence-represents-real-threat.html>.

Cite this Article
Md. Mamun-Ur-Rashid Askari. Significance of Ever-evolving Cybersecurity Landscape: Challenges and Possible Pathways. *National Journal of Cyber Security Law*. 2018; 1(1): 22–36p.