**DEPARTMENT OF STUDIES IN LAW,**
**UNIVERSITY OF MYSORE**
**MODEL UNITED NATIONS CONFERENCE-2019**
**&**
**Federation of International Students' Associations, Mysore (FISA-M)**

---

**Dear Delegates,**

We present to you the background guide of the Model United Nations Conference 2019. A background guide is merely a bird's eye view of the problem at hand. A legal overview has been provided so as to acquaint delegates with the burning international divisions the resolution of which will be critical to enable any progress on the agenda. This study guide should be a starting point for your research and you are encouraged to by all means further expand your realm of knowledge by delving into the themes and sub themes raised in the guide and the reference provided for further research.

***A MESSAGE FROM THE SECRETARY-GENERAL***

***Hello, everyone!***

***I am Sayed Qudrat, the Secretary General of Model United Nations, Department of Studies in Law, University of Mysore. I, have been a part of 10 MUNs so far. I have participated as the Secretary General in 7 MUNs held in JSS Law College Mysuru and I have acted in the same capacity in MUN conducted by the University of Mysore; Acharya Institute of Graduate Studies-Bangalore; St. Philomena's College Autonomous Mysore and Vidyavardhaka Law College Mysore. Discussing various issues concerning human trafficking, Intellectual property, asylum seekers, climate change and sustainable development, nuclear weapons, cybercrimes and international security I have also had the honour to adjudge one of the MUN conference conducted in JSS Law College Mysore.***

***I have presented papers on various burning and live topics such as International Terrorism, child Labour in Asian Countries, International law and International Security, Further, I have participated in various seminar workshops and Human Rights Conferences for instance; Seminar basic training on Human Rights, Labour law issues and Challenges, Seminar on Sensitizing Human Rights- A third world Approach, seminar on human rights of vulnerable sections of society , Human Rights in contemporary perspective, exploitation of women in Asian countries.***

***For this year's conference, I have endeavored to expand the reach of MUN, both in size and in content. We have set a theme which we believe will formulate flexible, workable and practical***

***solutions to current world problems and to encourage delegates to think beyond the traditional focus. The UN, though often criticized, is an important and unique international body as a platform for diplomacy and debate. MUN serves as a safe space for developing and scrutinizing new ideas, surrounded by a diverse group of people. My time in previous years has shown me that the experience, passion, and talent of the delegates and chairs that we host is unrivalled, and I am excited to see how you take on the theme and committees we have laid out this year.***

***I look forward to welcoming you all and providing you with an unforgettable conference experience. In the meantime, feel free to contact me at Sayedqudrathashimy@gmail.com with any questions or concerns regarding Model United Nations.***

***All the best!***
***Secretary General***
***Model United Nations Conference***

# BACKGROUND GUIDE

**COMMITTEE: UNITED NATIONS GENERAL ASSEMBLY (DISEC)**

**AGENDA: IMPACT OF CYBERCRIMES ON INTERNATIONAL SECURITY AND HUMAN RIGHTS**

## Introduction:

Cybercrime is an emerging form of transnational crime, and one of the fastest growing. As the Internet has become an almost essential part of our lives, providing information and communication all over the world, so criminals have taken advantage. With some two billion users worldwide, cyberspace is the ideal place for criminals because they can remain anonymous and gain access to all forms of personal information we knowingly, or unwittingly, store online. Threats to Internet safety have spiked dramatically in recent years, and cybercrime now affects more than 431 million adult victims globally.

The world's reliance on information and communications technology (ICT) is increasing exponentially as it becomes a major source of innovation and rapid growth. However, one must consider the possibility that our trust in technology could be more harmful than beneficial, especially with the advent of the newest front of warfare – in cyberspace. The threat and occurrences of attacks in cyberspace, or cyber warfare, has increased since the arrival of the new millennium, and with the escalating number of Internet users – exclusive of the current 2 billion– these asymmetrical and ambiguous attacks are only likely to increase in frequency. The potential hazard a strategically

coordinated cyber-attack poses to governments and organizations alike around the world is very real. Since the new millennium, the world has experienced major cyber-attacks on Estonia, the United States, China, South Korea and Iran, as well as on major corporations such as NASA and Lockheed. One only has to look as far back as May last year, when the United States charged five Chinese officials of cyber espionage.

Cyber warfare is not rooted in physical attack, but merely in cyberspace, and this is what makes it so incredibly dangerous. Cyber warfare does not involve stockpiling weapons, obtaining illegitimate materials via illegal methods or even any direct bodily harm. Rather, it is even more alarming since all one requires is a computer and the appropriate skill set. Cyber attacks work on some sort of intrusion through the Internet, usually done through complex computer malware. It is in the nature of a cyber attack to be difficult to detect, problematic to stop, and near impossible to track and locate, especially as hackers tend to use a plethora of techniques to cover up their tracks.

In addition to this, a major hindrance in combating cyber warfare is the lack of involvement of developing countries. Computer and Internet usage around the world is still largely limited to developed countries in North America and Europe, and NICs in Asia and South America. More than 60% of the world has no access to Internet facilities, ergo, leaving this percentage of the world's population unconcerned about such threats. Furthermore, hackers look to target entities withholding sensitive information that could potentially lead to financial or military rewards. This constrains the concern regarding cyber warfare to a small quantity of parties. But the truth remains that cyber warfare is not limited to large corporations. It can span from hacking and spying on individuals, to corporate espionage, and even large-scale attacks on countries. This is what makes it such a dangerous front of warfare. In today's world, where technology and the Internet are such an integral part of everyday lives, everyone is susceptible.

It is imperative that the framework for a global solution, at the least, should be proposed to deal with the threat of cyber warfare. Only a synergetic global network and a modicum of transparency are likely to curtail any possible government, individual or third-party infringements.

**Overview of the rise and role of cyber warfare**

Since the advent of information and communications technology in the late 20th century, major public as well as private services have been relocated online, including commerce, research and development, communications, power and fuel grids, and transportation. This relocation to the realm of cyberspace has made these services more susceptible to disruption, with the advent of cyber warfare. Cyber warfare is, in its essence, information warfare, although by no means does it encompass all the different forms of it. Cyber warfare can present itself in the shape of a military offensive, cyber terrorism, industrial espionage, ransomware, hacktivism or whistleblowing, and even general individual offenses and hacking. Cyber warfare is incredibly dangerous simply because the number of potential victims never decreases, as long as Internet usage increases. Everyone is at risk, especially if they are privy to sensitive or protected information, which could hand suitors a substantial advantage.
Rather surprisingly, despite the looming peril, the UN, along with most affected countries, has not engaged in active discussions or proposed any possible solutions or treaties, other than to sparsely elaborate on security in telecommunications. The only attempt to address the issue has been by the NATO, with the formation of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) in 2008 to conduct research and training on cyber security. The underlying reasons for this inactivity, and the base of the issue, is the inability to implicate an entity so far.

Motivations behind cyber warfare

Cyber warfare fundamentally operates on the same principles as classical warfare. It involves overwhelming the attacked party to gain control of the victim's resources for a financial, military, social or political advantage. The front for war has simply been shifted to cyberspace, and the fighting is now more symbolic than material. Hackers are now looking to gain unauthorized access to sensitive organizations or systems to hand either the third-party organization or government they are employed under a vital advantage. China and Russia are amongst a few countries to have purportedly conducted cyber attacks for corporate espionage and political purposes in the last 3 decades.

Similarly, it can also be used to bring harm. Cyber terrorism is the next suspected threat, especially with the relocation of communications, transportation and power grids online. If exposed or hacked, millions of people who depend on such systems could be at risk, and mass hysteria and panic could ensue. However, some groups looking to broadcast their political or social views may only take to the platform the Internet provides. Groups such as Anonymous and Lulzsec have perpetrated a flood of cyber attacks on civilian and corporate infrastructure since their formations in 2004 and 2011 respectively.

Problems with tackling cyber warfare

Cyber attacks are, by design, difficult to trace and uncover, since they are designed for privately disrupting or stealing from systems. Hackers use a variety of method to distort their IP address, which can usually be used to track the location of the attack. The use of or a combination of botnets, data encryption or using the IP address of another machine are just some of the ways in which attacks can be masked. In addition, hacktivist groups such as Anonymous use hackers from all over the world to further their cause, thus making it quite implausible to implicate one entity for a campaign at this current time. The software used by hackers is similarly advanced. Computer viruses can be spread by opening infected files on an attached email, or downloading an infected file from the internet, and after they propagate themselves in the machine, they are usually difficult to locate and eradicate. Viruses such as Zeus in 2009 (theft of financial information) and Flame (reconnaissance) in 2012 were highly sophisticated viruses, far ahead of their time, and comprised thousands of systems before discovery.

Antivirus software also do not successfully eradicate all possible viruses. The effectiveness of antivirus software has been declining in recent years, as malware grows more widespread. Malware developed earlier was easy to detect, as its destructive aftereffects were evident, but more recent viruses are highly advanced, and often developed by criminal organizations or entire governments, thus evolving into

untraceable, dangerous programs. Additionally, internal issues plague antivirus software, including false positives, detection issues and damaged files.

## Major Countries and Organizations Involved

### North Atlantic Treaty Organization (NATO)

NATO countries have been subject to countless cyber attacks in previous decades. As an intergovernmental military alliance, they take any threats to member states very seriously, well documented by the establishment of the Cooperative Cyber Defence Centre of Excellence (CCD COE) in 2008 in Tallinn, Estonia in the wake of the disastrous cyber attacks in Estonia in 2007. As an organization encompassing some of the most developed countries in the world, NATO takes the threat of cyber warfare very seriously, and is trying to integrate cyber defence systems into all NATO networks. The organization plays a key role in this issue since it is the only organization actively planning and developing methods to tackle cyber warfare, along with annual summit meets to discuss solutions and plans of action.

### International Telecommunication Union (ITU)

The ITU is a member of the United Nations Development Group (UNDP), a group which aims to give direction to the quality and impact of UN support at the country level. The ITU is tasked with spreading ICT in an affordable and equitable route to every member state, and hence is the only telecommunications organization with outreach to almost every country on the planet, in addition to 700 sector members and associates. The ITU plays a major role since it is the biggest link to the UN in this issue; thus any solutions will be run through the ITU before they are implemented.

### United States of America (USA)

At the forefront of tackling cyber warfare due to their position as a global superpower, the United States has received more than its fair share of cyber attacks, including the largest state-sponsored cyber attack in Titan Rain in 2003-06. In 2013, they considered

cyber warfare a larger cause of concern than extremist groups, thus highlighting that they are ready to address it as a serious threat. In addition to establishing the United States Cyber Command (USCYBERCOM) to tackle cyber warfare, the National Security Agency (NSA) also actively deals with similar threats. Home to large antivirus developers and some of the most technologically secure and advanced corporations in the world, the USA is at the forefront of the cyber war, and is the most devoted to finding a solution.

Estonia

Estonia has suffered the second-largest state-sponsored cyber attack in history in 2007, when Russia allegedly launched a mass DoS attack on numerous Estonian systems. As such, the cyber attack was what brought cyber warfare international coverage and attention. Years on, the Estonian cyber security system is considered the optimal model to implement for defence against cyber attacks today. Home to the CCD COE and a myriad of other cyber security projects, Estonia is the leader in implementing stratagems against cyber attacks.

People's Republic of China (PRC)

In recent years, China has become infamous for numerous alleged offenses regarding cyber warfare and online censorship. Perpetrators of some of the largest cyber attacks in history, such as the alleged involvement in Titan Rain in the USA, Operation Aurora in China itself (against Google, Yahoo, and more than 20 other corporations), and most recently, corporate espionage in the USA, China is perceived as a threat not only because of the vast numbers of cyber attacks originating from the country, but also because it is seeking to achieve the status of a 'superpower' in a possible fight for supremacy with the USA. This makes it a major entity and perhaps one of the initial locations for implementation of a solution.

Russian Federation

Once the United States' largest rivals at the height of information warfare in the Cold War, Russia has moved its fight to cyberspace. Russia is home to countless allegations

of cyber attacks, subterfuge and corporate espionage, including: one of the most advanced cyber attacks of all time in Estonia in 2007, attacks during the South Ossetia War in 2008 and now in Ukraine in 2014, making it another major entity in the fight against cyber warfare. However, other than allegations, there is no real evidence of Russia being involved in cyber warfare activities.

What is a cyber-crime? "Cyber crime" means any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them.[1]

Cybercrime exists in many forms, the most common being identity-related offences. This occurs by phishing (deceiving Internet users into giving their personal information), malware (unintentionally-installed software that collects personal information) and hacking (illegally accessing someone's computer remotely). Criminals tend to use these methods to steal credit card information and money. Furthermore, the Internet has also becoming a place for crimes related to copyright and intellectual property rights and also offences such as child pornography and abuse material.[2]

Cybercrime has grown easier as technology advances, and perpetrators no longer require great skills or techniques to be a threat. For example, software tools that allow the user to locate open ports or override password protection can be bought easily online. What has not grown easier, unfortunately, is the ability to find those responsible. With the anonymity that cyberspace provides, it is difficult for law enforcement to profile and locate the criminals. What is known, however, is that more than three quarters of cybercrime acts today are linked to organized criminal activity.

Cybercrime has rapidly grown into a business that may exceed three trillion US dollars a year. Without proper regulation, and insufficient capacity in many countries, combating cybercrime has proven difficult. A global effort is needed to provide better protection and firmer regulations because so far cyber criminals have hidden within legal loopholes in countries with less regulation. Perpetrators and their victims can be

[1] The new definition proposed in SA law – Electronic Communications and Transactions Amendment Bill, 2012 (26 October 2012)

[2] http://www.unis.unvienna.org/unis/en/events/2015/crime_congress_cybercrime.html#

located anywhere, but the effects are seen across societies, highlighting the need for an urgent and robust international response.

**How does cybercrime affect development?**

Developing countries lack the capacity to combat cyber-attacks and other forms of cybercrime. It is therefore not surprising that victimization rates are higher in countries with lower levels of development. Criminals also exploit countries' legal loopholes and weak security measures to perpetrate cybercrimes. The lack of cooperation between developed and developing countries can also result in "safe havens" for those committing cybercrimes.

**What is the United Nations doing to tackle it?**

An open-ended intergovernmental expert group was set up following the 12 th Crime Congress to study cybercrime, and consider how Member States, the international community and the private sector respond to it. By looking at sharing best practices and exchanging information on national legislation, it is hoped existing responses to cybercrime will be strengthened.

The United Nations Office on Drugs and Crime (UNODC) promotes long-term and sustainable capacity building in the fight against cybercrime through supporting national structures and action. Specifically, it draws on its specialized expertise on criminal justice systems to provide technical assistance in capacity building, prevention and awareness raising, and international cooperation, as well as data collection, research and analysis on cybercrime.

**Cybercrimes and Human Rights:**

The world of internet has become an inseparable part of human life. We use and depend on the world wide web almost for everything. Thus, when any misuse of this occurs, we get affected directly. Cyber rimes affects an individual in every walk of life, be it education; business; house hold issues and the like. The crux is to find a means to curb these crimes and penalise the wrong doers.

**Definition of Key Terms**

Cyber warfare : The deliberate use of computer technology to attack and disrupt the activities or communication systems of a state or organization. Cyber terrorism is a form of cyber warfare.

**Malware**

A piece of coded software that is capable of 'infecting' a computer. It embeds itself within an existing computer program, typically interfering with the system, such as corrupting or erasing data. It presents in different kinds, including viruses, trojans, worms and spyware.

Internet Protocol (IP)

The method by which information is sent between any two Internet computers on the Internet.

**Information and Communications Technology (ICT)**

ICT refers to all the technology used to handle telecommunications, broadcast media, intelligent building management systems, audiovisual processing and transmission systems, and network based control and monitoring functions.

**Cyber attack**

An attempt by hackers to damage or destroy a computer network or system.

**Denial-of-Service (DoS) attack**

A denial of service (DoS) makes a server or a network resource unavailable to legitimate users, usually by temporarily interrupting or suspending the services of a host connected to the Internet. The attacker (hacker) floods the network or server with data traffic, causing it to crash or become busy, and therefore temporarily unavailable.

Distributed Denial-of-Service (DDoS) attack

Similar to a DoS attack, numerous compromised systems are used to target a single system, preventing an individual or a select group from accessing a service or network. Victims of a DDoS attack consist of both the end-targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.

Advanced Persistent Threat (APT)

A cyber attack which employs stealth and multiple attack methods to compromise a high-value corporate or government target. The attack is near-impossible to initially

detect and provides the hacker with continuous access to the target system through a 'backdoor'. Usually a long, drawn out operation over months or year which involves theft, sabotage and surveillance of data.

**Exploit**

An exploit is a piece of software, a command, or a methodology that attacks one particular security vulnerability in a system. Exploits are a common function of malware. A backdoor is a form of an exploit, which bypass the normal authentication mechanisms. Generally, hackers use backdoors for easy and continued accessibility to a system after it has been compromised.

**Hacktivism**

Hacktivism is the act of hacking a website or computer network or disrupting computer services in an attempt to convey or broadcast a social or political message. The person who carries out the act of hacktivism is known as a hacktivist.

**Botnet**

A botnet is a group of computers connected in a coordinated fashion for malicious purposes. Each computer in a botnet is called a bot. These bots form a network of compromised computers, which is controlled by a third party and used to transmit malware or spam, or to launch attacks.

Data encryption and decryption

Encryption is a cryptographic method which uses an algorithm to transform sensitive information and data, making it unreadable for unauthorized users.19 Decryption is the process of transforming data and information that has been rendered unreadable through encryption back to its unencrypted form. Some of the items that are commonly encrypted include email messages, text files, images, user data and directories.

**Questions to ponder upon:**

i. Ancillary problems related to cyber crimes
ii. How do cybercrimes affect human rights?
iii. How is your country affected?
iv. What solutions would your country propose?
v. What constitutes a cyber-attack, cyber espionage, and hacking? How should

these actions be responded to? When does the use of information technology constitute an act of aggression?

vi. What principles can guide an international agreement on the limitations of the use of information technology for the sake of maintaining international peace and security?

vii. How should member states respond to the potential threat from non-state actors that acquire offensive cyber technology?


***CHIEF PATRON:***
**Hon'ble Vice Chancellor**
**University of Mysore**

***PATRON:***
***Prof. Dr. C. BASAVARAJU***
**Professor and Chairman**
**Department of Studies in Law**
***e-mail address: cbr_1563@yahoo.co.in***
***Mobile no. +91-821-2419844***

***Sayed Qudrat Hashimy***
***Secretary General,***
***Model United Nations Conference***
***Department of Studies in Law, University of Mysore***
*Email: Sayedqudrathashimy@gmail.com*
***Mobile No.+91 900 881 3333***

**President of General Assembly,**
**Model United Nations conference**
**SHUKRULLAH AHMADI**
**( FISA-M , PRESIDENT )**
Shukrullah.ahmadi85@gmail.com
**WHATSSP NO ( 8277166134)**
**Phone no. : +91 8217073695**

**Fathima Ibrahim**
**Chairperson,**
**Model United Nations Conference**
**email: fathimaibrahim31@gmail.com**

**Phone no. +91 9446276627**

**TAMANA SHARIFI**
**Under Secretary General**
**Model United Nations conference**
**Department of Studies in Law**
**email: tamansharifi652@gmail.com**
**Phone no. +917618710933**

**Coordinator,**
**Model United Nations Conference**
**Seif Mohammed Suleiman**
**Organising Secretary, FISA-M**
**email: smsuleiman47@gmail.com**
**Whats app no. +255 776 441 653**
**Mobile no. +91 99168 70734**

**RAPPORTEUR, MUN**
**Jaanaky vigneswaran**
**Academic Secretary, FISA –M**
**email: jaanvi1801@gmail.com**
**Phone no. +91 9148755815**

**DEPARTMENT OF STUDIES IN LAW,**
**UNIVERSITY OF MYSORE**
**MODEL UNITED NATIONS CONFERENCE-2019**
**&**
**Federation of International Students' Associations, Mysore (FISA-M)**

---

The Department of Studies in Law, University of Mysore, has honour to organize the first edition of Model United Nations Conference jointly with the Federation of International Students' Associations, Mysore (FISA-M) on the Agenda being "Impact of cybercrimes on International Security and Human Rights" under Disarmament & International Security Committee of United Nations General Assembly.

Participants can choose the country from the country matrix. Each participant will be allowed to represent only one country. Countries will be allotted according to preference on first come first serve basis.

**Registration fees is Rs. 200/-**

**Last date of Registration 15th December, 2019**

**The MUN will be held on 21, December, 2019**

**For further information, kindly contact the undersigned.**

# ***COUNTRY MATRIX***

| Serial No. | Country | |
|---|---|---|
| 1. | Afghanistan | |
| 2. | Albania | |
| 3. | Algeria | |
| 4. | Andorra | |
| 5. | Angola | |
| 6. | Antigua and Barbuda | |
| 7. | Argentina | |
| 8. | Armenia | |
| 9. | Australia | |
| 10. | Austria | |
| 11. | Azerbaijan | |
| 12. | Bahamas | |
| 13. | Bahrain | |
| 14. | Bangladesh | |
| 15. | Barbados | |
| 16. | Belarus | |
| 17. | Belgium | |
| 18. | Belize | |
| 19. | Benin | |
| 20. | Bhutan | |
| 21. | Bolivia | |
| 22. | Bosnia and Herzegovina | |
| 23. | Botswana | |
| 24. | Brazil | |
| 25. | Brunei | |
| 26. | Bulgaria | |
| 27. | Burkina Faso | |
| 28. | Burma (Myanmar) | |
| 29. | Burundi | |
| 30. | Cambodia | |
| 31. | Cameroon | |
| 32. | Canada | |
| 33. | Cape Verde | |
| 34. | Central African Republic | |
| 35. | Chad | |
| 36. | Chile | |
| 37. | China[2] | |
| 38. | Colombia | |
| 39. | Comoros | |
| 40. | Congo, Rep. of | |
| 41. | Congo, Dem. Rep. of | |
| 42. | Costa Rica | |
| 43. | Côte d'Ivoire | |
| 44. | Croatia | |
| 45. | Cuba | |
| 46. | Cyprus | |
| 47. | Czech Republic[3] | |
| 48. | Denmark | |
| 49. | Djibouti | |
| 50. | Dominica | |

| | | |
|---|---|---|
| 51. | Dominican Republic | |
| 52. | East Timor[4] | |
| 53. | Ecuador | |
| 54. | Egypt | |
| 55. | El Salvador | |
| 56. | Equatorial Guinea | |
| 57. | Eritrea | |
| 58. | Estonia | |
| 59. | Ethiopia | |
| 60. | Fiji | |
| 61. | Finland | |
| 62. | France | |
| 63. | Gabon | |
| 64. | Gambia | |
| 65. | Georgia | |
| 66. | Germany | |
| 67. | Ghana | |
| 68. | Greece | |
| 69. | Grenada | |
| 70. | Guatemala | |
| 71. | Guinea | |
| 72. | Guinea-Bissau | |
| 73. | Guyana | |
| 74. | Haiti | |
| 75. | Honduras | |
| 76. | Hungary | |
| 77. | Iceland | |
| 78. | India | |
| 79. | Indonesia | |
| 80. | Iran | |
| 81. | Iraq | |
| 82. | Ireland | |
| 83. | Israel | |
| 84. | Italy | |
| 85. | Jamaica | |
| 86. | Japan | |
| 87. | Jordan | |
| 88. | Kazakhstan | |
| 89. | Kenya | |
| 90. | Kiribati | |
| 91. | Korea, North | |
| 92. | Korea, South | |
| 93. | Kuwait | |
| 94. | Kyrgyzstan | |
| 95. | Laos | |
| 96. | Latvia | |
| 97. | Lebanon | |
| 98. | Lesotho | |
| 99. | Liberia | |
| 100 | Libya | |
| 101 | Liechtenstein | |
| 102 | Lithuania | |
| 103 | Luxembourg | |
| 104 | Macedonia[5] | |
| 105 | Madagascar | |
| 106 | Malawi | |
| 107 | Malaysia | |

| | | |
|---|---|---|
| 108 | Maldives | |
| 109 | Mali | |
| 110 | Malta | |
| 111 | Marshall Islands | |
| 112 | Mauritania | |
| 113 | Mauritius | |
| 114 | Mexico | |
| 115 | Micronesia | |
| 116 | Moldova | |
| 117 | Monaco | |
| 118 | Mongolia | |
| 119 | Montenegro[4, 6] | |
| 120 | Morocco | |
| 121 | Mozambique | |
| 122 | Namibia | |
| 123 | Nauru | |
| 124 | Nepal | |
| 125 | Netherlands | |
| 126 | New Zealand | |
| 127 | Nicaragua | |
| 128 | Niger | |
| 129 | Nigeria | |
| 130 | Norway | |
| 131 | Oman | |
| 132 | Pakistan | |
| 133 | Palau | |
| 134 | Panama | |
| 135 | Papua New Guinea | |
| 136 | Paraguay | |
| 137 | Peru | |
| 138 | Philippines | |
| 139 | Poland | |
| 140 | Portugal | |
| 141 | Qatar | |
| 142 | Romania | |
| 143 | Russia | |
| 144 | Rwanda | |
| 145 | St. Kitts and Nevis | |
| 146 | St. Lucia | |
| 147 | St. Vincent and the Grenadines | |
| 148 | Samoa | |
| 149 | San Marino | |
| 150 | São Tomé and Príncipe | |
| 151 | Saudi Arabia | |
| 152 | Senegal | |
| 153 | Serbia[6] | |
| 154 | Seychelles | |
| 155 | Sierra Leone | |
| 156 | Singapore | |
| 157 | Slovakia[3] | |
| 158 | Slovenia | |
| 159 | Solomon Islands | |
| 160 | Somalia | |
| 161 | South Africa | |
| 162 | South Sudan | |
| 163 | Spain | |

| | | |
|---|---|---|
| 164 | Sri Lanka | |
| 165 | Sudan (North) | |
| 166 | Suriname | |
| 167 | Swaziland | |
| 168 | Sweden | |
| 169 | Switzerland[4] | |
| 170 | Syria | |
| 171 | Tajikistan | |
| 172 | Tanzania | |
| 173 | Thailand | |
| 174 | Togo | |
| 175 | Tonga | |
| 176 | Trinidad and Tobago | |
| 177 | Tunisia | |
| 178 | Turkey | |
| 179 | Turkmenistan | |
| 180 | Tuvalu | |
| 181 | Uganda | |
| 182 | Ukraine | |
| 183 | United Arab Emirates | |
| 184 | United Kingdom | |
| 185 | United States | |
| 186 | Uruguay | |
| 187 | Uzbekistan | |
| 188 | Vanuatu | |
| 189 | Venezuela | |
| 190 | Vietnam | |
| 191 | Yemen | |
| 192 | Zambia | |
| 193 | Zimbabwe | |

***CHIEF PATRON:***
**Hon'ble Vice Chancellor**
**University of Mysore**

***PATRON:***
***Prof. Dr. C. BASAVARAJU***
**Professor and Chairman**
**Department of Studies in Law**
***e-mail address: cbr_1563@yahoo.co.in***
***Mobile no. +91-821-2419844***

***Sayed Qudrat Hashimy***
***Secretary General,***
***Model United Nations Conference***
***Department of Studies in Law, University of Mysore***
*Email: Sayedqudrathashimy@gmail.com*
***Mobile No.+91 900 881 3333***

**President of General Assembly,**
**Model United Nations conference**
**SHUKRULLAH AHMADI**
**( FISA-M , PRESIDENT )**
Shukrullah.ahmadi85@gmail.com
**WHATSSP NO ( 8277166134)**
**Phone no. : +91 8217073695**

**Fathima Ibrahim**
**Chairperson,**
**Model United Nations Conference**
**email: fathimaibrahim31@gmail.com**
**Phone no. +91 9446276627**

**TAMANA SHARIFI**
**Under Secretary General**
**Model United Nations conference**
**Department of Studies in Law**
**Email address: tamansharifi652@gmail.com**
**Phone no. +917618710933**

**Coordinator,**
**Model United Nations Conference**
**Seif Mohammed Suleiman**
**( Organising Secretary, FISA-M )**
**email: smsuleiman47@gmail.com**
**Whats app no. +255 776 441 653**
**Mobile no. +91 99168 70734**

**RAPPORTEUR, MUN**
**Jaanaky vigneswaran**
**(Academic Secretary, FISA –M )**
**Email address: jaanvi1801@gmail.com**
**Phone no. +91 9148755815**