SADIQ MUN VI

SOCHUM

STUDY GUIDE

STUDY GUIDE : ADDRESSING AND COUNTERING ISLAMOPHOBIA IN THE CONTEMPORARY 21ST CENTURY CONTEXT

COMMITTEE: SOCHUM

INTRODUCTION TO THE TOPIC:

The Social, Humanitarian, and Cultural Committee (SOCHUM) stands at the forefront of addressing pressing global issues, advocating for human rights, and fostering inclusive societies. In the contemporary landscape, one of the most pervasive challenges the world faces is the rise of Islamophobia. This study guide is dedicated to comprehensively understanding, analyzing, and formulating strategies to counter Islamophobia within the context of the 21st century.

Islamophobia, a multifaceted issue rooted in historical narratives, societal biases, and geopolitical complexities, continues to manifest in various forms across the globe. Its impact extends beyond individual discrimination, affecting policies, media

representations, economic opportunities, and social integration. In recognizing the urgency to address this issue, this study guide endeavors to delve into the depths of Islamophobia—its origins, impacts, and, most importantly, the pathways toward its eradication.The complexity of Islamophobia demands a holistic approach, emphasizing collaboration, education, and proactive measures. By fostering an environment of open discourse and critical analysis, this study guide seeks to inspire delegates to develop nuanced, sustainable, and effective resolutions to combat Islamophobia, thus contributing to a more inclusive and harmonious global society.

ADDRESSING ISLAMOPHOBIA:

Islamophobia is a fear, prejudice and hatred of Muslims that leads to provocation, hostility and intolerance by means of threatening, harassment, abuse, incitement and intimidation of Muslims and non-Muslims, both in the online and offline world. Motivated by institutional, ideological, political and religious hostility that transcends into structural and cultural racism, it targets the symbols and markers of being a Muslim. https://www.un.org/en/observances/anti-islamophobia-day

Hence, Addressing Islamophobia involves actively confronting, challenging, and seeking to eliminate prejudices, biases, discrimination, and negative perceptions specifically targeting Islam and Muslims. It encompasses efforts to counteract the irrational fear, stereotypes, and systemic injustices directed towards individuals or communities based on their Islamic faith or perceived association with Islam.

This involves a multifaceted approach that includes education, advocacy, policy reforms, promoting interfaith dialogue, media literacy, fostering cultural understanding, and encouraging inclusive societal practices.

UNDERSTANDING ISLAMOPHOBIA:

The term Islamophobia, popularized in the late 1990s. Islamophobia can be defined as the excessive and empirically unjustifiable fear, hatred of, or bias against Islam, Muslims, and Islamic civilization. These are translated into policies, attitudes, language, literature, and into condoned individual as well as collective behavioral patterns. **Islamophobia is a new term for a centuries-old idea and phenomenon**. Its evolution was steep and dynamic. Differences from one era and its context to another were in nuances and methods, rather than magnitudes and goals. While at first and for a long time Islamophobia

was in the spirit of "us versus them," in recent times, it came to be "them among us.

https://www.islamicity.org/72340/the-origins-of-islamophobia/

Organized mobilization against Islam and Muslims in liberal democracies surged after the 9/11 attacks in the United States by Al-Qaeda. This gave rise to what became a transnational, anti-Islamic movement. Prominent activist groups include the English Defence League (EDL), Patriotic Europeans against the Islamization of the West (PEGIDA), Stop Islamization, and Act! For America. While these groups have taken to the streets, the anti-Islamic movement is also an online phenomenon.

https://www.sv.uio.no/c-rex/english/groups/compendium/what-is-islamophobia.html#

IMPACT ON INDIVIDUALS AND SOCIETIES :

Islamophobia has profound effects on both individuals and societies, ranging from psychological impacts on individuals to broader societal repercussions.

Experts and human rights monitors report that widespread negative representation of Islam,fear of Muslims generally (not just Muslims extremists or terrorists) and the security and counter-terrorism policies have served to perpetuate, validate and normalize discrimination ,hostility and violence towards Muslims individuals and communities.Rights monitors assert that States directly restrict the right to freedom of religion or belief of Muslims; curtail enjoyment of this right by limiting Muslims' other fundamental rights; and securitize Muslim communities and/or their organizations. Members of Muslim communities themselves, especially those living as minorities, recount alarming tolerance or indifference to their experiences of anti-Muslim

bias, discrimination and violence. Among the concerns they have raised are: violent attacks and impunity for such attacks, including those causing mass casualties; industrial-scale internment designed to coercively change beliefs; disproportionate restrictions on the ability of Muslims to manifest their beliefs; limits on access to citizenship; and socioeconomic exclusion and pervasive stigmatization of Muslim communities.

In such climates of exclusion, fear and distrust, Muslims report that they often feel stigma, shame and a sense that they belong to "suspect communities" that are being forced to bear collective responsibility for the actions of a small minority. In India, for example, approximately half of police personnel reportedly believe that Muslims are "likely" to be prone to committing crimes, 36 per cent believe that Muslims are "somewhat" prone to committing crimes and 14 per cent believe that Muslims are "very much" prone to committing crimes.In surveys conducted in Europe in 2018 and 2019, an average of 37 percent of the population reported that they held unfavourable views of Muslims. In 2017, some 30 per cent of respondents to a survey conducted in the United States of America viewed Muslims in a negative light. In Myanmar, unchecked Buddhist nationalists peddling the view that Islam threatens to "overrun" the country and that Buddhists must stand up and " save" their way of life have contributed to egregious atrocities against Rohingya Muslims.

https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/086/49/PDF/G2108649.pdf?OpenElement

Globally, many Muslims report not feeling respected by those in the West. Significant percentages of several Western countries share this sentiment, saying that the West does not respect Muslim societies. Specifically, 52% of Americans and 48% of Canadians say the West does

not respect Muslim societies. Smaller percentages of Italian, French, German, and British respondents agree.

https://news.gallup.com/poll/157082/islamophobia-understanding-anti-muslim-sentiment-west.aspx

LEGAL FRAMEWORKS AND HUMAN RIGHTS:

Numerous international human rights instruments aim to protect individuals from discrimination based on religion or belief. Instruments like the Universal Declaration of Human Rights, International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social, and Cultural Rights emphasize the right to freedom of religion and prohibit discrimination on religious grounds.Moreover,

various United Nations agencies and bodies play a crucial role in addressing and combating Islamophobia on a global scale. Entities like the Office of the High Commissioner for Human Rights (OHCHR), UNESCO, and the United Nations Alliance of Civilizations (UNAOC) work to promote religious tolerance and combat discrimination.

Furthermore, the United Nations General Assembly adopted a resolution sponsored by 60 Member-States of the Organization of Islamic Cooperation (OIC), which designated 15 March as the International Day to Combat Islamophobia. The document stresses that terrorism and violent extremism cannot and should not be associated with any religion, nationality, civilization, or ethnic group. It calls for a global dialogue on the promotion of a culture of tolerance and peace, based on respect for human rights and for the diversity of religions and belief.

Marking the first International Day to Combat Islamophobia in 2021, UN Secretary-General António Guterres pointed out that anti-Muslim bigotry is part of a larger trend of a resurgence in ethno-nationalism, neo-Nazism, stigma and hate speech targeting vulnerable populations including Muslims, Jews, some minority Christian communities, as well

as others. "As the Holy Quran reminds us: nations and tribes were created to know one another. Diversity is a richness, not a threat," he added.

https://www.un.org/en/observances/anti-islamophobia-day

COMBATTING ISLAMOPHOBIA:

The Organization of Islamic Cooperation (OIC) undoubtedly has a large role to play in combatting rising Islamophobia and this remains one of the greatest challenges of contemporary times. Such fissures in societies call for a proactive approach by organizations like the OIC, which must come up with newer approaches towards tackling this rising menace. An important step in this direction should be the initiation of interfaith dialogue, for better understanding of each other's faiths. Such endeavours can be successful, if carried out at all levels starting from the media, academics, religious and political leaders. Electronic, print and most particularly, social media have a great role to play in this regard.

https://issi.org.pk/issue-brief-on-combatting-disinformation-and-islamophobia/

We can combat Islamophobia by :

Education and Awareness Programs:

Educational initiatives and awareness programs play a vital role in challenging misconceptions, fostering understanding, and combating Islamophobia at the societal level.

- Promoting Cultural Understanding: Education programs focused on cultural diversity and religious literacy help dispel stereotypes and misconceptions about Islam and Muslims, fostering empathy and respect.
- Critical Thinking Skills: Curriculum-based initiatives promoting critical thinking skills encourage individuals to question biases

and prejudices, enabling them to analyze information critically and discern misinformation or stereotypes.

Role of Religious Institutions:

Religious institutions, including mosques, Islamic centers, and community organizations, hold a significant role in combating Islamophobia by promoting interfaith dialogue, social engagement, and fostering a sense of belonging.

- Interfaith Dialogue: Religious institutions often serve as platforms for interfaith dialogues, encouraging interaction among diverse religious communities to foster understanding and cooperation.
- Community Outreach: These institutions engage in community outreach programs, educational workshops, and social initiatives that promote understanding, dispel misconceptions, and build bridges across religious and cultural divides.
- Advocacy and Support: Religious institutions advocate for the rights of their community members, provide support for those facing discrimination, and work towards creating inclusive spaces for all individuals regardless of their faith.

CASE STUDIES AND EXAMPLES OF ISLAMOPHOBIA:

Some events have brought about a significant impact on the trend and prospects of Islamophobia particularly the terrorist attacks against Muslims in New Zealand in March 2019 ; the terrorist attack in Sri Lanka in 2019 ; the European Union Parliamentary election in March 2019; the case against Myanmar for the genocide against Rohingya in the International Court of Justice in November 2019 ; the introduction of controversial Citizenship Amendment Act (CAA) by India in August 2019 ; and the havoc in France following the republication of derogatory cartoons of the Holy Prophet (PBUH) by Charlie Hebdo Magazine in September 2020.

https://www.oic-oci.org/upload/islamophobia/2021/The_13th_Islamophobia_Annual_Report_English.pdf

SUCCESS STORIES AGAINST ISLAMOPHOBIA:

The Muslim world is becoming more engaged in the efforts to address the issue of Islamophobia as seen from the rising interest, commitment, and actions taken by a number of Muslim countries. At the OIC level, Member States have given a stronger mandate to the Organization to combat Islamophobia. The Final Communiqué adopted during the Executive Committee Emergency Meeting in Istanbul in March 2019, requests the OIC to engage and take action to combat religious discrimination, Islamophobia, intolerance and hatred towards Muslims, as a matter of priority. The 14th Islamic Summit held in Makkah, Kingdom of Saudi Arabia, called on the OIC to devise strategies and plans to address the issue. In addition, an 'OIC Plan of Action on Combating Islamophobia, Religious Discrimination, Intolerance and Hatred towards Muslims' was adopted during the OIC Annual Coordination Meeting on the sideline of the 74th Session of UNGA in September 2019, paving the way for the efforts deployed by the Muslim world to take on a more significant dimension thanks to concerted action. A similar dose of enthusiasm was seen at the UN level, as Member Countries i.e. Saudi Arabia, Qatar, Iran, Malaysia, Egypt, Indonesia, Azerbaijan, Pakistan, and Turkey have been very active in advancing the Muslim world's contribution to the global efforts against Islamophobia, as well as against Xenophobia in general.

Such a positive trend unfolds in parallel with the current global action against Islamophobia, Xenophobia, intolerance, and any other forms of racism and discrimination. The OIC General Secretariat noted with gratitude that following the terrorist attack in New Zealand, significant measures have unrolled around the globe in the fight against

Islamophobia while providing greater protection to Muslims and other minorities. Few instances could be mentioned here: The UN has launched its Strategy and Plan of Action on Hate Speech; The EU has developed a new initiative on 'Countering Racism and Xenophobia'; The OHCHR decided to give a push to the full implementation of UN Resolution 16/18 on Combating Intolerance, Discrimination, Stereotyping, and Incitement of Violence against Persons Based on Religion.

Similarly, a string of measures have been taken by individual countries, such as New Zealand, which launched a nation-wide 'buyback' scheme aimed at getting rid of the country's semi-automatic weapons; Canada and Germany have outlawed certain far-right groups; Germany began fighting online hate speech while moving to step up surveillance of far-right groups in the country; Twitter was reported to have blocked Dutch far-right politician Geert Wilders's account for his 'hateful behaviour'.

https://www.oic-oci.org/upload/islamophobia/2021/The_13th_Islamophobia_Annual_Report_English.pdf

CONCLUSION :

The exploration of Islamophobia within the contemporary context reveals a complex and multifaceted issue that permeates societies worldwide. Throughout this study guide, we've delved into the various dimensions of Islamophobia, examining its origins, impacts, and avenues for mitigation.From dissecting the detrimental effects on individuals and societies to analyzing the contemporary challenges such as media representation, political discourse, and global events, the depth of this issue becomes evident. Additionally, we've explored the critical role of legal frameworks, human rights, socio-cultural perspectives, and the contributions of religious institutions and education in addressing and countering Islamophobia.The case studies and examples presented

highlight both the sobering realities of discrimination faced by Muslim communities and the encouraging success stories in combating this prejudice. By acknowledging these diverse experiences and approaches, we recognize the importance of concerted efforts and innovative strategies to foster inclusive societies that uphold fundamental human rights and respect for diversity. In striving for a world free from discrimination and fear based on religious beliefs, let us carry forth the lessons learned and the determination forged within this guide. Together, through dialogue, advocacy, and concerted action, let us create inclusive environments where every individual, irrespective of their background or faith, is embraced with dignity, equality, and respect.

STUDY GUIDE: ANALYSING THE CYBER CRIME MARKET AS A SOCIAL AND CULTURAL MENACE

COMMITTEE: SOCHUM

INTRODUCTION TO THE TOPIC:

There is no international definition of cybercrime. Broadly, cybercrime can be described as a broad concept encompassing cyber-dependent and cyber-enabled offences. Cyber-dependent crime requires an ICT infrastructure and is often typified as the creation, dissemination and deployment of malware, ransomware, attacks on critical national infrastructure (e.g., the cyber-takeover of a power plant by an organized crime group), taking a website offline by overloading it with data (a DDoS [Distributed Denial of Service] attack) or accessing confidential client data. Cyber-enabled crime can occur in the offline world but can also be facilitated by ICT. This typically includes online fraud, purchases of drugs online and online money laundering. https://www.unodc.org/unodc/en/cybercrime/our-approach

The Social, Humanitarian, and Cultural Committee (SOCHUM) is convened today to unravel the multifaceted dimensions of this phenomenon, recognizing its profound impact on our societies and cultures worldwide.Through exploring this topic, we aim not only to comprehend the mechanisms of the cybercrime market but also to underscore its profound societal and cultural ramifications. Understanding the psychological toll on victims, the erosion of privacy and trust, and the reshaping of our cultural perceptions is paramount in formulating effective strategies to combat this pervasive threat.

DEFINITION AND TYPE OF CYBER CRIME:

Cybercrime refers to any illegal activity that is carried out using digital technology or the internet. It encompasses a wide range of criminal activities that exploit vulnerabilities in digital systems, networks, or devices for financial gain, data theft, or disruption of services.

Types of Cybercrime:

1. Phishing: Fraudulent attempts to obtain sensitive information (like passwords, credit card details) by posing as a trustworthy entity in electronic communication.

2. Malware: Malicious software designed to damage, disrupt, or gain unauthorized access to computer systems. This includes viruses, ransomware, spyware, and worms.

3. Identity Theft: Stealing someone's personal information (such as social security numbers, bank account details) to commit fraud or other crimes.

4. Cyberbullying: Harassment, threats, or intimidation of individuals using digital platforms, often through social media, emails, or messaging apps.

5. Data Breaches: Unauthorized access or release of sensitive or confidential information, often through hacking or exploiting security vulnerabilities.

6. Cyber Extortion: Demanding payment or other favors by threatening to reveal sensitive information or launch attacks against an individual or organization's systems.

7. Online Fraud: Various fraudulent activities conducted online, such as investment scams, online shopping fraud, or auction fraud.

8. Distributed Denial of Service (DDoS): Overloading a network or server with excessive traffic, causing it to crash or become inaccessible.

9. Cyber Espionage: Illegally accessing confidential information from governments, companies, or individuals for espionage or competitive advantage.

10. Hacking: Unauthorized access into computer systems or networks with the intent to disrupt, steal information, or manipulate data.

Importance of analyzing cybercrime as a social and cultural menace :

Cybercrime is one of the fastest-growing criminal activities in the world. In fact, according to the **report from PR Newswire**, cybercrime has increased by a staggering 400% since the start of the COVID-19 pandemic, suggested FBI. This staggering increase highlights the need for greater awareness and prevention measures to protect against cyber threats. The effects of cybercrime can be devastating, ranging from financial loss and identity theft for individuals to reputational damage and legal repercussions for businesses. Additionally, cybercrime can have far-reaching consequences for society, from economic impacts to national security concerns and an increase in cyberbullying and harassment.55 million consumers were victims of identity theft in 2021, as per a report from **Norton**. This alarming number shows no signs of slowing down, and it's no longer a question of if you or your business falls victim to a cyberattack. Hence, it is important to consider cyber rime as a social and cultural menace.

https://www.linkedin.com/pulse/impact-cybercrime-individuals-businesses-society-join-welance

HISTORICAL BACKGROUND AND EVOLUTION OF CYBERCRIME:

Technically, the first cyber attack happened in France well before the internet was even invented, in 1834. Attackers stole financial market information by accessing the French telegraph system. From that

moment on, cybercrime has grown exponentially, marked by an intriguing evolution of tactics, techniques, and procedures — all implemented for malicious gain.

Still, cybercrime didn't really find its footing until the mid-point of the 20th century. Spurred on by the digital revolution, cybercriminals became early adopters of technology, using their head start and their smarts to engineer new, devious ways to part people and organizations from their data and dollars.

In 1996 the Council of Europe, together with government representatives from the United States, Canada, and Japan, drafted a preliminary international treaty covering computer crime. Around the world, civil libertarian groups immediately protested provisions in the treaty requiring Internet service providers (ISPs) to store information on their customers' transactions and to turn this information over on demand. Work on the treaty proceeded nevertheless, and on November 23, 2001, the Council of Europe Convention on Cybercrime was signed by 30 states. The convention came into effect in 2004. Additional protocols, covering terroristactivities and racist and xenophobic cybercrimes, were proposed in 2002 and came into effect in 2006. In addition, various national laws, such as the USA PATRIOT Act of 2001, have expanded law enforcement's power to monitor and protect computer networks**.**

https://www.britannica.com/topic/cybercrime

Cyber Crime Statistics

- Nearly 1 billion emails were exposed in a single year, affecting 1 in 5 internet users.
- Data breaches cost businesses an average of $4.35 million in 2022.
- Around 236.1 million ransomware attacks occurred globally in the first half of 2022.

- 1 in 2 American internet users had their accounts breached in 2021.
- 39% of UK businesses reported suffering a cyber attack in 2022.
- Around 1 in 10 US organisations have no insurance against cyber attacks.
- 53.35 million US citizens were affected by cyber crime in the first half of 2022.
- Cyber crime cost UK businesses an average of £4200 in 2022.
- In 2020, malware attacks increased by 358% compared to 2019.
- The most common cyber threat facing businesses and individuals is phishing.

https://aag-it.com/the-latest-cyber-crime-statistics/

DARK WEB AND ITS ROLE IN THE CYBER CRIME MARKET :

The dark web is a hidden part of the internet that requires specific software or configurations to access. It's commonly associated with illicit activities due to its anonymity features, allowing users to operate beyond the reach of conventional search engines. Within the dark web, marketplaces exist where illicit goods and services, including cybercrime tools and stolen data, are bought and sold. These marketplaces provide a platform for cybercriminals to operate without fear of immediate detection, facilitating the exchange of hacking tools, stolen credentials, malware, and other illegal offerings.

Monetization Methods and Economic Impact:

Cybercriminals monetize their activities through various means:

1. Sale of Stolen Data: Personal information, credit card details, login credentials, and intellectual property are sold to interested buyers on the dark web or other illicit platforms.

2. Ransomware Payments: Extorting victims by encrypting their data and demanding payment in exchange for decryption keys.

3. Fraudulent Activities: Cybercriminals engage in financial fraud, online scams, and identity theft to obtain monetary gains.

4. Cybercrime-as-a-Service (CaaS): Offering tools, services, or expertise for a fee, allowing less skilled individuals to engage in cybercriminal activities.

The economic impact of cybercrime is significant, with costs attributed to financial losses, damage to reputation, cybersecurity investments, legal fees, and the societal toll of dealing with the aftermath of cyberattacks. The global cost of cybercrime continues to escalate, underscoring the pressing need for concerted efforts to combat this thriving cybercrime economy.

SOCIAL IMPACTS OF CYBER CRIME:

When it comes to cybercrime, nothing is private — be it our geolocation, our conversations on social media, or even our bank account. With over 60% of the world's population now accessing the internet, it is easy for hackers to find vulnerable people and attack them.Children and the elderly are often cited as common victims of cybercrime, but they certainly aren't the only groups at risk. Even teens face cybercrime in forms like cyberbullying and solicitation. Cybercrime has a psychological impact on those affected, causing feelings of anxiety, depression, and even trauma.It has been found that even a single successful cybercrime can have far-reaching effects such as financial losses and theft of intellectual property. Collectively, as a society, we lose billions of dollars to cybercrime every year. In 2020, the global economy lost $945 billion to cybercrime, and this number is expected to steadily increase.Not just individuals, but businesses and even governments are vulnerable to cybercrime when not protected properly. It is possible for hackers to access customer and citizen data, which can generate distrust towards the involved organisation / government, which may lead them to pay millions to settle claims.

https://studyonline.port.ac.uk/blog/what-is-the-impact-of-cybercrime-on-society-and-the-economy

LEGAL AND REGULATORY FRAMEWORK:

International Laws and Conventions Related to Cybercrime:

1. Council of Europe Convention on Cybercrime (Budapest Convention): One of the primary international legal instruments addressing cybercrime. It provides a framework for harmonizing national laws, facilitating international cooperation, and establishing procedures for investigation and prosecution.

2. United Nations Convention against Transnational Organized Crime: While not specifically focused on cybercrime, this convention addresses organized crime, which often intersects with cybercriminal activities. It aims to prevent and combat transnational organized crime through international cooperation and legal measures.

3. Regional Initiatives: Various regional bodies, such as the European Union's General Data Protection Regulation (GDPR), have introduced comprehensive data protection and cybersecurity regulations to address cyber threats within their jurisdictions.

Challenges in Law Enforcement and Jurisdiction:

1. Jurisdictional Complexity: Cybercrimes often transcend national borders, making it challenging to determine jurisdiction. A crime committed in one country might originate from servers in another, complicating investigation and enforcement efforts.

2. Technical Complexity: Investigating cybercrimes requires specialized technical expertise. Law enforcement agencies face challenges in keeping up with rapidly evolving technologies and sophisticated cyber tactics employed by criminals.

3. Limited International Cooperation: Cooperation between countries for cybercrime investigations and information sharing is hindered by legal, cultural, and political differences. Mutual legal assistance treaties (MLATs) aim to facilitate cooperation but can be slow and cumbersome.

Role of Governments and International Organizations:

1. Legislation and Regulation: Governments play a crucial role in enacting and enforcing cybercrime laws, establishing frameworks for data protection, and implementing regulations to combat cyber threats.

2. Law Enforcement and Capacity Building: Governments support law enforcement agencies by providing resources, training, and technological infrastructure to enhance their capabilities in investigating and combating cybercrimes.

3. International Collaboration: International organizations like Interpol, Europol, and the United Nations Office on Drugs and Crime (UNODC) facilitate cooperation among countries, providing platforms for information sharing, capacity building, and coordinated efforts to combat cybercrime.

CASE STUDIES :

Some famous cyber crime cases :

1. The Melissa Virus

One of the earliest and biggest cyber threats came from the Melissa Virus in 1999 by programmer David Lee Smith. He sent users a file to open via Microsoft Word, which held a virus. Once opened the virus activated causing severe damage to hundreds of companies, including Microsoft. It is estimated it cost $80 million to repair the affected systems.

2. NASA Cyber Attack

In 1999, 15-year-old James Jonathan hacked and shutdown NASA's computers for 21 days! There were around 1.7 million software downloads during the attack, which cost the space giant around $41,000 in repairs.

3. The 2007 Estonia Cyber Attack

In April 2007, Estonia witnessed what is thought to be the first cyber attack on an entire county. Chiefly, it saw around 58 Estonian websites go offline, including government, bank and media websites.

4. A Cyber Attack on Sony's PlayStation Network

A cyber attack on Sony's PlayStation Network in April 2011 compromised the personal information of 77 million users.

5. Adobe Cyber Attack

The Adobe cyber attack was first thought to have breached the data of 2.9 million users. Moreover, it compromised the personal data of up to 38 million users! Adobe claims that only the passwords and credit card information of the first 2.9 million users were compromised, however, the remaining 35.1 million suffered the loss of their passwords and user IDs.

6. The 2014 Cyber Attack on Yahoo

In 2014, Yahoo was subject to one of the biggest cyber attacks of the year when 500 million accounts were compromised. During the attack, basic information and passwords were stolen, whereas bank information was not.

7. Ukraine's Power Grid Attack

The Ukraine's power grid attack in 2015 was the first cyberattack on a power grid. As a result of the attack, around half of the homes in the

Ivano-Frankivsk region of the Ukraine were without power for a few hours.

8. 2017 WannaCry Ransomware Cyber Attack

One of the biggest ransomware attacks of all time took place in 2017. Furthermore, it affected around 200,000 computers in over 150 countries. To sum up, the ransomware had a huge impact on several industries with a global cost of around 6 billion pounds to fix!

9. A Cyber Attack on Marriott Hotels

A cyber attack on the Marriott hotels and Starwood hotels group went undetected for years, which only came to light in 2018. Thus, by the time they became aware of the attack, an estimated 339 million guests had their data compromised. Consequently, the UK's data privacy watchdog fined the Marriott Hotels 18.4 million pounds.

10. The biggest password leak yet

In June 2021, we saw a compilation of about 8.4 billion passwords leaked in the RockYou2021 attack. In fact, it was the largest breach since the RockYou site in 2009 which affected 32 million accounts.

https://clearinsurance.com.au/10-biggest-cyber-attacks-in-history/

MITIGATION EFFORTS :

The UNODC Global Programme on Cybercrime ,according to General Assembly resolution 65/230, provides technical assistance and training to Member States to prevent and respond to cybercrime and technology-enabled crimes, including combating online sexual exploitation of children, responding to ransomware attacks and other cybercrimes, and collecting and preserving digital evidence. The Global Programme on Cybercrime is designed to respond flexibly to the needs identified in

Member States to prevent and combat cybercrime in a holistic manner. It does so by providing technical support in crime prevention and criminal justice, based on UNODC's assessment protocols and technical assistance tools. The programme utilizes an integrated approach to assist member states. It focuses on policy development and technical assistance, including capacity building activities, normative assistance, strengthening international and national cooperation within countries and with the private sector, and prevention and sensitization on the threats of cybercrime.

https://www.unodc.org/westandcentralafrica/en/Cyber-Crime.html#:~:text=The%20UNODC%20Global%20Programme%20on,responding%20to%20ransomware%20attacks%20and

CONCLUSION :

In the realm of the digital age, the pervasive shadow of cybercrime looms large, casting a profound impact on our societies, cultures, and the very essence of our interconnected world. From the clandestine depths of the dark web to the intricate web of cybercriminal networks, the exploration uncovered the nuanced structures and participants driving the cybercrime economy. Hackers, buyers, sellers, and the shadowy ecosystem of intermediaries actively engage in illicit transactions, perpetuating a thriving market that capitalizes on vulnerabilities within our digital infrastructure. As we conclude this exploration, the clarion call for concerted action reverberates. The SOCHUM committee stands as a beacon of hope, tasked not only with understanding the intricacies of cybercrime's societal and cultural impact but also with spearheading initiatives to safeguard our digital future. It is through collaboration, innovation, and unwavering determination that we shall forge a path towards a more secure, resilient, and culturally aligned cyberspace for generations to come.