JAMNABAI NARSEE INTERNATIONAL SCHOOL

G20
Study Guide

Table of Contents

Letter from The Chair

Dear Delegates,

I am extremely pleased to welcome you to the Group of 20 in International Youth Conference 2018.The Group of 20 is an international forum that aims to discuss key issues that the world faces today. I am honoured to be your Chair, I promise that this committee is going to keep you on your feet and is going to be an experience like never before. Each one of you have the power and responsibility to change and frame new policies for a better world.
Delegates the agendas of this committee address issues which have a long-term impact on each nation and it is vital to discuss them in order to map the road for a brighter future.

The world is on the brink of the 4th Industrial Revolution, a technological revolution which has the potential to help the world reach new highs and also the potential to take away the jobs of millions. This committee aims to question the existing cyber laws and frame laws to maximize the opportunity that avails the entire world. Delegates this agenda demands you to be spontaneous and think of unconventional ideas considering the dynamics of this committee.

The second agenda aims to address an issue that hampers our growth and questions conventional ideologies behind drafting banking policies. Infrastructural deficit is the root cause for pressing issues like weak GDP, poverty, lack of digital inclusion and much more. The world needs to unite and grow inclusively and sustainably for the betterment of future lives.
Delegates the committee is dynamic and holistic in nature and requires your expertise to shape the future it's your responsibility to act immediately in order to preserve the purpose of rules, laws and conventions because the rate of change and disruption possess the power to make all existing laws obsolete which will lead to a ruckus at a global stage which will be an unimaginable catastrophe.

With a combined Executive board experience of over 35 MUNs, you are sure to witness high quality debate. I would highly encourage delegates to use research to understand the agenda thoroughly and use research as a platform for their arguments and use their creativity to come with out of the box solutions. Make

sure that your research is unbeatable and you effectively voice out your opinions and solutions about the threats and opportunities that lie ahead.
Welcome to the Group of Twenty.

All the Best.

Regards,
Aarya Jhaveri, Chair,
Aliya Kamran, Vice Chair,
Angelina Minocha, R & D,
Harsh Jobalia, Moderator,
Khushi Chandani, Rapporteur

Agenda 1

Combating Cyber Threats in the 4th Industrial Revolution

I. Introduction

The 4th Industrial Revolution

Every few decades the world experiences a change, the introduction of something new that leads to a complete technological metamorphosis of humankind: an industrial revolution. Today at this exact moment a fourth industrial revolution is unfolding, it is characterized by a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres.[1] While the third industrial revolution was identified as the digital revolution, the fourth one is set apart by its velocity, scope, and systems impact in a number of emerging fields including robotics, artificial intelligence, blockchain, nanotechnology, quantum computing, biotechnology, The Internet of Things, 3D printing and autonomous vehicles.

The Fourth Industrial Revolution has the potential to raise global income levels and improve the quality of life for populations around the world. The technological innovation involved creates increased access to digital technologies for consumers and long-term gains in efficiency and productivity for producers. Some of the key advantages that are likely to occur as the revolution progresses include: increased reliability of industrial internet of things, evolved mobility of vehicles, improved responses of supply-chains etc. [2]

However, these advantages do not come without significant drawbacks.
This increased reliance on digital technology leads to grave cyber threats that require more advanced cyber security measures on a global scale. Possible threats include the hacking of transport systems - such as automated railways, traffic signals, cars, election interference, hacking of automated industrial machinery and even cyber-attacks on national defence systems.

Key Terms

The following are some of the key terminologies required for a thorough discussion regarding the same:

- **Cybercrime**- A crime in which a computer is used as a tool to commit an offense, it may involve the use of computer technology to access personal

information, business trade secrets or use the internet for exploitative or malicious purposes.

- **Cyberwarfare**- Involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks. [4]
- **Quantum Cryptography** - Uses our current knowledge of physics to develop a cryptosystem that is completely secure against being compromised without knowledge of the sender or the receiver of the messages.
- **Blockchain Cryptography** - Utilizes cryptography as a means of protecting the identities of users, ensuring transactions are done safely and securing all information and storages of value.
- **Ransomware** - A type of malicious software designed to block access to a computer system until a sum of money is paid.
- **Malware** - A software specifically designed to disrupt, damage, or gain authorized access to a computer system.

Additional Key Terms

- Malicious Artificial Intelligence
- Hackers:
    1. Black hat- They find private firms with weak security systems and steal confidential data.
    2. White hat- Also known as ethical hackers, remove viruses, perform pen tests and generally help people understand where their vulnerabilities are and fix them.
- Proxy
- Phishing

II. Historic Background

The unprecedented rate at which technologies are advancing has led to a growing number of consequences as well. Since the turn of the century the world has encountered multiple large-scale acts of cybercrime including, but not limited to, the following:

- **WannaCry**: A ransomware worm that spread rapidly across a number of computer networks in May of 2017. It was immensely damaging as it struck a number of important and high-profile systems, including many in Britain's National Health Service. It functioned by infecting Windows computers and encrypting files on the PCs' hard drive, making them impossible for users to access unless a ransom payment in bitcoin was made.

Symantec and other security researchers linked the attack to the Lazarus Group, a cybercrime organization that may be connected to the North Korean government. [5]

- **Political interference**: Within the past decade multiple cyber-attacks have occurred with the target to manipulate political scenarios. Some prominent examples of these include [6] –

- The leakage of the United States' democratic party candidate Hillary Clinton's personal emails in 2016. These were possibly released with the intent to create a bias against her.

- The malware attack on the French finance ministry at the G20 summit 2011 led to the exposure of sensitive financial information that shook the G20 team.

- The espionage operation in 2010 that stole classified documents from the Indian government and the office of Dalai Lama, which included documents related to Indian security, embassies abroad and NATO troop activity in Afghanistan. The attack used social network and cloud computing platforms. This attack placed a risk not only on global politics but also on national security for multiple countries.

- 2014 attack on the German Parliament, which lasted for several months and risked the privacy of the government and their data.

- **Monetary losses**: Cyber-attacks in the past few years have included several security breaches in the finance sector that have led to consequential amounts of monetary losses globally. These include:

- The 2017 Equifax data breach, where the financial data of nearly 145.5 million American citizens was stolen.

- The 2016 Indian banks data breach, where over 3.2 million debit cards were compromised.

- The 2012 credit card security breach, where nearly 10 million Visa and MasterCard customers' card data was compromised.

- The 2012 cyber warfare in Israel, where the stock exchange was disrupted.

Several other such breaches have occurred allowing for an approximate annual global cost of $152.81 million. [8]

Such cyber-attacks reached the recently developed blockchain system as well. Attacks on cryptocurrencies have now become regular and this is proving to be quite dangerous to several economies.

- 51% Attacks: Attackers use masses of computing power to take control of the blockchain and create alternate histories, thereby letting them spend their cryptocurrency twice. Because these attackers cover their tracks, no one quite knows what they do with the money, but there is no doubt that this breach is dangerous to the cryptocurrency network.

These types of attacks have occurred with many of the largest cryptocurrency networks including Monacoin, bitcoin gold, zencash, verge, litecoin cash etc. This high frequency of attacks on a technology that is central to the 4th Industrial Revolution raises the question of whether or not countries are prepared for the revolution.

- **Military Interference**: Cyber-attacks on military organizations across the globe has led to leakage of information regarding national defences, which poses as a grave threat to national security. Countries that have experienced such breaches include: USA (2008 attack on military computers), Iran (2010 Stuxnet attack), India (2010 espionage operation, Japan (2011 parliament attack), Canada (2011 hacking of government computers), Estonia (2007 breakdown of government websites) and many more.

Existing Problem

The United Nations has faced several challenges in the past while dealing with cybercrime due to its lack of definition in the UN charter. A common dispute has repeatedly occurred over Chapter I, Article 2, section 4, which states "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." and Chapter VII, Article 51, which states "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."

At the time during which the charter was framed cyber threats were close to non-existent, however today they are significantly perilous. Thus, many countries have raised questions like, "Does a cyber-attack constitute as a prohibited 'use of force'? If so, might a cyber-attack give rise to a right to use military force in self-defensive response pursuant to the rights reserved in Article 51?" [7]

With the forthcoming industrial revolution, essential systems providing water, electricity, healthcare, finance, food, and transportation are now increasingly software dependent, distributed, and interconnected. Hackers sitting on desks thousands of miles away can simply increase the pressure of an oil pipe in a middle eastern country and cause large scale damage to the economy and the environment. The Internet has made information exchange easier and more efficient, but it has also created a new space in which criminals and terrorists can

operate almost undetected. No longer is modern human conflict confined to the physical world; it has spread to cyberspace. Malicious cyber actors, internet distribution of child sex abuse material, e-mail scams and other transnational cybercrime activities are all examples of the threats that continue to rise in cyberspace. Current anomaly detection models focus primarily on analysing network traffic to prevent malicious activities, but it has been shown that such approaches fail to account for human behaviours behind the anomalies. [9]

Artificial Intelligence, which lies at the heart of the 4th Industrial Revolution acts as a major future threat as well. Cyberattacks performed by malicious AI raise the question of who should be held responsible for the crimes of such AI. Would it be the original developers or would the technology be shut down for its malicious acts? This would depend on the policies that a nation employs (although most countries do not have regulations to deal with such instances) or whether the AI was programmed to do something devastating or AI was programmed to do something beneficial, but it developed a destructive method for achieving its goal.

Another technological advancement that plays a large role in the 4th Industrial Revolution is 3D printing. While 3D printing was created with the intention of advanced manufacturing and larger access to goods, criminal purposes have been created out of it. The most significant one is the 3D printing of weapons. The world's first functional 3D printed gun was designed back in 2013 by Cody Wilson, a crypto-anarchist. Since then, designs of firearms for 3D printing have circulated across hundreds of thousands of computers. This has sent governments scrambling to impose laws that would control or prohibit 3D printed weapons, and in some cases even 3D models of firearms. Several countries such as USA, Australia, UK, Singapore and more have not wasted any time to ban these firearms and even the possession of their blueprints. However not all countries have taken such actions and the designs for these firearms have spread at a global scale due to the internet. Furthermore, the designs have travelled through the internet, which has made them technically available to everyone. Therefore, despite the attempts of countries' law enforcement 3D printed firearms have cropped up all across the world. Portals such as the dark web have also promoted

the development of these weapons and unless regulations are made on a more global scale stopping such weapons will continue to be a challenge.

Due to such threats and the lack of sufficient international regulation against cybercrime these cybercriminals often go unidentified or unpunished; causing the borderless crime industry to grow.

In Lisbon, Secretary-General Guterres emphasized his fear of such a catastrophe, noting that international law and nations defence systems are unprepared for, and have done little to mitigate the possibility of a major cyber-attack: "Episodes of cyber-warfare between states already exist. What is worse is that there is no regulatory scheme for that type of warfare, it is not clear how the Geneva Convention or international humanitarian law applies to it."

III. Conflicting Perspectives

The lack of a formal definition of a cyber-attack led to countries proposing their own definitions. One of these included the definition proposed by the U.S. National Research Council which classifies cyber-attacks as "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."

This definition focuses on the objectives of a cyberattack as opposed to the method of execution, which makes sense since broad objectives are sometimes easier to ascertain than the exact bug or virus used to disrupt the computer network.

However, this definition has not been accepted globally and experts argue that it fails to distinguish between a simple cybercrime and a cyber-attack. They believe that a simpler, more uniform definition that avoids ambiguity and overlap, and

facilitates a cleaner delineation between cyber-attack and cyber-crime should be created.

The Shanghai Cooperation Organization has expressed similar dissatisfaction with the definitions advanced by the US and other NATO nations. The SCO nations have often been diametrically opposed to NATO's cyber policies, which generally call for stricter definitions and stronger rights of retaliation. SCO nations have adopted an expansive vision of cyberattacks to include the use of cyber-technology to undermine political stability. According to the Shanghai Cooperation Agreement, one of the greatest cyber threats posed is the spread of information that is dangerous to "social, political and economic systems, as well as spiritual, moral and cultural spheres of other states."

NATO nations have not welcomed such a definition of a cyber-attack, as they fear it will lend legal legitimacy to the countries' efforts to suppress free expression and minority groups. China and Russia, on the other hand, see this clause as protection against Western interference in their affairs.

Western nations like the US and UK were willing to accept the agreement that imposed harsh sanctions against, unambiguous restrictions on, and the right to retaliate against aggressive acts in cyberspace. This was the one that the SCO countries argued against.

All in all, this conflict of interests has allowed the issue of cyber threats to persist in the world alongside the developing fourth industrial revolution.

IV. Recent Developments

In order to combat the growing the cyber threats several nations have begun to take independent action and have begun to form multilateral/bilateral treaties.

A] Bilateral Accords

1. **JOINT STATEMENT: The United States and India: Enduring Global Partners in the 21st Century:** The national leaders met in 2016 and discussed several different aspects regarding the development of their nations. Soon after their discussion a joint statement was published. In this they emphasized upon the opportunities that cyberspace creates as long as the internet is open, interoperable, secure, reliable, and underpinned by the multistakeholder model of Internet governance. They committed to enhance cyber collaboration on critical infrastructure, cybercrime, and malicious cyber activity by state and non-state actors, capacity building, and cybersecurity research and development, and to continue discussions on all aspects of trade in technology and related services, including market access.

2. **Singapore - Netherlands Memorandum of Understanding:** The Cyber Security Agency of Singapore and the National Cyber Security Centre of The Netherlands signed a Memorandum of Understanding (MOU) on cyber security cooperation to formalize their commitment to work together to foster a secure cyberspace in 2016. The agreement commits both parties to regular bilateral exchanges, sharing of cyber security and their best practices and strategies aimed at protecting critical information infrastructures as well as access to training and workshops.

3. **China-Russia Comprehensive Strategic Partnership of Coordination:** In 2015 the two countries signed the Sino-Russian cybersecurity deal which marked Sino-Russian cooperation in another arena—cyberspace. The treaty, which some have dubbed a "nonaggression pact" for cyberspace, details cooperative measures both governments pledge to undertake, including exchange of information and increased scientific and academic cooperation. With this, Russia and China continue to advance their vision of "information security," a view of security concerns in cyberspace that is markedly different from Western approaches of "cybersecurity."

Previously in 2011 the two countries had also submitted a proposal for an international code of conduct for information security to the United Nations, however the proposal failed to garner sufficient support.

4. **U.S.-EU Cyber Cooperation:** The United States and the European Union have worked in close coordination on cyber-related issues both bilaterally and in multilateral fora in the past. This cooperation was founded on the interest in an open and interoperable Internet of the two countries, and their commitment to multistakeholder Internet governance, Internet freedom, and protecting human rights in cyberspace. The cooperation has also established a working group in the past. This working group focuses on four areas where cooperative approaches add significant value to both regions: cyber incident management, public-private partnership on critical infrastructure cybersecurity, cybersecurity awareness raising, and cybercrime.

5. **Japan-Israel Innovation Partnership:** The Economic Policy Dialogue at ministerial level between the Ministry of Economy, Trade and Industry of Japan and the Ministry of Economy and Industry of the State of Israel was held in Jerusalem on May 3, 2017. Both sides welcomed the substantial development of the bilateral economic relationship and are pursuing Connected Industries as new vision for the future of industries.

The nations also expressed their expectation that the experts will analyze the cybersecurity challenges in new digital spaces (such as vehicles, aviation, medical IoT, etc.) as well as threats and risks in mass events.

B] Multilateral Accords

1. **Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security:** In 2013 they agreed that countries should not interfere with each other's critical infrastructure; they should not target each other's computer emergency response teams; they should assist other nations investigating cyber-attacks; and they are responsible for actions that originate from their territory.

The GGE offers its recommendations to promote peace and stability in State use of ICTs.

List of members: Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, Russia, United Kingdom, United States of America.

2. **The G20 Finance Ministers and Central Bank Governors Meeting Communiqué:** At the 2017 summit the member nations' Finance Ministers and Central Bank Governors discussed the malicious use of Information and Communication Technologies (ICT) and its impact on international financial systems.

3. **NATO Cyber Defense Pledge 2016:** In recognition of the new realities of security threats to NATO, the Allied Heads of State and Government, pledge to ensure the Alliance keeps pace with the fast-evolving cyber threat landscape and that the nations will be capable of defending themselves in cyberspace as in the air, on land and at sea. This pledge focuses on the idea that cyber defense is part of NATO's core task of collective defense and the main focus in cyber defence is to protect its own networks and enhance resilience across the Alliance.

NATO has taken other steps towards reinforcing cybersecurity on a global scale. This includes the formation of the Tallinn Manual in 2013.

4. **Joint Statement on Cyber Security by the Nuclear Security Summit:** In 2016, 29 states committed to ensure adequate cyber security at industrial control and plant systems at nuclear facilities. Increased attention in this area assists the nuclear operators and the supply chain to continue to strengthen the resilience of these systems, protecting them from potential malicious attack or accidental damage. The initiative involves participation in two international workshops on this topic.

5. **G7 Declaration on Responsible States Behavior in Cyberspace:** The Group of 7 remains committed to an accessible, open, interoperable,

reliable and secure cyberspace and recognizes the enormous benefits for economic growth and prosperity derived from cyberspace as an extraordinary tool for economic, social and political development. However, the nations are concerned about the risk of escalation and retaliation in cyberspace, including massive denial-of-service attacks, damage to critical infrastructure, or other malicious cyber activity that impairs the use and operation of critical infrastructure that provides services to the public.

Based on this idea the G7 has taken steps to promote security and stability in cyberspace. [10]

Despite the existence of several such bilateral and multilateral accords cybercrime continues to grow and pose as a serious threat to all nations. This is because of the absence of a binding cybersecurity law or code of conduct for the growing digital technologies. The growing intersection of biological, physical, and technical worlds requires a powerful cyber security response. Current technologies and cyber security solutions are starting to function more like human brains, processing and analyzing data to make complex decisions. The result of this shift, is that humanity is no longer just the beneficiary of technology; humanity is now inseparable from technology. And that means as the pace of innovation and transformation accelerates and the humanity-technology nexus irreversibly expands, the consequences of digital corruption or disruption are rising fast too.

C] Country-specific Policies

1. **USA:** The United States Department of Homeland Security deals with the cyber security measures in the country. Due to the approximately 400% increase in the number of data breaches in the US the government took action to strengthen their cybersecurity framework. The United States government has been working to introduce stricter laws to equip organizations to secure the data from the latest cyber threats. These include acts that invoke notifications regarding healthcare information, sharing of cybersecurity information with manufacturing firms and other voluntary public-private partnerships to improve cybersecurity for not only the government but also their citizens.

2. **Russia:** Russia's official approach is called "international information security". The strategy is based on four main concepts: Information space, Information security, cyberspace and cybersecurity wherein protecting information resources is a top national security priority. The regulations set by the country aim to systemize the actions of all the stakeholders involved with cyberspace. Despite the well-defined framework of information security in the country Vladimir Putin fired his internet advisor in June 2018, who is said to have failed to cultivate influence and put together a team of his own within the presidential administration.

3. **China:** China's Cybersecurity Law went into effect on 1st June 2017 and was framed to encompass both "network operators" as well as "suppliers of network products and services." The law takes a step further to allow the government to control and regulate data within the country and internet access through its Great Firewall. The law requires business information and data on Chinese citizens gathered within China to be kept on domestic servers and not transferred abroad without permission. In general, the law ensures a closed system of information security in the country.

4. **Israel:** Israel is considered to have cyber supremacy due to its advanced cybersecurity systems. Israel's National Cyber Initiative task force recognizes the fact that technology moves at an unprecedented speed and making a five-year strict plan would be ineffective, therefore the task force recommended developing an "ecosystem that will know what to do when unpredicted threats come." The ecosystem is a constantly evolving framework for collaboration between the government, businesses, and universities, with the government playing mostly a guiding, advisory role. This system allows the nation to continually gather intelligence and develop cybersecurity measures with respect to the rapid changes, resulting in the country being titled as the cybersecurity powerhouse.

5. **India:** India developed its National Cyber Security Policy in 2013. This policy aims at facilitating the creation of secure computing environment, enabling adequate trust and confidence in electronic transactions and

guiding stakeholder's actions for the protection of cyberspace. To accomplish these aims the government applied different strategies and even set up A national 24x7 mechanism to deal with cyber threats. India has also made attempts to set regulation for cryptocurrencies to eliminate their use in illicit transactions.

6. **DPRK:** North Korea's cyber security strategy utilizes cyberspace to ensure the survival of the Kim dynasty. They involve alleged cyberattacks that act as asymmetric weapons against a superior opponent's vulnerable information technology network. Furthermore, the country attempts to secure the cyber domain and control the information that runs through it strengthening the regime from outside attacks while dominating the domestic narrative.

V. Possible Solutions

As you might expect with a problem this large and complex, a range of solutions have been proposed in the past, however with the unprecedented rate of growth and development in the 4th Industrial Revolution there is a need for solutions that will last longer and apply to the vast variety of possible threats. Consider the following possible solutions:

1. **A Universal Legal Framework:** A set of recommendations on norms, rules, and principles of responsible behavior in cyberspace can be framed. Government experts from leading cyberpowers from all regions of the world could structure international laws, including the principles of the law of state responsibility, that would fully apply to state behavior in cyberspace.

Since the lack of clarity as to what rules apply in cyberspace is one of the factors contributing to instability and the risk of escalation, the explicit affirmation that international law is applicable to state activities in cyberspace, including to activities of non-state actors attributable to states, will allow the international community and affected states to react to violations more effectively. In cyberspace, states would have to comply with the prohibition on the use of force, the requirement to respect territorial sovereignty and independence, and the

principle of settling disputes by peaceful means in the same way as in the physical world.

2. **A specific, yet broad definition of a cyber-attack.** This could enable nations to identify cyberattacks more efficiently and take action accordingly. Inter-governmental bodies could use this definition to set laws to prevent cyber-attacks and monitor nations that breach those laws.

VI. Questions a resolution must answer

1. When should a cyber-attack be classified as a threat or use of force?
2. When, if ever, can a cyber-attack trigger the right to self-defense (Article 51)
3. How can the principles of necessity and proportionality be extended to address responses to cyber-attacks?
4. How should the law of national accountability be applied to or adjusted for cyber-attacks?

VII. Further research

It is essential to understand that this agenda's focus is on the 4th industrial revolution and therefore, delegates should focus on understanding the fast-changing technologies of the fourth industrial revolution and on finding solutions to the foreseeable cyber threats. In order to do this, it is necessary to understand the effectiveness of current cyber laws and find solutions on how the law will be relevant and match the disruption that the fourth industrial revolution will bring in the near future. The following links will provide as aid for this process.

[1]https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

[2] https://www.calamp.com/blog/2018/02/benefits-fourth-industrial-revolution/

[3]https://www.techopedia.com/definition/24748/cyberattack

[4]https://www.rand.org/topics/cyber-warfare.html

https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/1c6q2kc4v_50335.pdf

[5]https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

[6]https://www.cbronline.com/business/cybergate-5-major-political-cyber-attacks-4973433/

[7]http://unstudies.ir/static/fckimages/files/vol-87_III_waxman_cyberattacks.pdf

[8]https://www.statista.com/statistics/474928/average-annual-costs-caused-by-cyber-crime-worldwide/

[9]https://www.researchgate.net/publication/224223630_Dimensions_of_Cyber-Attacks_Cultural_Social_Economic_and_Political

[10]https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/G7+Declaration+on+Responsible+States+Behavior+in+Cyberspace+4-11-2017.pdf

https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf

https://carnegieendowment.org/publications/interactive/cybernorms

https://resources.infosecinstitute.com/invoking-article-51-of-un-charter-response-cyber-attacks-ii/#gref

https://cybersecforum.eu/en/2017-global-cybersecurity-policy-challenges-highlights

http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html

https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Agenda 2

Tackling Infrastructural Deficits for Inclusive Development

I. Introduction

Facilitating transport, promoting communication, providing energy and water, and boosting the health and education of the workforce enables the whole economy to flourish. The development and strengthening of logistical and transportation infrastructure has a potential impact both on economic development and poverty reduction. Infrastructure is the lifeblood of a modern economy.

Infrastructure has massive non-economic implications as well. A more efficient public transportation system can reduce greenhouse gas emissions and limit climate change. A national fiber optic network could facilitate the spread of new information faster than ever before. And a robust interstate highway system even supports American national security, allowing the military to move troops and supplies across the country in times of crisis.

The cost of building infrastructure is vast, but the costs of failing to make such investments are incalculable. Congested roads, antiquated air traffic systems, and clogged ports are just a few of the manifestations of an infrastructure deficit that is undermining our economic efficiency and lowering our quality of life. Decades of underinvestment in basic infrastructure have produced a variety of bottlenecks across transportation, water, freight, and communication networks.

Infrastructure projects are also a source of major employment that catalyze local economic growth and develop skills at all levels in the workforce which then provides the underpinning for developing new products and services, opening access to new markets and reducing waste and environmental impact.

In order to boost growth and counter the slowdown in emerging markets, efforts around the world must be stepped up to ensure that its benefits reach everybody in society. Inclusive growth also means making the best use of all resources and

the entire population, young and old, men and women. Labor market, education and training programs must all work to maximize opportunity and inclusiveness.

Without taking such steps countries will not be able to grow in a sustained way in the coming years. As the world is coming up against increasing resource constraints to growth which will be making it increasingly difficult to raise the level of economic growth without a larger share of the population participating in that process. Despite huge gains in global economic output, the current social, political and economic systems are exacerbating inequalities, rather than reducing them. Rising income inequality is the cause of economic and social ills, ranging from low consumption to social and political unrest, and is damaging to our future economic well-being. Sociopolitical instability and violence have been seen to follow episodes of highly uneven growth, either from absolute deprivation for some people or from a sense of unfairness when economic gains are shared very unequally. Hence, it is significant to ensure that everyone has the opportunity to benefit from global economic integration and technological progress with governments worldwide devoting attention and resources to the challenges of making growth more inclusive.

Key terminologies:

- **Infrastructure**- The term for the basic systems of a business or nation, for example transportation, communication, sewage, water and electric systems. These systems tend to be high-cost investments and are vital to a country's economic development and prosperity.
- **Infrastructural deficit-** Refers to the lack of infrastructural systems in certain economies. This occurs as a result of a steady decline in government infrastructure spending combined with a steady increase in the cost of building additional infrastructure.
- **Inclusive development-** consists of ensuring that all marginalized and excluded groups are stakeholders in development processes. In this context it applies to the development of infrastructure at a global scale, which prevents the exclusion of low-income countries.

- **Sustainable development**- economic development that is conducted without depletion of natural resources and low negative environmental impact.
- **Physical Infrastructure-** This consists of the tangible systems required for operation in a business or country. Roads, bridges, canals etc.
- **Social Infrastructure-** This involves the Knowledge, skills and efficiency needed by the citizens in a country in order for them to participate in the operations of their society.
- **Economic Infrastructure-** The facility of a country, which makes business activity possible. This includes financial services such as banking and investment.

II. Historic Background

The term 'infrastructure', since 1927, is used to refer to the systems responsible for "rolling out" basic power, water, sewerage, and communications services across geographical territories as public systems of standardized services.

Throughout history, countries have developed infrastructure at different rates, which has led to vast disparities in the availability and quality of these systems.

In the early 1800s the United States of America began developing infrastructure systems with the purpose of nation-building to bind the Republic together. Since then the country initiated several projects including the Works Progress Administration in 1934, which involved the development of schools, hospitals, libraries, firehouses, airports, water treatment plants, playgrounds, tunnels, roads etc. Since then the country has continued to invest in infrastructure heavily, which has caused the nation to rank 8th in the global infrastructure ranking.

Not many nations followed such patterns of infrastructural investment and their decisions were heavily influenced by large scale global events, such as war.

After World War II, nations were worried that a situation like the great depression may arise once again. In order to prevent this, governments of many nations initiated multiple infrastructure development projects. The United States, Soviet Union, Western European and East Asian countries in particular experienced unusually high and sustained growth, together with full employment during this period.

In July 1944, delegates from 44 allied nations met to regulate international monetary and financial order in the post-war era. This was known formally as the United Nations Monetary and Financial Conference. It ended with agreements about the creation of the International Monetary Fund (IMF) and the International Bank for Reconstruction and Development (IBRD), both of which played a role in infrastructural investment during the following years.

Despite such initiatives there has been an evident disparity among the infrastructure setups in different nations and even within nations. For this reason, the Millennium Development Goals were created. The intent was to promote a better and safer living standard for people in all countries. Although these goals created improvements all across the world, the imbalance in infrastructure quality and quantity has persisted. In 2005, G8 finance ministers agreed to provide enough funds to the World Bank, the IMF and the African Development Bank (AfDB) to cancel $40 to $55 billion in debt owed by members of the heavily indebted poor countries to allow them to redirect resources to programs for improving health and education and for alleviating poverty.

Throughout global history measures have been taken to promote a more inclusive infrastructure development, however national debts, war, political conflicts etc. have led to severe deficits in many countries. In the past, global organizations have been driven to take various measures to solve this problem.

III. The Problem

Infrastructure consists of hard and soft components. The hard and visible infrastructure, such as roads, railways, electricity, and telecommunications, must be accompanied and supported by its soft component, such as policies and regulations, to enable the system to perform well and generate impacts. The right mix and synergy of the two is important to ensure that the infrastructure system supports inclusive growth and poverty reduction. Well-functioning and efficient infrastructure promotes inclusiveness by expanding access to vital services and improving economic opportunities for all.

Slow progress in living standards and widening inequality have contributed to political polarization and erosion of social cohesion in many advanced and emerging economies. This has led to the emergence of a worldwide consensus on the need for a more inclusive and sustainable model of growth and development that promotes high living standards for all.

Most citizens evaluate their respective countries' economic progress not by published GDP growth statistics but by changes in their households' standard of living — a multidimensional phenomenon that encompasses income, employment opportunity, economic security, and quality of life. And yet, GDP growth remains the primary focus of both policymakers and the media and is still the standard measure of economic success.

What gets measured gets managed, and the primacy of GDP statistics tends to reinforce the amount of attention paid by political and business leaders to macroeconomic and financial stability policies, which influence the overall level of economic activity, relative to that paid to the strength and equity of institutions and policy incentives in such areas as skills development, labor markets, competition and rents, investor and corporate governance, social protection, infrastructure, and basic services. These play an important role in

shaping the *pattern* of economic activity and particularly the breadth of social participation in the process and benefits of growth.

A lack of infrastructure development signals barriers to growth and overall development. Unfortunately, developing Asia still shows a significant deficiency in infrastructure services, and this varies considerably across countries. About 1.8 billion people in the region are not connected to basic sanitation services, 0.8 billion lack electricity, and 0.6 billion do not have access to safe water. The key challenge is therefore to provide high quality and efficient infrastructure systems that can support more inclusive and higher economic growth. The potential of Asia to match Europe's current standard of living by 2050 is real, but it requires a continuation of the infrastructure development that has supported the growth over the last few decades. The challenges are enormous. In terms of funding, Investment in infrastructure is far less than what is needed to sustain vigorous growth and make it truly inclusive. The global infrastructure gap projected from now to the year 2035 amounts to USD 5.5 trillion according to some estimates. Meanwhile, institutional investors around the world have USD 80 trillion in assets under management, typically offering low returns.

A more prevalent problem that persists globally is the rural/urban infrastructure disparity. The manifestation of poverty goes beyond the urban-rural divide, it has sub regional and regional contexts. It is therefore critical, and there is great value to be gained, by coordinating rural development initiatives that contribute to sustainable livelihoods through efforts at the global, regional, national and local levels, as appropriate. Strategies to deal with rural development should take into consideration the remoteness and potentials in rural areas and provide targeted differentiated approaches. There are evident developmental gaps and disparities which tend to increase in the process of continued development. It might be due to differences in endowment of natural resources or technological development or manmade impediments and so on. As a result, the problem of disparity exists between rural and urban areas and has become more accentuated in globalization period. Rural areas tend to have more scattered layouts and limited planning since the time of early settlements. This leads to poor communication

and transport facilities, which often leads to shortages of other infrastructural developments.

A combination of the aforementioned issues requires united global attention in order to tackle the deficits and take decisions that bring results to the ideas of inclusive development.

IV. Recent Developments

WEF

The WEF proposes a measure of its own, dubbed the "inclusive development index." While it takes into account growth, as measured using GDP per capita, employment, and productivity, it also incorporates several other metrics, including gauges of poverty, life expectancy, public debt, median income, wealth inequality and carbon intensity. The index also considers investments in human capital, the depletion of natural resources, and damage caused by pollution.

This broader index of economic progress and wellbeing shows how the traditional measure of growth often falls short. In the past five years, almost a third of the 103 countries covered by the WEF index experienced a decrease in their inclusive development scores even as GDP increased. Among the 29 advanced economies in the sample, all but three have experienced economic growth over that period, but most—16 out of 29—saw their measures of social inclusion deteriorate, according to the WEF. Income inequality has risen or remained stable in 20 of these advanced economies, and poverty has increased in 17.

OBOR

The Belt and Road Initiative is geographically structured along several land corridors, and the maritime silk road. Infrastructure corridors encompassing

around 60 countries, primarily in Asia and Europe but also including Oceania and East Africa, will cost an estimated US$4–8 trillion. The initiative has been contrasted with the two US-centric trading arrangements, the Trans-Pacific Partnership and the Transatlantic Trade and Investment Partnership. These programs aimed at encompassing countries, financially, receive the support of Silk Road Fund and Asian Infrastructure Investment Bank; technically, are guided by B&R Summit Forum.

UNDP

The Sustainable Development Goals (SDGs), otherwise known as the Global Goals, are a universal call to action to end poverty, protect the planet and ensure that all people enjoy peace and prosperity. These 17 Goals build on the successes of the Millennium Development Goals, while including new areas such as climate change, economic inequality, innovation, sustainable consumption, peace and justice, among other priorities. The goals are interconnected – often the key to success on one will involve tackling issues more commonly associated with another. The SDGs work in the spirit of partnership and pragmatism to make the right choices now to improve life, in a sustainable way, for future generations. They provide clear guidelines and targets for all countries to adopt in accordance with their own priorities and the environmental challenges of the world at large. The SDGs are an inclusive agenda. They tackle the root causes of poverty and unite us together to make a positive change for both people and planet.

V. Country & International Organisation Policy

United States of America

Most of American infrastructure was designed in the 1960s, and since then the population has doubled. Thus, infrastructure is old and over-stretched. While European nations spend 5% of their GDP in developing infrastructure, the US spends only 2.4%.

Just taking into account bridges in danger: 4 in 10 US bridges are more than 50 years old, 56,000 were structurally deficient in 2016, 188m trips across a structurally deficient bridge per day (average) and it will take $123bn estimated backlog funding to rehabilitate bridges.

The American Society of Civil Engineers (ASCE) warns that "many dams are not expected to safely withstand current predictions regarding large floods and earthquakes". Overall, says the society, $4.6tn (£3.6tn) will be needed by 2025 to bring US infrastructure to an acceptable standard. Less than half that amount has so far been allocated for the work. Even water infrastructure is in a bad condition. Two trillion gallons of drinking water are lost every year from water main breaks and $1tn estimated funds are needed to maintain and expand pipe system. Trump's administration aims to use economic growths to fund infrastructure, but experts are not sure that it is a realistic goal.

Africa

The Economic Commission for Africa (ECA) has reiterated that infrastructure deficit in Africa remains a major challenge to trade facilitation, intra-regional trade as well as economic development and transformation on the continent.

Africa needs about 93 billion U.S. dollars annually until the year 2020 to close its infrastructure gap. Regional approaches and strategic partnerships to address problems of trade facilitation are increasingly being recognized since international trade involves the use of infrastructure and services of at least two countries.

"A regional approach is an efficient means of coordinating actions, setting priorities, reviewing progress, mobilizing resources, allocating funds, and monitoring contribution levels, with regard to solving common problems," said the Deputy Executive Secretary of ECA, Giovanie Biha.

"Africa must look inwards in financing its infrastructure development and dismantling obstacles to intra-Africa trade and the movement of persons across the continent," she said.

Biha noted the strides that the regional economic communities (RECs) are making in easing border pressures and promoting intra-Africa trade, and she cited the Chirundu One-Stop Border Post between Zambia and Zimbabwe as an excellent example of what the region can achieve with strong political will.

The population is growing fast in nations like Nigeria. World Population Prospects prediction that by 2050, Nigeria will displace the United States as the third most populous country in the world after China and India. More generally, economic growth has not kept up with population growth. Hence, the enormous slums outside city centers.

Tanzania-Zambia Railways (Tazara), one of the region's biggest post-independence infrastructure projects, is still plagued by derailments and breakdowns after almost four decades in operation.

Less than two percent of the rail line's cargo capacity is being used, according to a Tazara regional director who spoke to the Zambian daily Lusaka Times. Heavy goods have to be transported by other, more expensive means.

Still, transport infrastructure is not even the region's biggest problem, keeping the lights on is.

"The majority of countries in sub-Saharan Africa still experience regular power-outages, which of course contribute to a low productivity of many firms," said German Development Cooperation economist Matthias Grossmann.

Power is Africa's biggest infrastructure weak point, with as many as 30 countries facing regular power outages, according to a 2010 report by the World Bank and France's development agency.

Middle East

Middle East governments and industries continue to face challenges and pressure to perform and deliver "more for less" on social and economic infrastructure projects, despite an increase in oil prices compared to 2016.

The U.A.E has achieved the highest ranking in the Middle East and North African region for quality of infrastructure

"The UAE maintains its high ranking across several indices with its abundance of free trade zones, no corporation tax, the offer of full ownership and unlimited repatriation of profits still setting the benchmark for emerging markets," says Elias Monem, CEO of Agility Middle East and Africa. "The capital Abu Dhabi has several high-profile infrastructure projects coming online, and we are accommodating that growth through our expanding business. The countries in the region are moving aggressively to spur non-energy economic growth, create jobs, lure new investment, and develop knowledge economies."

The World Bank said, "Other countries that were highly ranked in the quality of infrastructure include Bahrain, Oman, and Saudi Arabia, ranking fifth, sixth and seventh respectively. MENA's population is projected to increase by more than 40% over the next few decades, and industrial demand is growing alongside it. The region will need to invest over $100 billion a year to maintain existing and create new infrastructure to serve the growing communities and cities across the region. And as we learned from the Arab Spring, these populations will hold their governments accountable to deliver it."

Oil exporters in particular have filled this need by supplying public financing that has largely been supported by natural resource revenues. But these revenues have been hit hard by volatile oil prices, alongside weaker growth in export markets such as the Eurozone and China. For a number of MENAT (Middle East, North Africa and Turkey) oil exporters, these trends create significant pressures to carefully consider their investment strategies and plans for the long term.

Fiscal reform to rationalize public expenditures can help ensure governments deploy sufficient resources for infrastructure. But unlocking and unleashing additional sources of capital will be critical to filling this gap. Global institutional and equity investors like pension funds, insurers, sovereign wealth funds and endowments hold trillions of dollars in assets. There are a number of ways MENAT

countries can make infrastructure projects more attractive and feasible. Here are just three of them.

China

China leads the world in infrastructure investment.

Infrastructure development remains a top priority for China's government, which has long recognized that a modern economy runs on reliable roads and rails, electricity, and telecommunications.

The foundations upon which new infrastructure is being developed are supporting continued rapid economic growth with railway, roads, airports, water, energy and rural projects seeing significant investment. The continued expansion of the high-speed rail and city-wide metro networks are prime examples of China's ambitions to further enhance its transport systems to benefit the wider economy.

For infrastructure investors, contractors, operators and equipment companies, China has for many years been and continues to represent a land of great opportunity, but also of significant challenges. Looking forward, China's impressive infrastructure building targets to 2020 are set to bring a major flow of infrastructure projects on stream. In order to benefit from infrastructure's stable cash flows and returns, domestic insurance, pension and other funds are increasingly being attracted towards the infrastructure sector.

Financing for infrastructure investment is likely to be a major consideration. The continued development of China's financial system and growing awareness of investors may see changes in the way infrastructure projects are financed and owned, and greater use of different project financing options.

Russia

Russia has a long way to catch up both on the increasing infrastructure investment as share of GDP and private sector participation. The share of private

sector as a percentage of cumulative infrastructure investments in Russia over 2006–2010 is estimated at 16%. The same indicator for the US was 29%, India — 40%, EU new members — 44%, EU old members — 64%, and Chile — 66%.

The main challenge in the infrastructure sector is that of consistently managing to structure and deliver projects that are both bankable and sustainable.

Russia is still developing its approach to the project life cycle, which broadly consists of three main stages: project origination, project preparation and, finally, project implementation and monitoring. The first two require substantial improvements for a PPP market to take off. The infrastructure market is still in its infancy in Russia with the first Russian PPPs achieving financial close only in 2010. With the notable exception of Pulkovo airport, none of the other transport infrastructure PPPs has yet completed the construction stage.

Russia has unique long-term potential for infrastructure development due to the healthy state of public finances, current high demand for infrastructure development and good prospects for such demand to continue.

European Union

EU countries are putting their prosperity at risk by spending too little on digital and transport infrastructure after years of chronic under-investment, the European Investment Bank has said in its annual investment report. The bank said that, although business investment was recovering, government investment remained at a 20-year low of 2.7 percent of EU gross domestic product. Overall investment has grown by an annual average of 3.2 per cent since 2013, well above the 1995-2005 average of 2.8 per cent. “We see a recovery, we see strengthening investment. But that is exactly the moment where you have to look at the long-term challenges,” said Debora Revoltella, chief economist at the EIB. “Much more needs to be done to put the issue of infrastructure spending into the political narrative, to explain that it’s for the good of the long-term health of the economy.” Creaking infrastructure limits growth by preventing businesses and

people from making the most of economic opportunities. Without investment to maintain and improve facilities, the capacity to produce goods shrinks, making growth slower in the longer term. This is not just a problem for the region's poorer economies — Germany suffers from one of the poorest digital infrastructure networks in the OECD economies. But countries hit hard by the region's sovereign debt crisis, such as Ireland and Spain, have made deep cuts to infrastructure investment to balance their books. Spending on infrastructure for the region as a whole is no longer falling but remains 20 per cent below its pre-crisis level and gaps between Europe's best and worst performers appear set to widen. Transport infrastructure, such as roads and bridges and rail links, is the worst affected. Recommended Brussels' heavy hand on Europe's digital economy A wobbly Merkel means a weaker Europe China's investment in Europe offers opportunities — and threats the report called for public infrastructure in investment to be made a priority at all levels, whether European, national or municipal. Fifty percent of spending takes place at the municipal level, according to EIB estimates. Of the municipalities polled, more than a third said they had invested too little over the past five years, against less than 1 per cent that said they had spent too much. However, business investment has staged a comeback. The level of corporate investment returned to its pre-crisis level earlier this year and the EIB poll indicated the recovery was likely to continue as companies remain bullish on the economic outlook.

India

India will require investments of about $4.5 trillion by 2040 to develop infrastructure to improve economic growth and community well-being, according to the Economic Survey 2017-18.

"The current trend shows that India can meet around $3.9 trillion infrastructure investment out of $4.5 trillion. The cumulative figure for India's infrastructure investment gap would be around $526 billion by 2040," it said.

There was massive under-investment in infrastructure sector until the recent past due to collapse of public private partnerships, especially in power and

telecom projects; stressed balance sheets of private companies; issues related to land and forest clearances, it said.

The need of the hour is to fill the infrastructure investment gap with financing from private investment, institutions dedicated to infrastructure financing like National Infrastructure Investment Bank and also global institutions like Asian Infrastructure Investment Bank and New Development Bank which are focusing more on sustainable development projects and infrastructure projects.

The Survey pointed out that there was scope for developing the shipbuilding industry, currently dominated by South Korea, China and Japan, in India. This will not only create a strong manufacturing base but also generate millions of jobs.

“India is located strategically on the international trade route, whereby it can attract ships plying from west to east in the trade route for its ship-repair activity. Geostrategic location of India, abundance of labor and quality of work are the strengths for the ship-repair business,” it said.

Further, it added that the share of Indian Railways in freight movement has been declining over a period of time primarily due to non-competitive tariff structure. “While the passenger fare had remained more or less flat, the freight fare has increased sharply over the year.”

The telecom sector is going through a “stress period with growing losses, debt pile, price war, reduced revenue and irrational spectrum costs,” the survey added. A new entrant has disrupted the market with low-cost data services and the revenue of incumbent players has fallen. The crisis has also severely impacted investors, lenders, partners and vendors of these telecom companies,” it said.

International Monetary Fund

In the face of crumbling bridges and super-low interest rates, many countries are talking and planning to increase spending on infrastructure. And it's not just about more spending; it's about smart spending. This is something that the IMF has urged countries to consider for several years, starting with our Fall 2014 World Economic Outlook.

Bridges, roads, and highways, along with telecoms, ports and airports are all part of the backbone that supports a country's growth and the global economy.

Investing in building schools, public housing and hospitals, known as social infrastructure, can provide a powerful impetus for economic activity and jobs in countries. Canada and the United Kingdom have announced and begun plans to invest billions in the coming years to fix and modernize their infrastructure, sorely in need of an upgrade. The incoming U.S. Administration has also indicated its intention to increase investment in infrastructure.

For the past several years, the IMF has analyzed the data and produced new research on the benefits and best way to spend taxpayer dollars on infrastructure. With interest rates still low, the IMF research suggests that debt-financed investment could virtually pay for itself by boosting demand in the short run and productivity in the long run. But that comes with a caveat: the quality of investment matters. So, countries should invest well, where there is a clear need, and invest efficiently.

Two weeks ago, IMF Deputy Managing Director Tao Zhang gave a speech about how countries can meet the growing needs, and challenges, of investing in public infrastructure.

VI. Questions a Resolution Must Answer

1. How can cooperation among countries and sharing of information be achieved?
2. What is the role of the G20 in promoting bilateral and multilateral agreements between countries? And how can it do so?
3. What targets and indicators should be used as a measure of inclusivity of growth?
4. How should globalization be addressed in regards to urbanization?
5. How should the issue of unequal opportunities be tackled as a consequence of urbanization to promote inclusive growth?
6. What methods should be utilized as an engine of inclusive growth and sustainable urbanization?
7. What comprehensive and holistic approach can be adopted to adequately address the topic of improving global access to financing;

VII. Additional Resources

http://www.oecd.org/futures/infrastructureto2030/infrastructureto2030volume2mappingpolicyforelectricitywaterandtransport.htm

https://ppiaf.org/activity/global-analysis-global-trends-infrastructure-policies-related-unsolicited-proposals-and

http://www3.weforum.org/docs/WEF_II_InfrastructureInvestmentPolicyBlueprint_Report_2014.pdf

https://www.weforum.org/reports/infrastructure-investment-policy-blueprint

https://www.cfr.org/backgrounder/state-us-infrastructure

http://www.dw.com/en/poor-infrastructure-is-key-obstacle-to-development-in-africa/a-15264436

https://www.csis.org/analysis/global-infrastructure-development

http://www.worldbank.org/en/topic/publicprivatepartnerships/brief/global-infrastructure-facility-backup