

# STUDY GUIDE

**ECOSOC**  
IașiMUN 2019



## Table of Contents

<b>Welcoming letter</b> .....	<b>3</b>
<b>Introduction to the committee</b> .....	<b>4</b>
<b>Topic A: The Issues of external debt</b> .....	<b>5</b>
1. Overview of the topic .....	5
2. Key terms .....	6
3. Historical background .....	7
4. Current Situation and Issues .....	8
5. Position of major actors .....	10
6. Points to adress .....	11
7. Further reading .....	11
<b>Topic B: Below-replacement fertility</b> .....	<b>13</b>
1. Overview of the topic .....	13
2. Key Terms .....	14
3. Historical background .....	14
4. Current Situation and Issues .....	16
5. Position of major actors .....	17
6. Points to adress .....	20
7. Further reading .....	20
<b>Topic C: Combatting cybercrime</b> .....	<b>21</b>
1. Overview of the topic .....	21
2. Key Terms .....	21
3. Historical background .....	23
4. Current Situation and Issues .....	24
5. Position of major actors .....	26
6. Points to adress .....	28
7. Further reading .....	29

## *Letter from the chairs*

*Honourable and lovely delegates,*

The board is ecstatic to have you, wonderful people, both novice and experienced delegates, in the **Economic and Social Council of Iasi Model United Nations Conference 2019**. Congratulations for choosing to make a difference for yourself and for the community you are part of!

Let us introduce you to the world you are about to enter. This is the committee where no one is afraid to speak, everyone has their own voice, no one is left behind in discussions, everyone shares the positive energy and each and everyone spends valuable and great time. We, as chairpersons, are here for you to share the pride of seeing you grow. More than anything, we will be dedicated to you, body and soul, all along this challenging, but beautiful process of debating.

Being two girls armed with ambition and desire, we assure you will not lack diversity in feelings, approaches and mentalities, as we complete each other as you complete us. We consider that every chairperson should share the same enthusiasm a first timer experiences and we can assure you that we do. Alternatively, we expect to see in you the passion we had as debaters.

This year's topics are in your hands, delegates. You are indebted to the world which was given as a gift to you at the moment of your birth. Resolve these problems in order to pass it on to the new generations, at least as prosperous as it was given to you.

We can hardly wait to find out what solutions you come up with in order to solve the issues proposed by us through these topics, which, let's face it, are not very approachable and easy to debate on. We truly believe in you and your abilities to transform our topics into fruitful debates, but if you have any questions in regards to the topic, conference, MUNs in general or any type of questions, do not hesitate to address them because we will try our best to help you. We are looking forward to meeting all of you!

*Sincerely, your chairpersons,  
Chiriac Nicola-Delia and Alexandra Corduneanu.*

## *Introduction to the committee*

The Economic and Social Council (hereinafter ECOSOC) was established in 1945 by the UN Charter as one of the six main bodies of the United Nations and is dedicated to sustainable development. It is the principal organ of the UN for coordination, dialogue and finding solutions for issues regarding economic, social and environmental issues, and, subsequently, implementing them in all the member states. The 54 ECOSOC members meet in two annual meetings, one organizational session and one substantive session, after which they write a report for the General Assembly. Even though they are elected yearly, also, by the General Assembly, they have a mandate of three years, based on their geographical position. In recent years, the council has been divided into five regional commissions, as well as eight functional commissions, separated by topics, in order to ensure extensive research on each department done by professionals.

Furthermore, there is a number of non-governmental organisations that have received consultative status to the Economic and Social Council, meaning that they are concerned with most activities of the Council and that have a substantial role in achieving the Council's goals. As of 2018, there are 5081 organisations with consultative status that are entitled to deliver oral presentations about their activities during the Council's meetings.

The most recent and well-known decision taken by the Council is the elaboration of the Sustainable Development Goals in 2015, a collection of 17 goals concerning all member states which are to be reached in 2030. They have been discussed in the United Nations Conference on Sustainable Development and guided by the former Secretary-General's statement, "We don't have plan B because there is no planet B".



## ***Topic A : Issues of external debt***

### **1. Overview of the topic**

Debt, whether internal or external, has always been a solution for a country to pursue different activities that require funds the government does not have.

External debt have been classified into four heads by most economists :

- Public and publicly guaranteed debt
- Private non-guaranteed credits
- Central bank deposits
- Loans due to the IMF

Moreover, in recent years, LDCs have been more and more encouraged to take out loans, in order to achieve economic growth and development. Even though, the government can plan ahead the way in which the funds will be used, they are not safe from potential unforeseen issues. These issues include weather phenomena, economic recessions, problems with the said government or usual delays.

The vicious cycle starts when they start borrowing more money to finish the project and are left with more debt than they have predicted and have to start cutting off funding on certain sectors that they consider “not that important”, namely education, healthcare or plans that concern the protection of the environment.

However, if we take a look on the list of the countries with the highest external debts compared to their GDP, ten out of the first fifteen countries are part of the European Union, with Luxembourg having the highest ratio, 6307% of their GDP in 2017. Nonetheless, many of these countries have a positive NIIP value, meaning that they can afford to have such large sums of indebted money. The downside is that these countries, out of too much confidence, tend to forget about the said unforeseen circumstances, alongside the possibility of devaluation in the exchange rate, which would, ultimately, lead to them not being able to pay the money back.

## 2. Key terms

**External debt** = the amount of debt a country owes to foreign creditors such as other governments, private commercial banks or global institutions (World Bank/International Monetary Fund)

**Least Developed Countries** = low-income countries facing issues concerning sustainable development; there are currently 47 countries deemed by the Committee for Development as LDCs (including Afghanistan and Niger)

**Tied loans/aid** = loan made by a government to a foreign borrower, provided that the borrower will use the funds to buy products from the country lending the money. There has been endless criticism directed towards tied aid due to the political aspect of it, as it seems that it rarely actually helps the country receiving the money.

**Debt relief/Debt cancellation** = partial/total forgiveness of debt or the slowing or debt growth that is considered a viable solution for the underdeveloped countries failing to pay back the external loans in due time

**Debt-to-GDP-ratio** = the ratio between a country's debt and its total economic output (measured by gross domestic product). The World Bank considers that if the debt-to-GDP ratio is higher than 77% for a long period of time, the economic growth of the country is slowed down.

**Economic recession** = a significant decline in economic activity across the economy, lasting more than a few months, normally visible in real GDP, real income, employment, industrial production, and wholesale-retail sales (according to the US National Bureau of Economic Research). According to the IMF, the world enters global recessions over a cycle that lasts between eight and ten years, which means that during a recession, countries are unable to pay their debts, since they cannot sustain themselves.

**Net international investment position (NIIP)** = the difference between a country's external financial assets (all assets owned abroad) and liabilities (owed money). The NIIP states whether a country is a creditor nation, when they have a positive NIIP value, or a debtor nation, when their NIIP value is negative.

### 3. Historical background

At the beginning of the early modern times, the powerful monarchs of Europe would often take out loans for wars from wealthy citizens or foreign monarchs willing to help and, afterwards, refusing to pay them back. Thus, William III of England created the first central bank in England, in order to fund the government for his war against France, and, subsequently, other English wars and Imperial conquests. Afterwards, the syndicate of traders and merchants became the Bank of England, in order to keep track of the money lent to the national government and other countries' governments.

Maybe the most well-known loan made by a foreign country towards others is the Marshall Plan. In a decade when the war destroyed most of European economies, preventing them from continuing the industrialisation process, the Marshall Plan became the epitome of how potential recessions could be prevented, even though the funds coming from the United States were only the headstart. When used cautiously, external loans can be extremely useful for development and industrialisation, which was what the European countries needed after the second world war.

However, it has been shown that this tactic doesn't work quite as well on LDCs and this is why many organisations have been created with the sole purpose of helping these countries get rid of poverty. For example, Eurodad (European Network on Debt and Development) is a coalition of 47 non-governmental organisations that was created in 1990 to work on issues related to debt, poverty reduction and development.\

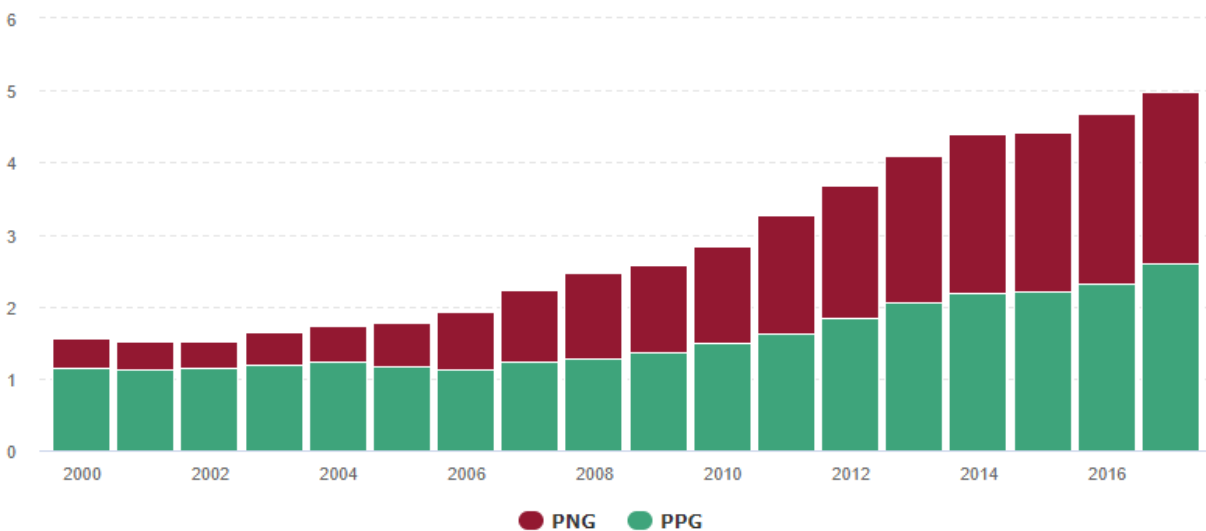
Their stated goals are:

- “Push for development policies that support poor and democratically-defined sustainable development strategies.”
- “Support the empowerment of Southern people to chart their own path towards development and ending poverty.”
- “Seek a lasting and sustainable solution to the debt crisis, appropriate development financing, and a stable international financial system conducive to development.”

Eurodad has focused on the issue of illicit capital flight, as well, because it has been discovered that more than 50% of these illicit financial flows originate from poor to rich countries, affecting and aggravating the incidence of poverty and need of taking out loans.

#### 4. Current situation and issues

As previously mentioned, one very grave issue is in regards to the LDCs and their need of taking out loans from foreign creditors or global institutions. As of recently, more and more countries with developing and transition economies rely on external funds, making the total external debt stocks in developing and transition economies almost 5 trillion US dollars in 2017. Also, there seems to be a shift towards the private sector debt since 2007, and now, more than 60% of external public debt of said developing countries lay in the hands of private creditors.

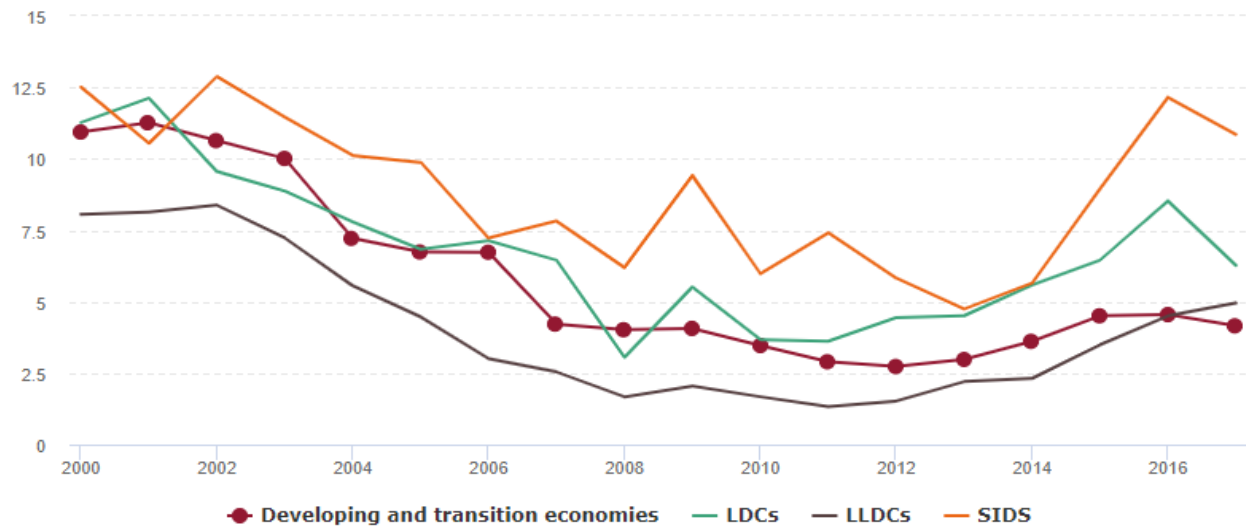


(PPG = public and publicly guaranteed ; PNG = private non-guaranteed)

Debt service ratios are important indicators of a country's debt sustainability (the ability of a country to meet the government's debt obligations), calculated as a proportion of exports of goods and services. If, until 2012, the developing countries reported a fall in this ratio (increased export earnings, reduction of debt servicing, or a combination of both), when debt service reached 2.7% of exports, in 2017, it rose again to 4.2%. The figure below shows the ratios reported in different groups of countries, as well as the average ratio.

LDCs have had a chaotic evolution in regards to the debt service ratio, due to the volatile commodity prices, amongst others. SIDS have the same issue, but different causes, as their exposure to natural disasters lead to the volatility of their main revenue sources.





( LDCs = least developed countries; LLDCs = landlocked developing countries ; SIDS = Small Island Developing States)

Another issue related to debt is the Eurozone debt crisis, although the problem is mainly tied to internal debt from private commercial banks. This crisis has been taking place since the end of 2009, and at first, countries relied only on internal loans, but, since the crisis has not gotten any better, countries, such as Greece have been taking out foreign loans as well, reaching a ratio of 228% of their GDP in 2017.

The causes were multiple:

- There were no penalties set by the Maastricht Treaty (which founded the European Union) for countries that exceeded the debt-to-GDP ratio, mainly because Germany and France were also spending more money than they had, and it would have stopped their economic growth. Also, they wanted to strengthen the euro's power and the transactions made by the European countries only helped their goal.
- The Eurozone system includes having a monetary union through the same currency (euro) but without a fiscal union, common taxation, pension and treasury functions. Also, the differences in work ethics, retirement ages and budget discipline made it very hard for the European countries to remain economically independent.
- Loss of confidence played a huge role in the quick escalation of the debt crisis, with it being as much political as it is financial. The banks that suffered the biggest losses were located in countries such as Greece or Spain, considered to be weak countries.

## **5. Position of Major Actors**

### **European Union**

The European Union tried coming up with different solutions in order to stop the Eurozone debt crisis. In 2010, the EU, alongside the IMF, disbursed 110 billion Euros to Greece, with a second bailout of approx. 140 billion Euros in mid-2011. Other countries that have received bailouts are Ireland and Portugal, around the same time.

The European Financial Stability Facility (EFSF) was created by the Eurozone members to provide emergency aid to countries in economic difficulty, as well as the European Financial Stabilisation Mechanism (EFSM).

Regarding the funding of LDCs, the European Union has created the European Development Fund (EDF), the organisation that provides aid in African, Caribbean and Pacific countries, as well as the special territories of the European Union, the 31 territories of EU member states that enjoy special status for historical, geographical or political reasons.

### **The United States of America**

Although the president of the United States and most people are not concerned about the US external debt, according to the Government Accountability Office, the country is on a “fiscally unsustainable” path because of projects on which the spending will increase, such as Medicare or projects within Social Security.

Another important problem the United States of America faces is the high holding of government debt by the People’s Republic of China, which is considered by many a strategy to replace the US dollar with the yuan as the world’s global currency. However, China is basing their economy on the competition between the two currencies and their trading, so the collapse of the dollar would only disrupt the international markets.

### **Luxembourg**

Having the highest debt-to-GDP ratio, namely 6037%, also, doesn’t represent a very big issue for the country’s government, since their NIIP values are positive and, overall, they are considered to be one of the most prosperous countries in the world. Their efforts to reduce their external debt come at a slow pace, with their taxes being raised more and

more everyday, with their tax on alcohol standing at 17% in 2018. Also, the student loans and scholarships have been lowered at public universities due to the cutting of funds.

### **Afghanistan and Niger**

Afghanistan and Niger are two of the countries considered to be at a very low rate of development by the United Nations, with the latter being one of the problematic debtors, historically speaking. As with many LDCs, they have been reluctant to take out loans, recently, from external sources because of the risks of not being able to pay them back.

## **6. Points to be addressed**

- Is debt cancellation a viable solution for LDCs in urgent need of funds for development?
- How can the most powerful countries contribute to the economic vicious cycle the LDCs enter whenever they borrow funds from external sources?
- How can the United Nations speed up the process of implementing the 17 SDGs, in order to minimise the impediments in sustainable development?
- How can the LDCs keep their debt sustainable?
- How can the Eurozone countries, mainly the ones still greatly affected by the crisis, achieve financial success and overcome their issues?

## **7. Further reading**

<https://sustainabledevelopment.un.org/?menu=1300>

[https://en.wikipedia.org/wiki/List\\_of\\_countries\\_by\\_external\\_debt](https://en.wikipedia.org/wiki/List_of_countries_by_external_debt)

<https://www.economicshelp.org/blog/14874/debt/problems-of-external-debt/>

<https://www.investopedia.com/terms/e/external-debt.asp>

[https://www.un.org/ga/search/view\\_doc.asp?symbol=A/73/180](https://www.un.org/ga/search/view_doc.asp?symbol=A/73/180) - report of the Secretary-General on external debt sustainability and development

<http://www.tffs.org/pdf/edsg/ft2014.pdf>

<https://www.investopedia.com/terms/e/european-sovereign-debt-crisis.asp>

## **Topic B: Below-replacement Fertility**

### **1. Overview of the Topic**

The world is fighting (more with than against) an insidious phenomenon: below-replacement fertility. Even if the total population increases, this has not been due to more people being born, but primarily to the development of medicine. Over the centuries, it has progressively treated most of the deadly illnesses and moreover, it has provided treatments for various inoffensive conditions which could have brought up severe complications. Hence, life expectancy is remarkably higher and so are living standards.

It is important to notice that the increase of the population is not based on new resources, but on the same old ones - which will sadly, but inevitably vanish at some point. If there are no new births to take on the “responsibility of growing old” than it is left to the world to run on the remaining resources until extinct.

Fortunately or unfortunately, neither the causes nor the effects of below-replacement fertility became immediately noticeable. The phenomenon itself is a sum of factors which have drastically changed both governments’ institutions and individuals on multiple levels. Among the factors responsible for below-replacement fertility levels are lower child mortality rates, widespread education, increased urbanization, improvements in the status of women, including increased employment and economic independence, availability of modern contraceptives, delayed childbearing as well as the decline of marriage and pension systems and increased costs of childrearing. Available demographic evidence suggests these factors will persist and become widespread globally.

The consequences - some of which disastrous - are no fewer: altering the composition of labor force, decreased wages and overall productivity, declining demand for services and goods, pressure put on governments for the elders’ needs, overstrained youth obliged to supplant an economic whole, and last but not least, the declining interest for the education system whose quality will diminish - the root of most problems in the world.

## 2. Key terms

**Replacement:** The term refers to the 1:1 ratio between the number of deaths and births among a current generation. The concept is rather logical and does not represent a statistics made at a certain point in time: the number of deaths is “invisioned” and is equal to the number of people at that moment. Thus, it is only natural that unless an equal number of births is recorded and no external factors are involved, the nation will gradually become narrower and narrower and eventually become extinct. The demographical process of “replacement” means counterbalancing a death - a decline in the number of people - with a newborn - a rise in the number of people, as to keep the total number constant. Thus, the word “replacement” could be translated to “constancy”.

**Below-replacement fertility:** If the replacement fertility ratio is 1:1, below-replacement fertility means that there will not be sufficient births to equal the number of deaths. Taking into consideration the fact that only females can give birth and that every child comes from two parents, then the below-replacement fertility indicator is under 2. If the ratio were met, then both the mother and the father would have a successor to take their place and maintain a constant population. Otherwise, not every person will be replaced and young people will be noticeably fewer than the old people within the same generation.

**Fertility:** The term refers to the number of births women would have, on average, during their reproductive lifetime in the absence of mortality. The common measure of fertility is known as the period total fertility rate (TRF). A TFR of 2.1 is often referred to as the replacement level fertility. Why the .1? Within the view of this topic, when a person is born, they are expected to grow and procreate as to demographically replace themselves after their death. Unfortunately, the infant mortality (global value: 29‰) does not permit it 100%. The extra 0.1 is a margin safety for any occurring destabilising conditions.

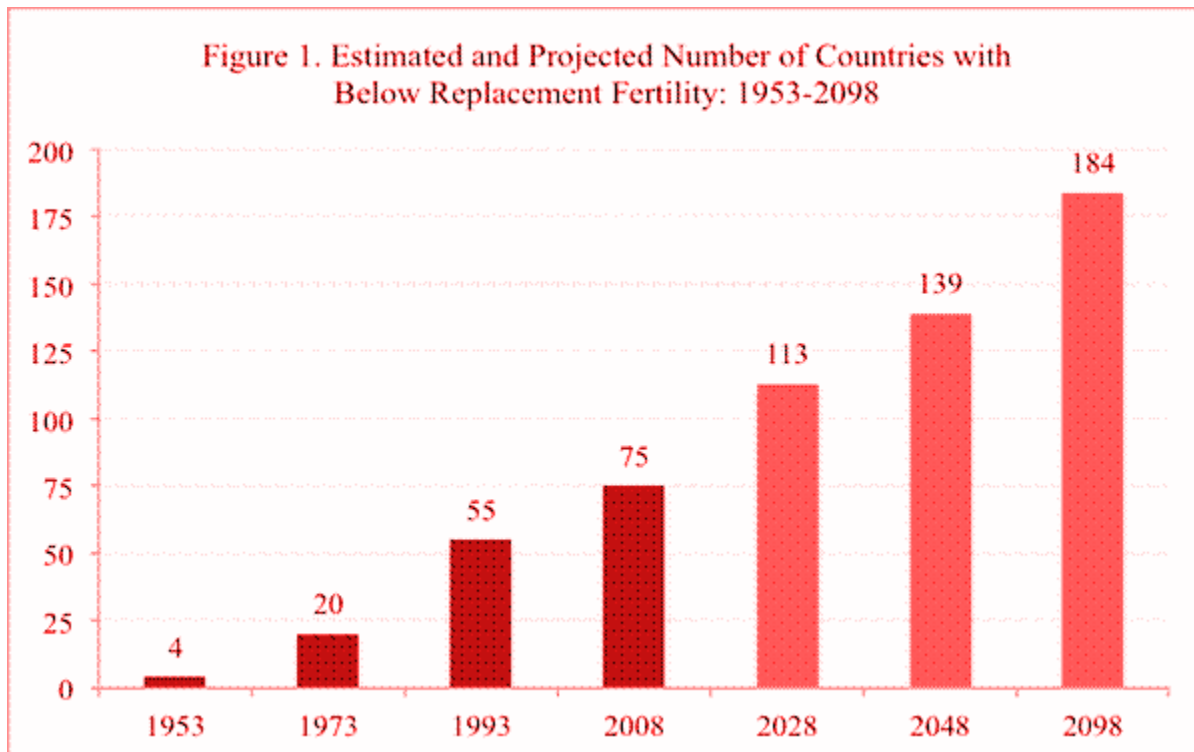
## 3. Historical Background

Fertility at or above replacement levels has prevailed for most of human history: by definition, it was necessary for human survival. As a long-term average, fertility must have been slightly above replacement. Nevertheless, below-replacement fertility is not a new phenomenon. Many human populations did become extinct in the remote and not so remote past. In most of the cases it was because of a high mortality rate that raised the

level of fertility needed to replace the population. If in the past, the mentality towards fertility behaviour permitted establishing a new balance (the lowest fertility level being of 2.79 in France at the beginning of the twentieth century), nowadays the same problem requires modern solutions.

Total fertility levels below two, unambiguously below replacement, became common in many countries of the West in the period between World War I and II. This raised considerable concern about depopulation, even though population growth still continued, as the changed age distribution temporarily delayed the onset of a decline in population numbers. After World War II, fertility levels rose significantly, creating the unexpected baby boom. But by the late 1950s in the United States and in the early 1960s in much of Europe, the trend reversed and fertility fell rapidly. During the demographic transition, in conjunction with a decline in mortality, fertility within marriage fell sharply. For the first time, fertility control was practised on a wide scale.

By the end of the twentieth century, virtually all developed countries and a few developing countries exhibited below-replacement fertility. Italy, Spain, Germany, Japan, and South Korea, had TFRs not much above 1.



#### **4. Current situation and Issues**

One of the alarming consequences of the phenomenon is change in distribution of the world population which lead to dramatic swings in the locus of global political and economic power. The recent economic growth and rise of China to superpower status, and the relative decline of Western Europe, can partially be attributed to the underlying population base.

Not only externally, but also internally will the distribution affect social and economic standards. The increase in the number of older people and the reduction in the number of children has strengthened the major industry supporting the elderly (medical care) and weakened the major industry supporting children (public education). Although expenditures per pupil have risen, the real income of teachers has diminished, and the quality of people entering teaching, as measured by test scores, has deteriorated. Thus, it is not surprising that, the ablest college graduates are choosing training for the proliferative medical care industry than entering the industry of public education. Unless fertility rises above replacement, primary education will not again become a high growth industry and fewer brilliant people will rise from a smaller population.

Continued low fertility also changes the age composition of the labor force in such a dramatic way that between 1901 and 1981 the number of elders along with the costs of their pensions has doubled, whereas the one of newborns has halved. Affected were some of the world's largest economies, such as China and Japan. The youth, who is supposed to load the economic mechanism, enters the labor force in positions with low pay and little authority. Competition lacking, the normal expectation of advancement cannot be sustained. Government's urge to fill the economic gap pressures the young force who receive smaller wages for double the work. Majorizing the retirement age is foreseen, but the overall productivity will be comparably lower because of the increase in the median age of the workforce. At the same time, a small number of entrants relative to the number of older workers result in the absence of the qualities young workers offer, such as vigor and adaptability to new technology.

What is more, a consumer market revolution is foreseen including decline in the housing market, and other fields which used to fuel the economy. Continued move toward a world with fewer children will not only significantly reshape consumer markets but, given a positive association between birth rates and GDP growth, will also jeopardise the vitality



of urban economies in the future. A study made at Harvard University has found that “10 % growth in the population ages 60 and older decreases growth in GDP per capita by 5.5%.” The consumer market, the goods and services demand, the incentive to immigrate and self-sustainability are endangered.

## **5. Position of Major actors**

### **China**

China’s fertility decline to below-replacement level occurred over three decades and in three phases. Most of the decline took place in the 1970s, before the launching of China’s one-child policy in 1980. In the early 1990s, fertility dropped below replacement level and since then, has further declined to around 1.5 births per woman today.

In November 2013, China announced a historical yet cautious step towards phasing out one-child policy. Couples who are both only children were now allowed to have a second child. Despite the enthusiastic and popular response to the announcement, only 2.5 % of the estimated 11 million eligible couples had applied for approval to have a second birth, far below all the projections made before the policy change.

Assuming a fertility level of 1.47 births per woman, the proportion of Chinese aged 60 and above will rise to 25 per cent by 2030. Over the same 20-year period, the number of Chinese in this age group will rise from about 180 million to more than 350 million. This places China, along with the Republic of Korea, and to some extent Japan, among the fastest-ageing societies in the world.

### **Italy**

In Italy, the declining fertility rate is causing concern, as it currently sits at 1.33. The average age for first-time mothers in Italy is 31 years old, the highest in Europe. A large reason that women in Italy are not having children is because they are not financially ready to raise a child, and the government doesn’t help with the cost of childcare. The low fertility rate combined with a longer life expectancy has left Italy with a significantly older population (a median age of 45.9 years compared to Europe’s median of 42.8 years).

Declining fertility rates, combined with longer life expectancy, has also left Italy with a significantly older population. Its median age is 45.9 years compared to the EU's median of 42.8, higher than any other European country except Germany.

Population forecasts predict 27 % of Italians will be aged over 64 by 2030, compared to just 18 % at the start of the century. By contrast, the share of population aged between 25 and 44 decreased from 30.6 to 26.3 % in the last 15 years.

The shrinking of the working-age population is threatening the sustainability of the country's pension system. Total pension expenditure is already the second highest in the EU, at 16.5 percent of GDP.

### **Norway**

Norway is another European country experiencing falling fertility rates, at 1.68 children per woman. An important factor in Norway for the decrease in childbirths is the increasing age for first-time mothers, which sits at an average of 29.5 years. Additionally, there are fewer larger families. This will harm Norway in the long term, as there will be fewer people of working age to pay the taxes that fund Norway's welfare systems. Norway is exploring options to encourage childbirth, such as paying a mother in pension savings for each child born.

### **South Korea**

In 2018, South Korea's total fertility rate fell to less than one child expected per woman, a record low. South Korea is the largest country ever to have fallen below one. In the long run, such a low birthrate could cause slower economic growth, less innovation, greater inequality, less stable public finances, greater intergenerational conflict, and more difficulties integrating immigrants.

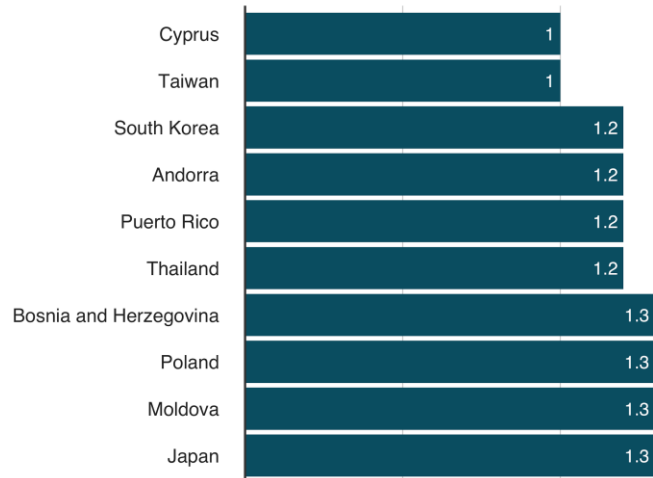
Understanding as much, since 2006, the government has tried tax incentives, expanded child care, housing benefits, special holidays for baby-making for some government workers, support for in vitro fertilization, generous parental leave from work, subsidized play dates, and other benefits. Their goal was to increase the total fertility rate to 1.6 children per woman by 2020. And while birthrates did rise as high as 1.3 kids per woman in 2012, they have fallen sharply since. That failure—despite at least \$130 billion in spending - has understandably led many policymakers and commentators to look for new policy tools, like egalitarianism. South Korea's ongoing social campaign to induce men to do more housework is a good example.

## Niger

At the other extreme, Niger ranks number 1 in the world, topping the list at 7.153 children per woman, followed by Somalia at 6.123 children per woman. Niger also has the highest birth rate in the world of 44.2 births per 1,000 people. The high fertility rate in Nigeria, according to a paper published by the UN, can be attributed to a low use of contraception, early and universal marriage, the high child mortality rate, early child bearing and child bearing within much of the reproductive life span, and high social values placed on child bearing.

### Where women are having fewest children

Average fertility rate, bottom 10 countries in 2017

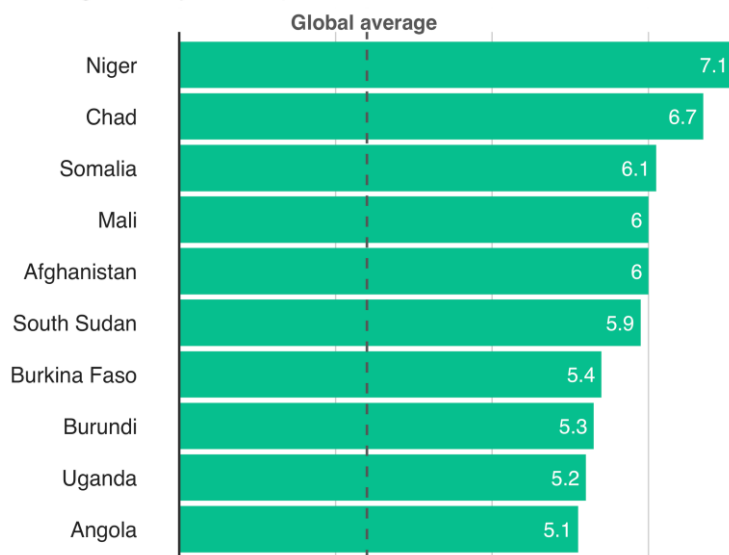


Source: Global Burden of Disease

BBC

### Where women are having most children

Average fertility rate, top 10 countries in 2017



Source: Global Burden of Disease

BBC

## 6. Points to address

- How can proliferative countries help the others?
- Would it be viable to ban contraception methods again?
- How are fertility rates and gender equality linked?
- Can the problem be solved through automation?
- What other economic domains are affected?
- How does immigration interfere with the problem?

## 7. Further read

<https://www.newsecuritybeat.org/2014/06/governments-falling-birth-rates/>

<https://yaleglobal.yale.edu/content/replacement-fertility-declines-worldwide>

<http://worldpopulationreview.com/countries/total-fertility-rate/>

<https://foreignpolicy.com/2019/07/25/how-to-fix-the-baby-bust/>

## *Topic C: Combatting Cybercrime*

### **1. Overview of the topic**

Cyber Attacks are classified into two main branches: Cybercrime, when a person is harmed by an individual or a group by means of any type of telecommunication network and Cyberwarfare which include cyber offences that cross international borders, such as espionage or terrorism. Clearly, the latter is more important and hard to program. Nowadays, it has become more and more common for people to conduct criminal activities on the internet, especially since there are countless methods in which criminals can hide their identities and avoid getting caught by the authorities. Thus, the internet is considered to be the safest environment for criminals that wish to do harm to others or just steal information or money from them.

### **2. Key Terms**

**Cybercrime** = Cybercrime is a criminal act and can be defined as "an offence that is committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)"

As underlined by the Budapest Convention (2001) some terms related to the technical nature of a cybercrime have to be further explained, and explicitly defined;

- a. "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;
- b. "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;
- c. "service provider" means: i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service.
- d. "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the

chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

**Cyberwarfare** = Defined as any virtual act of aggression with a political motivation aiming to affect the enemy's computer and information systems. The ultimate goal is to paralyze the financial and organizational systems via means of alternation or theft of top secret information, thus undermining and rendering useless networks, important websites and essential services.

There are 2 possible acts of virtual aggression:

- i. Sabotage the end goal is to disrupt the flow of operations and equipment necessary for the military and financial computer systems to function properly such as but not limited to; communications, fuel, power and transportation infrastructures.
- ii. Espionage and/or security breaches the theft and unlawful acquisition of classified information from the enemy's institutions for purposes of military, political or financial nature. The method used is the disabling of the rival's networks, software, computers or the Internet.

**Cybersecurity** = the safeguarding of an online system's security, an online database's intactness and overall, the maintenance of one's virtual "sovereignty". To safeguard the above methods of prevention are of utmost importance. One to protect themselves has to have a comprehensive and indepth understanding of the enemy's "arsenal" as well as possible strategies. This translates to having a knowledge upon the potential information threats, such as an advanced virtual "virus" or other malicious programs. Cybersecurity defense strategies are largely based upon;

- i. Identity management,
- ii. Risk management
- iii. Incident management

**Computer Emergency Response Team** = "A computer emergency response team (CERT) is a group of experts who respond to cybersecurity incidents." In general, the designation of CERT aims to confront the evolution of viruses, malware as well as other cyber-attacks, via the application of real-world solutions to these problems. They may be associated with government or work as employees of a major corporation. For instance, the U.S. Computer Emergency Readiness Team (US-CERT) operates under the U.S. Department of Homeland Security.

**Denial-of-Service Attack** = “A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service.” In a DoS attack, the hacker usually sends a plethora of messages asking the server or network to authenticate requests whose return addresses are invalid. The server or network, unable to find the return address of the perpetrator when sending the authentication approval, causes the server to wait before termination of the connection. When the network closes the connection, the hacker sends more authentication messages whose return addresses are also invalid. This results in the restart of the authentication process, keeping the network or server busy.

DoS attacks can cause ineffective or inaccessible services, connection interference or even interruption of network traffic.

**Phishing** = Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

### **3. Historical Background**

Fifty years ago, words such as hacking, malware, the dark net were known only to certain individuals who were very skilled in programming and were called “hackers”. Even though they do not get credit for “inventing” hacking, in the 1960s at MIT (Massachusetts Institute of Technology) we could find the most intelligent and intellectually advanced people in programming, some of which who have invented “UNIX” and the programming language for it, “C”.

As for actual hacking, the first computer worm was created in 1989 by Robert Morris. Aggressively and rapidly spread, this self-propagating virus managed to severely obstruct internet services. The Morris worm was a significant incident, interpreted as the first ever widespread example of denial-of-service (DoS) attack. However, internet back in late 1980s was in its very early stages, making the impact of Morris worms nearly insignificant compared to the devastating consequences they would have today.

The next decade brought an important increase in internet users, consecutively expanding the risks and challenges in cyber space. New threats, called “viruses” went viral and dominated cyber warfare. Instances such as the Melissa and the ILOVEYOU virus (two

of the most famous viruses) brought about the infection of millions of PCs, causing the failure of email systems world-wide, all conducted under the scope of servicing strategic and financial interests. Antivirus technology was developed as a response to these threats, targeting the viruses' signatures and hindering them from executing. Additionally, these attacks marked the starting point of the awareness raising process in terms of opening emails from untrusted or unverified sources. This phenomenon was more evident in several companies due to the ability of viruses to spread among corporate email accounts and bring into public eye questions about the security and the uprightness of the company.

During the millennium decade cyber-attacks changed radically, becoming more target-oriented. Between 2005 and 2007, the first serial data violation of credit card numbers took place. The mastermind behind this previously unheard fraud was Albert Gonzalez, who created a criminal ring that enabled him to steal information from approximately 45.7 million payment cards. The card holders were customers of US retailer TJX, costing the company more than \$256 million. This massive security compromise made matters more serious, as enterprises found out the hard way the dreadful consequences of being exposed to threats and started to arm themselves with state-of-the-art security systems adapted to new reality challenges.

Target breach is a process in which the perpetrators are able to lift "track data", enabling them to manufacture and sell counterfeit cards. 40 million of debit and credit cards were stolen via this scam, causing severe turbulences to the existing cyber security practices. The perpetrators used an indirect route, via a third party, by hacking into point-of-sale (PoS) systems, using a specifically developed code, grabbing decrypted credit card numbers. This incident made cybercrime a matter of public response, rendering ineffective the ad hoc approaches by companies and pointing out the necessity of the adoption of a holistic strategy towards the issue.

Admittedly, the sophistication of cybercrime makes it truly difficult to prevent. Organizations should emphasize on how to hinder a possible spread of the breach and construct solid post-crisis management strategies in the purpose of controlling the aftermath and responding to it efficiently. Building organizational resilience is a key factor in alleviating the "pain" caused by cyber threats in every aspect of their existence.

## **4. Current Situation and Issues**

Hacking has become one of the primary and easiest activities to do on the internet, mainly because of the freedom the users, which is still a priority in preventing the spread of cybercrimes. Respect for privacy is the cornerstone of democracy, because it is



directly linked to free thought and expression. However, privacy of computer networks is just as important as it includes many times sensitive personal data. Thus, the need for investigation of such crimes arises now more than ever. Nowadays, there are some “hacking” trends, linked to the development of technology in all departments:

- Attacks via smartphone are related to unsafe browsing of the internet. More than 60% of fraud online is accomplished through mobile platforms, and, according to the RSA (cryptosystem used for secure data transmission), 80% of mobile fraud is achieved through mobile apps. As most people use their phones to manage financial operations or handle sensitive data outside the security of their home network, this becomes a prominent threat. The fact that users typically hold all their information on their phone, and that smartphones are now used for two-factor authentication - one of the most widely used cybersecurity tools - increases the security risk if the device is lost or stolen.
- Most of the biggest industries already use machine learning (ML) and artificial intelligence (AI) to automate their processes and improve overall performance. Cybersecurity and cybercrime are no exception.

AI is often considered to be a dual-use technology - while more cybersecurity companies are implementing AI-driven algorithms to prevent threats, hackers are also taking the opportunity to become more effective.

The majority of AI qualities serve malicious purposes. AI systems are cheap, scalable, automated, anonymous and they provide physical and psychological distance for the attacker, diminishing the immediate morality around cybercrime.

- Artificial intelligence for cybersecurity evasion. Cybercriminals are using various evasion methods to avoid detection, and AI helps to optimize different elements of this process.
- Artificial intelligence in phishing. AI could help to create content that can pass through typical cybersecurity filters, such as email messages that are indistinguishable from those written by humans.
- Artificial intelligence in social engineering. While social engineering is one of the most popular hacking techniques, it takes a lot of time to

implement properly. AI could help in not only collecting information, but also by writing emails or calling potential victims.

With new advances in AI-driven technology, utilizing AI in cyber attacks will become an even more popular and dangerous trend.

If we had to analyse all cybercrime news, we would have to write countless books, and we still wouldn't have enough paper to describe them.

## **5. Position of major actors**

### **The United States of America**

Internet-based crime is one of the fastest growing security threats in the United States. As internet use increases, there has also been a shift in how people use computers for transactions and communication. Personal information such as email addresses, phone numbers, names, and other login credentials are utilized by hackers to commit identity fraud. In a September 2018 survey of U.S. adults, 32.7 percent of respondents stated that they had experienced a hack of their social media or e-mail account. In another survey conducted during the same year, 14 percent of respondents stated that their online accounts had been hacked more than once. Overall, consumers in the United States are keenly aware that the risk of becoming a victim of cybercrime is increasing.

### **People's Republic of China**

If a Chinese citizen (particularly an urbanite who grew up in the 1990s and 2000s) is asked about cybercrime, the response is likely to be online fraud. Online fraud has been a growing phenomenon in China in recent years, but a public uproar arose from a report last year about a telephone fraud directed against an incoming college student, Xu Yuyu. The swindlers, posing as education bureau officials, persuaded Ms. Xu to transfer RMB 9,900 (approximately US\$1,439) under the pretense that the transfer was necessary to receive financial aid. When Ms. Xu found out she had been defrauded, she reported the case and, on the way home, fell unconscious and died a few days later of cardiac arrest. Whatever the cause of the death, the case highlighted the prevalence of online scams in China. Given the globalization inherent in the Internet, even the so-called "Great Firewall" cannot contain this activity in China -- or keep it out of China. Whether outside or inside of China, the activity for now is mostly directed at China and Chinese victims. That activity will undoubtedly spread to victims in other countries.

## **The Russian Federation**

For years, the Russians have been preparing the digital battlefield, treating our critical infrastructure as if it were their own cyber weapons range.

Overseas they've gone even further. In 2015 and 2016, the Kremlin planted malware in Ukraine's electric grid, disrupting power for hundreds of thousands of residents in the middle of winter. Keenly aware of its capabilities and motivations, Director of National Intelligence Dan Coats has said that "the warning lights are blinking red again" — an allusion to CIA Director George Tenet's warning to Congress just months before 9/11. Furthermore, there is proof of other Russian attacks on countries, such as Estonia (Estonian cyberattacks in 2007), France (Macron e-mail leaks in 2017), Georgia (during the 2008 South Ossetia war), Germany, Kyrgyzstan, Poland, UK ("Brexit" referendum) or Venezuela. The most well-known online interference that Russia has had on foreign countries is the one on the 2016 elections for president.

## **Norway**

Despite its utopian reputation, Scandinavia is a cyber battlefield with data breaches and malware campaigns wreaking havoc. This region boasts some of the highest Internet penetration rates across the board, reaching 97%. Moreover, Sweden and Norway rank the second and third in the world by average connection speeds, respectively. The large-scale deployment of fiber optic and LTE infrastructure ensures that even people living on remote islands have unrestricted access to top-notch technologies. CEO frauds and investment scams are amongst Norway's biggest concerns in the security context. The victims are lured into investing in a new startup or cryptocurrency ICO (initial coin offering) with allegedly high returns. Having raised the funds, the crooks vanish without a trace. Another common tactic is to impersonate a company's executive by hacking their email account and then dupe the staff into transferring funds to a rogue destination.

In early January 2018, a hacking crew compromised the medical records of more than half of Norway's population. The adversaries targeted an entity called Health South-East RHF, which provides healthcare services in 18 counties, including the capital city Oslo. The organization's authority spans about 3 million Norwegians, with the country's total population being 5.2 million citizens. By the time the IT personnel identified anomalous traffic patterns, the data leak was in full swing, exposing numerous customers' personal

information. Analysts claim the malefactors may take advantage of this data by orchestrating successful future frauds that will appear highly trustworthy.

Back in December 2011, a hacker gang calling themselves “Team Appunity” compromised the database of Hemmelig.com, Norway’s major sex services website. The hacktivists ended up making the list of 26,000 “clients” publicly available.

This shaped up to be a predicament for some Norwegian politicians, celebrities, business leaders, military officers and other representatives of the national elite who turned out to have registered accounts with the embarrassing online marketplace. In an anonymous commentary to local media, the attackers said the service wasn’t well secured, and it took them mere minutes to hack it.

## **6. Points to be addressed**

- What are the circumstances in which cyberattacks can be considered a good thing?
- How can governments ensure security for their citizens on the internet without infringing their freedom?
- How can we prevent the further development of methods in which hackers can access confidential data?
- Should people try reducing their time spent online and the information they provide on the internet in order to protect themselves?
- What legal framework can be adopted and, hopefully, implemented in all member states?

## 7. Further reading

[https://www.unodc.org/documents/organized-crime/UNODC\\_CCPCJ\\_EG.4\\_2013/CYBERCRIME\\_STUDY\\_210213.pdf](https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf)

[https://www.unodc.org/documents/terrorism/Publications/Use\\_of\\_Internet\\_for\\_Terrorist\\_Purposes/ebook\\_use\\_of\\_the\\_internet\\_for\\_terrorist\\_purposes.pdf](https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/ebook_use_of_the_internet_for_terrorist_purposes.pdf)

<https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime>

<https://www.cybersecurity-insiders.com/list-of-countries-which-are-most-vulnerable-to-cyber-attacks/>