



DISEC

STUDY GUIDE

Table of Contents

Table of Contents		ii
Letter from the Secretary-General		iii
Letter from the Under-Secretary-General		iv
Dear distinguished participants,		iv
1.	Historical Background of the Issue	1
2.	Weaponization of Data and Misinformation Today	4
3.	Information Warfare	9
4.	A Recent Occurrence Regarding the Issue: Cambridge Analytica Scandal	11
5.	Key Issues that the Delegates Must Discuss	13
6.	References	15

Letter from the Secretary-General

Honorable participants,

My name is Arda and I, as the Secretary-General of the Gazi College Model United Nations 2022, am very honored to welcome you all to the fourth annual session of GCMUN on behalf of our Director-General Deniz Başak and also our well-prepared academic and organization team members.

While organizing GCMUN our aim was to provide all of our participants significant and remarkable experiences; and consequently, rising awareness through global issues that our world is facing has been our main purpose. In this conference, we ensure you that you will gain diversified world visions about the current situation from our agenda items and it will redound your debating and negotiating skills, therewithal your knowledge and sensibility.

As the academic team of GCMUN'22 we have chosen our committees in order to make you focus on various topics and they are suitable for various levels of MUNers, so you will be able to enjoy. We have 6 different committees for both highly experienced and unexperienced delegates. Our first GA committee is GA-1:DISEC and our second one is UNEP. Moreover we have United Nations Security Council, North Atlantic Treaty Organization, JCC: British Civil Conflicts and lastly a JR United Nations International Children's Emergency and Fund committee which we only opened for middle school students in order for them to state their opinions confidently about the current issue of the world since every child are affected from every single conflict that composed in our world.

I highly encourage all of you to be well-prepared and enthusiastic in order to be efficient during the conference.

Best regards,

Letter from the Under-Secretary-General

Dear distinguished participants,

My name is Alara Irmak Tümer and I will be serving as the Under-Secretary-General of the General Assembly 1: Disarmament and Security Committee (GA1: DISEC) for this year's GCMUN. It is an utmost pleasure to welcome you all to this conference.

Within these three days, you will be discussing one of the major issues of today's world: weaponization of data and cyber security. My motivational drive in choosing this topic for our discussions is that we are all involved in this issue without even noticing it. Whether we like it or not, we are all civilians of a digitalized world and therefore are all using technology and social media in order to gain information. With technology and social media having access to our data and controlling all information; authorities and hackers gained even more power to conduct acts of weaponization of data and misinformation. As the world is to face even more developments within technology and therefore is about to face even more issues regarding the weaponization of data and misinformation if no other solutions are proposed and/or actions are taken; it is crucial to consider the political, economic, social, legal, technological and most importantly, ethical aspects of the issue to come up with solution ideas regarding this issue at hand. Since you are all familiar with technology and social media in addition to possessing great minds to figure out solution ideas; I believe that not only will you enjoy this committee but also come up with efficient solution proposals.

I hope that this topic will give relish to your discussions and wish for you to have fruitful debates. Take care.

Alara Irmak Tümer

Under-Secretary-General of GA1: DISEC

1. Historical Background of the Issue

Even though the word "data" forms the image of technological developments of today, misinformation, also addressed as "fake news" has long been used as a means of achieving what is wanted by authorities and therefore could be classified as "weaponization of data". Although there have been many occurrences throughout history regarding this issue, this study guide will only examine some of them to give the delegates an understanding of how fake news emerged and was used towards people even without the technological developments of today:

• The Fake News that Hit Italy

The first ever fake news that we know of took place in Trento, Italy, within the year 1475, on an Easter Sunday.¹ Simonino, a two year old toddler had gone missing, leading Franciscan preacher Bernardino da Feltre to give a series of sermons, claiming that the Jewish community had murdered Simonino, drained his blood and drunk it to celebrate Passover, a Jewish holiday.² As all rumors do, this rumor was also spread fast. Not much after, da Feltre was claiming that Simonino's body had been found in the basement of a Jewish house.³ As a response to this situation, the Prince-Bishop of Trent Johannes IV Hinderbach immediately ordered the city's entire Jewish community arrested and tortured.⁴ It was no surprise that the story inspired surrounding communities and paved the way for them to commit similar atrocities. Recognizing that the story was actually fake, the papacy intervened to the situation and tried to stop both the spreading of the story and the murders and tortures.⁵ However,

¹ Soll, Jacob, Jeremy B. White, Sam Sutton and Carly Sitrin, and Bill Mahoney and Josh Gerstein. "The Long and Brutal History of Fake News." POLITICO Magazine, December 18, 2016.

https://www.politico.com/magazine/story/2016/12/fake-news-history-long-violent-214535/. ² Ibid.

³ Ibid.

⁴ Ibid.

⁵ Soll et al, *The Long and Brutal History of Fake News*.

Hinderbach refused to meet the papal legate, and feeling threatened, he spread even more fake stories about Jews drinking the blood of Christian children.⁶ With the invention of the printing press in the year 1439 by Johannes Gutenberg, many news stories started to be printed and therefore was incredibly difficult to understand what was right and what was not. even though there were many news sources from official publications by political and religious authorities, to eyewitness accounts from sailors and merchants. However, there was no concept of journalistic ethics or objectivity; leading to such occurrences like Italy once faced.

• 1755 Lisbon Earthquake

As the act of printing reached a bigger territory, so did the fake news. Many of the fake news were about sea monsters, witches and sinners being responsible for natural disasters.⁷ An example of this could be given as the Lisbon Earthquake of 1755. The acts of the church and many European authorities blaming the earthquake on divine retribution against sinners even effected Voltaire, an Enlightenment philosopher, to attack religious explanations regarding natural events and disasters; and become an activist against fake religious news.⁸

Yellow Journalism

Simply put, the notion "yellow journalism" may be summarized as "sensationalism over facts".⁹ Journalists of the 1890s realized that exaggerated news with shocking headlines gets the most attention.¹⁰ The word "clickbait" of today could be given as the "modernized" version of yellow journalism.

1998

⁶ Ibid.

⁷ Ibid.

⁸ Ibid.

⁹ "U.S. Diplomacy and Yellow Journalism, 1895–1898." U.S. Department of State. U.S. Department of State. Accessed May 29, 2022. https://history.state.gov/milestones/1866-1898/yellow-journalism.

¹⁰ "A Brief History of Fake News." Center for Information Technology and Society - UC Santa Barbara. Accessed May 29, 2022. https://www.cits.ucsb.edu/fake-news/brief-history.

• The Second Red Scare of 1950s

Although this historical occurrence is classified as an abuse of authority, it also includes misinformation and therefore is scrutinized within this study guide.

Joseph McCarthy, the former Republican United States Senator from the state Wisconsin between the years 1947 and 1957,¹¹ was the chair of the Senate Committee on Government Operations and the Permanent Subcommittee on Investigations.¹² Using his authority caused by his position, he initiated the investigations of Communist Party of the United States of America (CPUSA) members in addition to their sympathizers and engaged them with public accusations (which were made with unsubstantiated evidence) of political disloyalty, which later became labeled as "McCarthyism".¹³ Between 1950 and 1954, McCarthy accused many people without credible evidence causing them to lose their reputations. The denial of civil liberties and in some cases their lives, like Rosenberg's, who committed the ironic "crime" of freedom of speech, led to outlawry.

2. Weaponization of Data and Misinformation Today

Although it could be stated that the weaponization of data and acts of misinformation existed way before, it is no doubt that the threat is getting bigger with the developments of technology and the emergence of social media.

¹¹ Pufong, Marc G. McCarthyism. Accessed May 29, 2022.

http://www.mtsu.edu/first-amendment/article/1061/mccarthyism.

¹² Ibid.

¹³ Ibid.

In order to give expert views, we may have a look at the "Era of Awareness: 7th Annual SAP National Security (SAP NS2) Solutions Summit" that took place on 30th of October, 2018. Within the summit, a panel named "The Dark Side of Data: When Information is Weaponized" paved the way for the participants to gain the opportunity to fully understand the risks of this issue via listening to expert's opinions about the situation at hand. The panel welcomed its moderator Ken Dilanian, a national security reporter from NBC News; Maren Cattoner, an ecosystem architect that worked within the MIT regarding security risks of data; Andre Pienaar, the founder and managing partner of C5 Capital, a firm that invests on secure data ecosystem and its branches such as but not limited to cyber security, cloud infrastructure, data analytics and space;¹⁴ Jeffrey C. Chapman, the CEO of Babel Street, which is an AI enabled "data-to-knowledge" company that helps the civilians to double-check the information they gained on whether it is true and from a reliable source;¹⁵ Dr. Richard Forno, a senior lecturer on cyber security and an internet researcher at the University of Maryland, Baltimore Country; and lastly retired general Scott Bethel who is now the President and CEO of IntegrityISR, which is a company that delivers innovative Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) solutions via employing former military service members, national security experts, and academic professionals.¹⁶

Dr. Richard Forno strongly believes and advocates that we are, in fact, moving towards an era of "conventional warfare".¹⁷ He explains his argument regarding this issue as; "... we shall look at this situation from both a technological perspective and an informational perspective. I like to view it as a three-fold prism. There is the physical dimension where we

¹⁴ "Our Firm." Our Firm | C5 Capital. Accessed May 29, 2022. https://www.c5capital.com/our-firm/.

¹⁵ "About Us." Babel Street. Accessed May 29, 2022. https://www.babelstreet.com/about-us.

¹⁶ "We Know ISR." We Know ISR, January 27, 2022. https://integrityisr.com/about-integrity-isr/.

¹⁷ SAP NS2, "The Dark Side of Data: When Information is Weaponized," *YouTube* video. 30:46. November 6, 2018. https://www.youtube.com/watch?v=sEVF53mu-eE.

operate in in the real world and in cyber space. There is also the informational meet medium, the messaging, what is being conveyed, again, whether it is on a network bits and bytes or communication in the news media. And then there is also what I call the third aspect, the third leg of this prism is what I would call that cognitive element and that is really what I think the date where the danger is in many ways because whatever we do whether it is cyber warfare, cyber security, journalism, medical research; you name anything we do revolves around the most complicated computer system in the world but also the one that's most vulnerable and the easiest one to exploit and that is the human brain and the cognitive element; therefore I think is really where a lot of the emphasis we are seeing these days with things like fake news and cyber is converging,".¹⁸

It is also emphasized by Ken Dilanian that there is no defense against this situation in terms of the government, meaning, there is no government-wide effort to combat this problem at hand.¹⁹ However, there are private sector efforts, such as Scott Bethel's company, in order to overcome this problem. As a former military servant, he states; "... we use the term 'weapon' which implies a certain military context. There are five war fighting domains: space, air, sea, land and cyber. Cyber is the only one that is completely man made, man manipulable and where warfare occurs when people are buying sweaters, emailing their mom and taking on other countries. So, there are two ways to look at the defense against weaponized data: nation states tend to go in volume so they tend to bombard the Facebook trilogy: Facebook, Twitter and Instagram; with all kinds of data, with a perception of news. In the Middle East for example, ninety-three percent of young people get all of their information through that and then they respond on what is that. For insurgents, they tend to be a lot more precise because what they are trying to do is command and control and they are trying to do a making, have an effort towards getting action out of a group. So, ultimately, as a nation state

¹⁸ Ibid.

¹⁹ Ibid.

the defense is incredibly difficult because the insurgent groups are remarkably sophisticated and agile. So the way to defend against that is to increase the volume and the size of data to overpower and circumvent insurgent operations and objectives,".²⁰

Jeffrey C. Chapman, on the other hand, points out to a very important aspect of the issue which is the ability of people to determine which news is fake and which is not.²¹ However. the word "ability" here, does not mean that all civilians possess this ability. First and foremost example could be given as the difference between the Onion and the AP. The Onion is a "news media" that is satire, the AP however, is a legitimate news media that delivers real news.²² Although it is expected for the people to understand the vast difference between the two news medias, people tend to be fooled by the Onion, thinking that the news published there are real, when in reality, they were written to mock the political occurrences.²³ Jeffrey C. Chapman also points out that even if all people knew the difference between these two news medias, the hacking of legitimate news medias is also something very common, and therefore even the AP or other legitimate news medias could not be trusted from time to time.²⁴ He gives the example of the hacking of the twitter account of the AP in the year 2013 and how they sent out the news of a conflict within the White House and the president being injured within that conflict.²⁵ Chapman states that people do not tend to stop and think about the accuracy of the news they saw.²⁶ He states that most of the time, most people tend to believe in the first news that pops up in their feed is true and that they do not care to open up other news medias to verify the accuracy of the news they saw, even if the news is non-sense.²⁷ This could probably be the most serious issue at hand since this act of the

²⁰ SAP NS2, *The Dark Side of Data: When Information is Weaponized.*

²¹ Ibid.

²² Ibid.

²³ Ibid.

²⁴ Ibid.

²⁵ SAP NS2, *The Dark Side of Data: When Information is Weaponized.*

²⁶ Ibid.

²⁷ Ibid.

civilians could actually be used against them by political authorities in order to manipulate them. "Twitter trolls" could be given as a perfect example to this situation.

So, how can governments respond to this problem of manipulated data? For now, in order to answer this question without prejudice, it is best if we put aside the fact that political authorities sometimes tend to use manipulated data to their benefits; and think that they actually want to solve this problem at hand. In order to answer this question, Andre Pienaar states; *"I think policy and the law are important tools in dealing with this challenge but they need to be augmented by innovation driven by entrepreneurs. ... In this realm of war and peace, data has become absolutely central to this quest and as president Reagan said: 'To build a strong peace; we need hope, confidence and facts' and preserving facts and being able to preserve facts through innovation is I think is at the heart of this mission. And as we have seen in the innovation economy that the focus have moved from hardware to software, to data; and so the focus of innovation is now on preserving facts, ".²⁸.*

When asked about the most critical national security risks surrounding the weaponization of data, Maren Cattonar states, "... I actually think that data has been weaponized for a significantly long amount of time. You can look at the events from Estonia, Ukraine ransom-ware attacks on hospitals, so it is nothing new. ... I was watching a public television program the other day and it featured the Concorde which was a quite technical accomplishment and then they also featured the copied version of the Concorde ... that was just an example of the theft of intellectual property and how you can take one model and actually can duplicate and maybe even improve upon it. So there are nation states that are stealing intellectual property and doing some really interesting stuff with it. So that is a probable and happening subject matter, and then in addition to that the probable and not likely to happen are the OPM breach where it stole individual's data and what if you

²⁸ Ibid.

coupled that data with the theft of data from a hospital or a trusty ancestory.com account? Could you then weaponize that information and create synthetic viruses using CRISPR where you are gene editing and targeting a specific population?".²⁹ She also talks about quantum computers and quantum computing that is a development of the future and not the situation of today's world but also states that who gets to quantum computing first, will disrupt everything we are talking about now and will enable new solutions and architectures for cyber security. She goes on with her speech stating; "...but what you are looking at now is probable and is happening. It is misinformation, it is fake news and how it influences people and people are the ones who control the data, create the data, analyze the data and make sense of the data. So you have mercenary actors or intentional actors that with the examples right now of the synagogue shooting, the explosives that were sent in the mail to nation states that are actually going after influencing elections and then you have also the intentional influence when someone clicks on a phishing link or plugs in an IOT device that is unsecure. So the crux of it is national security is jeopardized by the people and I think how information is conveyed to those people influences that all.".³⁰

3. Information Warfare

North Atlantic Treaty Organization's (NATO) explanation of information warfare is "an operation conducted in order to gain an information advantage over the opponent. It consists in controlling one's own information space, protecting access to one's own information, while acquiring and using the opponent's information, destroying their information systems and disrupting the information flow. Information warfare is not a new phenomenon, yet it

1005

²⁹ SAP NS2, The Dark Side of Data: When Information is Weaponized.

³⁰ SAP NS2, The Dark Side of Data: When Information is Weaponized.

contains innovative elements as the effect of technological development, which results in information being disseminated faster and on a larger scale, ".³¹

• Cyber-Warfare

Since we are now living in a digitalized world, it is no surprise that cyberspace and new technologies relating to this area provide a crucial field for information warfare. Within cyber-wars, one can observe cyber-attacks such as the destroying of information systems of the opposing side and also social-cyber-attacks that consist of the creation in a specific image of the world in people's minds; consistent with the goals of the information warfare conducted by a given country.³²

Information War and the Internet

NATO summarized the influence of the internet regarding information warfare as "The Internet enhances and expands the possibilities of data acquisition, information defence and information disruption, and makes it easy to reach both the citizens of a given country and the international community. Given the speed of communication, wide coverage and low cost of (dis)information campaigns, social media play a crucial role. Social networking sites are also a valuable source of information on the target groups to which (dis)information activities are to be addressed,".³³

• Information Warfare: The Annexation of Crimea

Much like the "twitter trolls" of today that we know that are used for political interests, the Russian Federation spent more than nineteen million dollars to fund six-hundred people to

³¹ Media - (Dis)Information - Security. PDF File.

https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf. ³² Ibid.

³³ Media - (Dis)Information – Security.

constantly comment on news articles, write blogs and operate throughout social media.³⁴ The intention of the Russian Government in performing such an act was to create an image of a population that is supportive of the annexation.³⁵ Despite from the people paid to spread supportive messages towards the annexations and to spread fake news, social media platforms also facilitated a platform for such messages to reach millions of people faster than before, making it easier for the Russian Federation to achieve its goal. The Strategy Bridge, **a** non-profit organization focused on the development of people in strategy, national security, & military affairs, states *"Crimea served as a proving ground for Russian Information Operations, as well as the larger applications of cyber warfare. It brought the cyber domain to light among the masses and showed social media to the world as a potent weapon system, ".³⁶*

4. A Recent Occurrence Regarding the Issue: Cambridge Analytica Scandal

The political consulting firm Cambridge Analytica was working for the Trump campaign in the year 2016 when Facebook exposed the private data of eighty-seven million users.³⁷ According to a former Cambridge Analytica employee, the company received the data from Facebook via a Russian-American researcher who worked at the University of Cambridge: Aleksandr Kogan.³⁸ So how did Kogan collect up to 87 million users' data? The beloved online-quizzes were handy enough to trick people. By building a Facebook "quiz" app, not only did Kogan collect data from the people who took the quiz but also the app exposed a loophole in Facebook Application Programming Interface (API) that allowed the app to

³⁴ Holloway, Michael. "How Russia Weaponized Social Media in Crimea." The Strategy Bridge. The Strategy Bridge, May 10, 2017.

https://thestrategybridge.org/the-bridge/2017/5/10/how-russia-weaponized-social-media-in-crimea.

³⁵ Ibid.

³⁶ Holloway, How Russia Weaponized Social Media in Crimea.

³⁷ Chang, Alvin. "The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram." Vox. Vox, March 23, 2018.

https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram. ³⁸ Ibid.

collect data from the Facebook-friends of the ones that took the quiz.³⁹ Even though Facebook prohibited the selling of data collected with this method, Cambridge Analytica sold the results anyway.⁴⁰

Actions of the United Nations (UN) Regarding This Issue and Their Role

- Disarmament and Security Committee: Just like Scott Bethel says, we have been using a lot of military terms regarding this issue, an example could be given as the notion "weaponization of data". Since, as its name suggests, the Disarmament and Security Committee deals with disarmament in addition to global challenges and threats to peace that affect the international community,⁴¹ the committee is highly related with this issue at hand and has to come up with solution ideas.
- The UN Office of Counter-Terrorism (UNOCT): The UNOCT has set out several initiatives in the field of new technologies, one of which is a project on the use of social media to gather open source information and digital evidence to counter terrorism and violent extremism while respecting human rights.⁴²
- The Cyber Security and New Technologies Programme: Not only does this programme aim to enhance capacities of Member States of the UN and private organizations in preventing cyber-attacks carried out by terrorist actors against critical

³⁹ Ibid.

⁴⁰ Ibid.

⁴¹ "United Nations, Main Body, Main Organs, General Assembly." United Nations. United Nations. Accessed May 29, 2022. https://www.un.org/en/ga/first/.

⁴² "Cybersecurity | Office of Counter-Terrorism." United Nations. United Nations. Accessed May 29, 2022. https://www.un.org/counterterrorism/cybersecurity.

infrastructure, but also seeks to mitigate the impact and recover and restore the targeted systems should such cyber-attacks occur.⁴³

5. Key Issues that the Delegates Must Discuss

• Cyber Security Measures

Even though a technical aspect, the discussion upon measures regarding cyber security is a must for the delegates, since most of the issues discussed within the study guide are related with cyber-attacks, cyber-space and therefore, cyber security. Even though the delegates do not have to know each and every technical detail, doing a little research according to what they think of as a solution idea might come in handy when they are writing their resolutions.

• Ethical Aspects

It is incredibly important for the delegates to point out the ethical aspect of the issue since the authorities' misinformation acts keep the citizens from learning the real news is not the only crucial issue that needs to be solved but also the gaining information from individual's personal data. Whether the aim is political, economic, psychological... etc., such acts are a violation of human rights and privacy.

Legal Aspects

After scrutinizing the ethical aspects of the issue, the delegates may take the issue to a legal level. Since, as stated before, the weaponization of data and misinformation are acts violating

⁴³ "Cybersecurity | Office of Counter-Terrorism." United Nations. United Nations. Accessed May 29, 2022. https://www.un.org/counterterrorism/cybersecurity.

human rights and privacy, it would be best if the civilians were protected under an international or nation state level law. However, the delegates must realize that they do not have the authority to implement regulations but rather suggest doing so.

• News Credibility

Misinformation in its own is a threatening problem. Whether it is done intentionally, for example like the political authorities do, or done unintentionally, like the hacking of the AP; one thing is clear: the issue of misinformation must be handled immediately. The delegates may want to scrutinize the technological aspects of the issue if they want to, but since the issue would be way technical, it could be recommended for the delegates to mostly focus on the legal aspects of the issue, such as an international penalty system. But then again, it is not restricted for the delegates to dwell upon the technological aspects of the issue if they want to. This, of course, will mean that the delegates shall have a thorough knowledge towards them.

6. References

"A Brief History of Fake News." Center for Information Technology and Society - UC Santa Barbara. Accessed May 29, 2022. <u>https://www.cits.ucsb.edu/fake-news/brief-history</u>.

"About Us." Babel Street. Accessed May 29, 2022. <u>https://www.babelstreet.com/about-us</u>.

Chang, Alvin. "The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram." Vox. Vox, March 23, 2018. https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica -trump-diagram.

"Cybersecurity | Office of Counter-Terrorism." United Nations. United Nations. Accessed May 29, 2022. <u>https://www.un.org/counterterrorism/cybersecurity</u>.

Holloway, Michael. "How Russia Weaponized Social Media in Crimea." The Strategy Bridge. The Strategy Bridge, May 10, 2017. https://thestrategybridge.org/the-bridge/2017/5/10/how-russia-weaponized-social-media-in-cr imea.

 Media
 (Dis)Information
 Security.
 PDF
 File.

 https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information warfare.pdf.

"Our Firm." Our Firm | C5 Capital. Accessed May 29, 2022. https://www.c5capital.com/our-firm/.

Pufong, Marc G. McCarthyism. Accessed May 29, 2022. http://www.mtsu.edu/first-amendment/article/1061/mccarthyism.

"United Nations, Main Body, Main Organs, General Assembly." United Nations. United Nations. Accessed May 29, 2022. <u>https://www.un.org/en/ga/first/</u>.

"U.S. Diplomacy and Yellow Journalism, 1895–1898." U.S. Department of State. U.S. Department of State. Accessed May 29, 2022. https://history.state.gov/milestones/1866-1898/yellow-journalism.

SAP NS2. "The Dark Side of Data: When Information is Weaponized" *YouTube* video. 30:46. November 6, 2018. <u>https://www.youtube.com/watch?v=sEVF53mu-eE</u>.

Soll, Jacob, Jeremy B. White, Sam Sutton and Carly Sitrin, and Bill Mahoney and Josh Gerstein. "The Long and Brutal History of Fake News." POLITICO Magazine, December 18, 2016.

https://www.politico.com/magazine/story/2016/12/fake-news-history-long-violent-214535/.

"We Know ISR." We Know ISR, January 27, 2022.

https://integrityisr.com/about-integrity-isr/.

