# Security Council

## Addressing the weaponization of information in international conflicts

German International School
of The Hague
Model United Nations

**Forum: Security Council**

**Issue: Addressing the weaponization of information in international conflicts**

**Student Officer: Lily Elshehawi**

**Position: Deputy Chair**

## Introduction

In the modern digital age, the rapid advancement of technology has revolutionized the way information is created, shared, and consumed. While information has always been a crucial tool in war, diplomacy, and governance, the widespread use of social media, artificial intelligence, and cyber technologies have significantly increased its impact. Today, information is not only a means of communication but also a powerful weapon that can be strategically manipulated to achieve political, economic, and military objectives.

The weaponization of information refers to the deliberate use of false, misleading, or strategically crafted narratives to influence public perception, destabilize governments, and manipulate international relations. This practice includes disinformation campaigns, propaganda, cyber warfare, psychological operations, and algorithmic manipulation, all of which can be deployed by state and non-state actors alike. Unlike traditional forms of warfare, information warfare operates in the gray zone space between peace and conflict where adversaries can weaken their opponents without direct military engagement.

This growing phenomenon poses serious threats to democracy, national security, and global stability. Disinformation campaigns can erode public trust in institutions, manipulate elections, incite social unrest, and even justify acts of war. Cyberattacks targeting media, government, and financial institutions further exacerbate these risks, creating an environment where truth becomes difficult to distinguish from falsehoods. As nations and organizations struggle to combat these challenges, understanding the mechanisms and implications of information warfare is critical in developing effective countermeasures.

## Definition of Key Terms

| | |
|---|---|
| Cyber Propaganda | The use of digital platforms, especially social media, to spread biased or misleading materials to influence public assumptions and political consequences. |
| Deepfake Technology | Artificially generated or manipulated videos, images, or audio files that appear real but are fake. This technology can be used for political manipulation or fraud. |
| Disintegration | Deliberately false or misleading information that extends with the intention of cheating, manipulating in opinion or causing disadvantages. |
| Echo Chamber Effect | An event on social media where users are primarily exposed to information that reinforces their existing views, while opposing perspectives are systematically filtered. |
| Hybrid Warfare | A form of warfare that combines conventional military tactics with non-military means such as cyberattacks, economic pressure, and information warfare. |
| Media Literacy | The ability to analyse information, assess sources and differentiate between reliable and misleading materials. Media is an essential tool in dealing with literacy dissolution. |
| Misinformation | Misinformation is false or misleading information shared without the intent to deceive. It can spread rapidly due to social media and news outlets, often by individuals who believe it to be true. While not always malicious, misinformation contributes to confusion and can be exploited by bad individuals. |
| Psychological Warfare | Tactics aimed at weakening the morale or behaviour of a population or political opponent through fear, confusion, or targeted messaging. |
| Weaponization of Information | Strategic use of information to achieve political, economic or military objectives. This may include disintegration, publicity, public opinion manipulation and propaganda. |
| Propaganda | Propaganda is biased or misleading information designed to influence opinions, emotions, or behaviours. It is often used by governments, organizations, or political groups to |

| | |
|---|---|
| | promote a particular ideology or agenda. Propaganda can be spread through media, speeches, art, or education. |
| Cyber Warfare | Cyber warfare involves the use of digital attacks, such as hacking and malware, to disrupt or damage an adversary's critical infrastructure, government systems, or information networks. It can be used to steal sensitive data, disable communication systems, or manipulate financial and political systems. Cyber warfare is often conducted by state actors, but terrorist groups and hackers also engage in it. |

## General Overview

In today's mutually connected world, information has become a powerful tool, which can shape public perception, affecting political decisions, and even changing courses of international conflicts. The weapon of information refers to the intentional use of misinformation, disintegration and propagation to destabilize societies, manipulates political outcomes and get strategic benefits. The incident has intensified with the rise of digital technology and social media, making it easier to spread false or misleading stories globally.

One of the most important aspects of this issue is the difference between misinformation and disintegration. The wrong information refers to false or misleading information that is inadvertently spread, often due to lack of facts. In contrast, disintegration is made intentional and distributed to cheat the audience, manipulated in public opinion, or causes damage. These strategies are often used by state and non-state actors to control stories, suppress dissatisfaction or create confusion during conflict.

A major tool in modern information war is cyber propagation, where digital platforms such as social media, news websites and messaging apps are exploited or exploited to spread false content. This can take the form of fake news articles, manipulated images and deepfake videos, which use artificial intelligence to create realistic but false materials. These methods are designed to destroy confidence in democratic institutions, fuel social divisions and manipulate political decisions.

The historical use of propagation in war is not new. Throughout history, governments have used publicity to influence both domestic and international audiences. During the Cold War, both the United States and Soviet Unions are engaged in comprehensive information war, promotes ideological superiority and defame their opponents. However, in the digital age, the scale and speed on which disintegration spreads has reached unprecedented levels, making it more difficult to control and counter.

Many recent conflicts have demonstrated the disastrous impact of the Information War. Russia-Ukraine War offers one of the most striking examples, in which Russia used state-control media, online bots, and fake social media accounts to justify military functions and spread anti-outer publicity Accounts have been used. Similarly, foreign intervention in the

Democratic elections has been a growing concern with allegations of Russian arbitration in the 2016 US presidential election and on the ongoing cyber-affected campaigns in Europe. In Asia, China has been accused of using a disruptive strategy to influence Taiwan's elections and the global perception of its policies.

The results of the information war are far ahead of politics. Socials who are victims of massive dissolution campaigns often experience growing polarization, where citizens are opposed to camps based on the narratives manipulated. Additionally, confidence in traditional media and Democratic institutions declines, making it easier to tighten information and silence protests for the ruling rule.

International organizations have recognized the need to combat the weaponization of information. The United Nations has urged countries to take strong measures against disintegration, protecting the freedom of speech. Organizations like NATO and European Union have introduced cyber security initiatives and laws such as the Digital Services Act (2022), which aims to regulate online platforms and limit the spread of fake news

However, addressing the issue comes with many challenges. It is difficult to balance the disintegration between combating and preserving free speech, as excessive regulation can cause censorship. Additionally, technology develops rapidly, making it difficult to detect and combat false narratives. Many governments also define what is the formation of "fake news", to define it, because political bias often affects the interpretations of truth.

To effectively combat the weaponization of information, a multi-layered approach is required. Governments should implement strong cyber security measures, social media companies should take more responsibility for monitoring materials, and media literacy programs should be expanded to help citizens seriously assess that information that They consume. Strengthening independent journalism and fact-checking organizations is also important to combat the spread of misleading materials.

The weaponization of information is a significant threat to global stability, democracy and security. Since international conflicts continue to develop, a strategy used to manipulate public perception and influence political consequences. The international community should work together to address this growing challenge, while ensuring that attempts to deal with disintegration do not compromise the basic principles of free expression and open debate.

## Major Parties Involved

The weaponization of information is a global issue involving multiple key actors, including powerful nations, international organizations, and technology companies. Each of these parties has its own perspective on the issue, influenced by political, economic, and security interests.

**Russia:**
Russia has frequently been accused of using disinformation, cyber warfare, and digital propaganda as strategic tools in international conflicts. The Russian government views information warfare as a crucial element of modern geopolitical strategy, both as a defensive mechanism against perceived Western hostility as well as an offensive tool to expand its influence. Unlike conventional military operations, which require significant resources and direct engagement, information warfare provides Russia with a cost-effective and deniable means of destabilizing adversaries, influencing global narratives, and advancing its strategic interests.

A major component of Russia's information warfare strategy is its state-controlled media, particularly RT (Russia Today) and Sputnik, which serve as key platforms for disseminating pro-Kremlin narratives to global audiences. These outlets frame geopolitical events from a Russian perspective, often portraying Western democracies as corrupt, unstable, and aggressive. They amplify anti-Western sentiment, highlight divisions within foreign societies, and challenge the legitimacy of Western policies, particularly regarding NATO, the European Union, and U.S. foreign interventions.

Beyond traditional media, Russia also utilizes social media platforms, online forums, and digital content farms to spread disinformation. Troll farms such as the Internet Research Agency (IRA), based in St. Petersburg, have been implicated in coordinated efforts to manipulate public discourse, spread conspiracy theories, and influence political debates in multiple countries. These operations often involve:

- Bot networks and fake accounts that amplify divisive narratives.
- Deepfake technology and manipulated images/videos to create confusion.
- Astroturfing tactics to make propaganda appear as grassroots activism.

One of the most high-profile accusations against Russia is its cyber interference in foreign elections, particularly in the United States and Europe. The most notable example is the 2016 U.S. presidential election, where Russian-linked actors allegedly conducted a hack-and-leak operation targeting the Democratic National Committee (DNC) and engaged in widespread social media manipulation to polarize American voters. Reports from U.S. intelligence agencies concluded that Russian operatives sought to undermine public trust in democratic institutions, fuel political divisions, and sway the election outcome in favor of candidates deemed more favourable to Russian interests.

Similar interference tactics have been observed in European elections, including in France, Germany, and the United Kingdom. Russian cyber operatives have been accused of:

- Spreading false narratives about candidates and political parties to shape voter perceptions.
- Leaking sensitive government or party documents to damage reputations.
- Supporting populist and anti-EU movements to weaken European unity.

Russia's information warfare tactics are part of a broader hybrid warfare strategy, which combines disinformation, cyber operations, economic pressure, and military threats to achieve strategic objectives without engaging in open conflict. This approach has been particularly evident in:

- Ukraine: Since the annexation of Crimea in 2014, Russia has conducted extensive disinformation campaigns to justify its actions, discredit the Ukrainian government, and sow discord among Western allies.
- Baltic States: Estonia, Latvia, and Lithuania have frequently been targets of Russian cyberattacks and propaganda aimed at undermining NATO presence and stirring ethnic tensions.
- Africa and Latin America: Russian media and online influence campaigns have expanded into developing regions, seeking to counter Western influence and foster partnerships with local governments.

**United States of America:**

The United States has been a strong advocate for countering disinformation and defending against the weaponization of information, particularly following allegations of foreign interference in U.S. elections. The 2016 and 2020 presidential elections were pivotal moments that intensified concerns about cyber threats and information manipulation. Reports from U.S. intelligence agencies concluded that Russia engaged in large-scale disinformation campaigns and cyber operations to sow discord, weaken trust in democratic institutions, and influence voter perceptions. In addition to Russia, the U.S. has accused China, Iran, and other state and non-state actors of attempting to manipulate public discourse and interfere in domestic affairs.

In response to these threats, the U.S. government has implemented various cybersecurity measures and imposed sanctions on foreign institutions and individuals involved in disinformation campaigns and cyberattacks.

These measures consist of different approaches on political, economic and digital topics.

The U.S. has placed sanctions on Russian, Chinese, and Iranian entities accused of conducting cyber interference and disinformation campaigns. These sanctions have targeted intelligence agencies, media organizations, and private actors linked to state-sponsored cyber operations.

Since 2016, the U.S. has invested heavily in securing election infrastructure, working with tech companies and intelligence agencies to monitor and prevent foreign influence

campaigns. The Cybersecurity and Infrastructure Security Agency (CISA) plays a key role in detecting and mitigating cyber threats to democratic institutions.

The U.S. government has worked with platforms like Facebook, Twitter, and YouTube to combat the spread of false information by identifying and removing fake accounts, bot networks, and state-sponsored propaganda. However, regulating online content remains a complex challenge due to concerns over free speech and censorship.

Agencies like the NSA, FBI, and CIA have intensified their efforts to monitor, detect, and counter cyber threats from foreign adversaries. The U.S. Cyber Command plays a critical role in launching counter-cyber operations to disrupt hostile digital activities.

One of the biggest challenges in combating disinformation in the U.S. is the protection of free speech and press freedom, which are fundamental principles enshrined in the First Amendment of the U.S. Constitution. Unlike authoritarian regimes that can impose strict information controls and censorship, the U.S. cannot easily regulate false information without risking violations of democratic rights. This makes it difficult to find a balance between preventing foreign propaganda and protecting free expression.

To address this, U.S. policymakers and civil society organizations focus on media literacy programs, fact-checking initiatives, and public awareness campaigns to help citizens critically analyze information. Institutions like the National Endowment for Democracy (NED) and the Global Engagement Center (GEC) work to counter foreign propaganda while promoting independent journalism and open dialogue.

The modern digital age has blurred the lines between information warfare, cyber operations, and public diplomacy. While Russia and China are frequently identified as leading actors in disinformation campaigns, Western nations including the U.S. also engage in information influence efforts, diplomatic messaging, and strategic communication operations.
The challenge moving forward is how democratic societies can effectively counter disinformation and foreign cyber threats while upholding principles of free speech, transparency, and open debate. As information warfare becomes an increasingly sophisticated tool in global conflicts, the need for international cooperation, robust cybersecurity, and public resilience is more critical than ever.

**China**

China is another prominent player in the information warfare landscape. The Chinese government tightly controls domestic information through state media and great firewalls, which sensors foreign materials. Unlike Western democracies, which emphasize free speech and open information flow, China operates a highly centralized information environment, where the government maintains strict control over news, online platforms, and public discourse.

Domestically, China enforces rigorous censorship through its state-controlled media and the Great Firewall, which blocks foreign websites, censors' online discussions, and filters political content that contradicts government-approved narratives.

One of the most defining aspects of China's information strategy is its strict control over domestic information flow. The Great Firewall of China is a sophisticated system of internet censorship and surveillance that restricts access to foreign media, social media platforms, and politically sensitive content.

Some key elements of this system include the ban of certain websites such as Google, Facebook, Twitter, YouTube, and Wikipedia that are inaccessible in China, limiting exposure to external viewpoints.

Another restriction for the citizens is tight regulation of domestic platforms. The Chinese social media sites such as WeChat, Weibo, and Douyin (TikTok's Chinese counterpart) are heavily monitored, with strict policies on political discussions.
The Chinese government has an active employed internet police and automated censorship. China employs thousands of internet censors and AI-driven surveillance tools to delete content critical of the government and prevent dissent.
Lastly state-controlled media outlets, including Xinhua News Agency, China Central Television (CCTV), and the People's Daily, play a crucial role in reinforcing official narratives and promoting China's political ideology. These media channels frame domestic and global events in ways that support the Chinese Communist Party (CCP) while downplaying negative coverage.

Beyond its domestic censorship**,** China has been accused of spreading state-sponsored propaganda, suppressing criticism as well as an active engagement in international information warfare to shape perceptions of its policies and expand its global influence.

China actively works to control the international narrative on politically sensitive topics, such as the territorial conflict between Taiwan and China. China opposes Taiwan's independence and seeks to delegitimize its government by spreading narratives portraying Taiwan as an inseparable part of China while pressuring foreign media to avoid language that implies Taiwan's sovereignty.
Since the 2019 pro-democracy protests in Hong Kong, China has sought to frame protesters as violent extremists, while censoring domestic news about police brutality and the suppression of civil liberties.
Reports from international organizations and human rights groups have accused China of committing human rights abuses against Uyghurs in Xinjiang, including mass detentions, forced labor, and re-education camps. China has responded by spreading counter-narratives

portraying these camps as vocational training centers and dismissing criticism as Western propaganda.

China has heavily invested in global media expansion to counter Western narratives and promote pro-China viewpoints.
Media outlets such as CGTN (China Global Television Network), Xinhua, and China Daily produce English-language content that presents China in a positive light and amplifies pro-Beijing narratives. These platforms often criticize Western democracies while highlighting China's economic and technological advancements.
China provides grants, training programs, and financial incentives to foreign journalists and news agencies in developing countries to encourage pro-China reporting. This is particularly evident in Africa, Latin America, and Southeast Asia.
Chinese state actors and influencers are active on platforms such as Twitter, YouTube, and Facebook (despite them being banned in China) to promote Chinese policies and attack critics

China has been implicated in covert cyber operations aimed at influencing foreign audiences and discrediting opponents. Chinese actors have been found creating and amplifying fake social media accounts to spread misinformation, particularly in response to criticism about Hong Kong, Xinjiang, and Taiwan.
Chinese cyber groups have been linked to hacking operations targeting foreign governments, businesses, and media organizations to access sensitive information and disrupt democratic processes.
The Chinese government engages with Chinese-language media and community organizations abroad to promote pro-Beijing messages and discourage dissent among overseas Chinese populations.

**European Union (EU):**

The European Union has taken a strong stance against disintegration, especially in response to the Russian propaganda efforts targeting the member states of the European Union. The East StratCom Task Force of the European Union was designed to identify and combat foreign disintegration, and the Digital Services Act (2022) aims to regulate social media platforms to prevent the spread of fake news.

**NATO (North Atlantic Treaty Organization):**

The NATO recognizes the weapons of information as an increasing safety threat. Alliance has developed a strategy for disintegration, including facts, cyber defence programs and public awareness campaigns. NATO often highlights the use of Russia's disintegration as a tool to weaken western unity and destroy democratic institutions. The organization encourages member states to invested in cyber security and to strengthen cooperation to prevent the spread of manipulated information.

**Social media and tech companies (meta, x, Google, tickets, etc.):**

Technology companies play an important role in controlling the spread of disintegration, as many campaigns rely on platforms such as Facebook (META), X (East Twitter), YouTube, and TikTok. These companies have introduced fact-check programs and AI equipment to detect and remove false content. However, they face criticism to combat dissolution and not enough for discrepancies in material moderation. Some governments push for strict regulation, while tech companies argue that extremely aggressive policies can limit censorship and freedom of expression.

**United Nations:**

The United Nations has acknowledged the dangers of disinformation and the role it plays in fuelling conflicts. The United Nations has called for global cooperation to combat the spread of false information, while also ensuring that rules do not violate speech. Agencies such as UNESCO focus on promoting media literacy and moral journalism, while the United Nations efforts against cyber threats tried to establish international norms for responsible information-sharing.

## Timeline of Events

**1914-1918** - *World War I and the Rise of Propaganda*

Governments used mass media to spread nationalist propaganda, manipulate public opinion, and demonize enemies. This marked the beginning of modern information warfare.

**1933-1945** - *Nazi Germany's*

Propaganda Machine Joseph Goebbels, as Minister of Propaganda, led large-scale misinformation campaigns to control public perception, suppress opposition, and justify military aggression.

**1947-1991** - *Cold War and the Spread of Disinformation*

The United States and the Soviet Union engaged in psychological warfare, using propaganda, covert operations, and media influence to promote their ideologies and discredit opponents.

**2003** - *Iraq War and the Role of Misinformation*

The U.S. justified the invasion of Iraq based on intelligence reports claiming Iraq possessed weapons of mass destruction (WMDs). These claims were later proven false, fuelling debates on political misinformation.

**2014** - *Russian Annexation of Crimea and Disinformation Tactics*

Russia used state-controlled media, fake social media accounts, and fabricated narratives to justify the annexation of Crimea and discredit Ukrainian resistance.

**2016** - *Russian Interference in the U.S. Presidential Election*

Russian actors allegedly spread false news, hacked emails, and used social media bots to influence the U.S. election, leading to international concerns about foreign interference in democratic processes.

**2019-2021** - *COVID-19 Pandemic and Global Disinformation*

The pandemic saw an explosion of false information regarding vaccines, treatments, and the origins of the virus. Governments and social media companies struggled to contain the spread of misinformation.

**2022** - *Russia-Ukraine War and the Use of Information Warfare*

Russia launched large-scale disinformation campaigns to justify the invasion of Ukraine, while Ukraine and Western allies countered with fact-checking efforts and sanctions against Russian media outlets.

**2023** - *AI and Deepfake Technology in Disinformation*

The rapid advancement of AI-generated deepfakes raised concerns about their use in spreading false narratives, influencing elections, and destabilizing societies.

**2024** - *Global Regulations on Digital platforms Intensify*

In response to increasing threats from disinformation, governments worldwide implemented stricter laws to regulate online platforms, leading to ongoing debates about free speech versus security.

## Previous attempts to solve the issue

1. European Union's Digital Services Act (2022)

The Digital Services Act (DSA) introduced strict regulations for online platforms, requiring them to remove harmful content, particularly disinformation related to elections, health, and security. The EU has also established fact-checking networks and imposed fines on companies falling to combat misinformation.

But there was a Risk of over-censorship and limiting free speech.
Additionally, the Misinformation still spreads quickly before platforms can reach and at last, some governments misuse disinformation laws and suppress opposition.

2. NATO's Strategic Communications against Disinformation

NATO has actively countered Russian propaganda, particularly in Eastern Europe, through fact-checking initiatives and cybersecurity programs. The NATO StratCom Centre of Excellence works on identifying and countering false narratives.

The challenges are, that non-member states, particularly Russia and China, perceive NATO's efforts as biased. Also, disinformation actors continually adapt their tactics, making it difficult to counter effectively and lastly, internal divisions within NATO countries are sometimes fueled by disinformation.

3. U.S. Government Actions Against Foreign Influence

The United States has implemented sanctions and cybersecurity measures against foreign entities involved in election interference, while agencies like the Global Engagement Center (GEC) track and counter disinformation campaigns.

Challenges are, that Efforts are sometimes seen as politically motivated, leading to accusations of bias. Additionally, Tech companies resist government intervention due to concerns about free speech and foreign disinformation actors constantly evolve their methods, making prevention difficult.

4. Social Media Platforms' Factchecking and Content Moderation

Companies like Meta (Facebook), X (Twitter), Google, and TikTok have introduced fact-checking partnerships and AI-driven content moderation to combat disinformation, particularly during elections and global crises.

Challenges are the inconsistent enforcement across different platforms and regions. As well as the automated systems struggle to distinguish between satire, opinion, and genuine misinformation and the disinformation networks adapt by moving to private groups and alternative platforms.

## Possible Solutions

### 1. International treaty on digital disinformation

A legally binding international agreement can be established to regulate the proliferation of disintegration on borders under the United Nations. This treaty will set global standards to identify and combat false information, require social media platforms to increase transparency, and set up a outline for international cooperation in fighting disintegration campaigns.

### 2. Stronger AI-Powered detection and fact-Checking Systems

Governments, international organizations and tech companies can invest in advanced artificial intelligence to detect and remove false information. AI-operated equipment can manipulate deepfacks, fake news and materials in real time, making them reduce the spread of harmful narratives before reaching large audiences.

### 3. Global media literacy and public awareness campaigns

Educating the public on how to identify disintegration is a long -term solution to propagate and reduce the effectiveness of false narratives. Governments, school and media organizations can launch educational programs, functioning and awareness campaigns to teach important thinking skills and promote fact-ties habits among internet users.

# Bibliography

https://www.oii.ox.ac.uk

https://shorensteincenter.org

https://www.rand.org

https://www.unesco.org/en

https://digital-strategy.ec.europa.eu/en/policies/online-disinformation

https://stratcomcoe.org

https://www.state.gov/global-engagement-center

https://www.brookings.edu

https://www.cfr.org

https://carnegieendowment.org/?lang=en

https://www.bbc.com/news/bbcverify

https://www.nytimes.com/section/cybersecurity

https://www.reuters.com/fact-check/

https://www.theguardian.com/world/information-warfare

https://transparency.meta.com/de-de/

https://jigsaw.google.com

https://www.pewresearch.org

https://www.un.org/en

https://www.osce.org

https://www.europarl.europa.eu/portal/en

https://cepa.org

https://www.washingtonpost.com