DISINFORMATION AS A TOOL FOR ESPIONAGE

Aadya Dubey, PhD Scholar- Barkatulla University, Bhopal

ABSTRACT

Ever since the Russians meddled with America's Presidential elections in 2016, disinformation has become much more of a global issue. Disinformation was traditionally employed as one of the techniques for performing wartime espionage, but it has recently evolved into a method for doing it during peacetime as well. This paper explores the relevance of disinformation in the international domain. It demonstrates many of the prominent cases and instances in our history where disinformation was used in order to mislead people during peacetime and how it is being used as a tool for espionage. It is very challenging to deal with disinformation on an international scale as there is a limit to the regulations by international law. This paper will qualitatively analyse various aspects of disinformation used for espionage during peacetime that are prevalent in our society and how greatly it affects our society. Such analysis might help people by not getting misled. We will be better positioned to avoid being duped by intentionally misleading information. Also, this paper shows the research that how disinformation affects large communities internationally and the ways that a government could use to control and prevent the spread of such fake news.

Keywords: Disinformation, Espionage, International Law, Peacetime, Fake News, Security

INTRODUCTION

Disinformation is a severe challenge to democracy. Today's newest and deadliest weapon of war might not be tanks or soldiers but rather the unregulated and rapid spread of domestic and international disinformation campaigns through social media. The biggest example of such a campaign is Russia's interference in the 2016 America Elections. Also, on Feb. 27, Facebook said it discovered Russian efforts to spread misinformation about Ukraine on its platform.[1]The recent example of spreading fake news and disinformation was seen in the pandemic, and India has emerged as the biggest source of Covid misinformation, with 1 in 6 pieces of fake information coming out of the country, a new Times of India study has found.[2]

Disinformation is spreading because, sadly, it works. The harsh reality is that we are all vulnerable to this new type of weapon with theuse of social media. Furthermore, it is simple to fall victim unintentionally since malicious actors are getting more inventive with how they display and spread false information and disinformation. Also, even worse, we might be the ones who spread it by clicking or tapping a button to send the news to our friends and family.

DISINFORMATION is "*false information deliberately and often covertly spread (as by the planting of rumours) in order to influence public opinion or obscure the truth*."[3]However, it is important to acknowledge that disinformation has evolved into a complex problem, one that is far bigger than the definition above. Previously it was a domestic issue, but now, it has become an international issue. A New York Times examination of hundreds of American posts shows that one of the most powerful weapons that Russian Agents used to reshape American politics was spreading mis- and disinformation that real Americans were broadcasting across various social media platforms, which is now believed to be at the centre of a far-reaching Russian program to influence the 2016 presidential election.[4]

[1]Helen Lee Bouygues, *When misinformation becomes a weapon: How you can fight back*, FORBES (March 16, 2022, 10:09 AM), https://www.forbes.com/sites/helenleebouygues/2022/03/16/when-misinformation-becomes-a-weapon-how-you-can-fight-back/?sh=5ec5fdd36aad.
[2]Chandrima Banerjee, *India World's biggest Covid misinformation source: Study*, THE TIMES OF INDIA (Sep. 15, 2021, 17:22 IST), https://timesofindia.indiatimes.com/india/india-worlds-biggest-covid-misinformation-source-study/articleshow/86229400.cms.
[3]Merriam-Webster, https://www.merriam-webster.com/dictionary/disinformation (last visited Oct. 29, 2022)
[4]Nicholas Confessore& Daisuke Wakabayashi, *How Russia harvested american rage to reshape U.S. politics*, THE NEW YORK TIMES (Oct. 9 2017), https://www.nytimes.com/2017/10/09/technology/russia-election-facebook-ads-rage.amp.html

WHAT IS DISINFORMATION?

The term "Disinformation" became even more popular after the COVID-19 pandemic. However, some countries use misinformation and fake news in a context similar to disinformation. It is to be noted that disinformation is not synonymous with misinformation or fake news. Misinformation means incorrect or misleading information.[5] It is when false information is shared, but there is no intent to mislead.People spread false information because they believe it is true when it is not. Whereas fake news items are lies – that is, deliberately false factual statements distributed via news channels.[6]

So, when the information is deliberately created with the intention to mislead and cause harm, it is referred to as 'Disinformation'. Disinformation frequently contains "half-truths" or some elements of reality. As a result, the consumer will find it more challenging to identify disinformation. Today, political disinformation has become an important issue that needs to be dealt with. Political disinformation, or propaganda, as a subset of disinformation, is the intentional dissemination of false information seeking to shape perceptions around some aspect of political discourse.[7]

While disinformation is not a new concern, new technologies have enabled people and organisations to broadcast messages faster and to a wider audience than ever before. Disinformation campaigns enlist a huge number of people or groups to interact with the content, which encourages others to share and post it. A disinformation campaign occurs "*when a person, group of people or entity (a "threat actor") coordinate to distribute false or misleading information while concealing the true objectives of the campaign*."[8]The Govt must

[5]Merriam-Webster. https://www.merriam-webster.com/dictionary/misinformation , (last visited Oct. 29, 2022)
[6]For an overview, see M. Verstraete et al., 'Identifying and Countering Fake News', Arizona Legal Studies Discussion Paper no. 17-15 (2017), at 5–9.
[7]*Legal Responses to Disinformation - a Policy Prospectus*, ICNL, (Dec. 2, 2021), https://www.icnl.org/wp-content/uploads/2021.03-Disinformation-Policy-Prospectus-final.pdf
[8]Public-Private Analytic Exchange Program (U.S.), *Combatting Targeted Disinformation Campaigns A whole-of-society issue*, HOMELAND SECURITY DIGITAL LIBRARY (Oct. 2019), https://www.hsdl.org/c/view?docid=845040

deploy new methods to curb these practices, and the public must be aware of such campaigns so they do not become prey to them.[9]

Today, it is found that some multimedia and algorithms are developed to mislead and change the original meaning of the information and spread distrustful and manipulated information among the people, which is called synthetic media. Hence, knowledge about disinformation is more important now than ever. We have already discussed different forms of information disorders and gathered that many use the term 'Disinformation' as a common or general reference to all the above categories. Disinformation also takes many different forms. For a better understanding of the same, let us discuss a few of them:

Fabricated Content- Here the information is made with the guilty intention to make people believe that they will have some financial or political gain, but in the end, they lose their money to the frauds.

Manipulated Content- When genuine information or imagery is manipulated to deceive.[10]

It usually involves photographs and videos that have been edited in such a way that they appear real enough, but the overall meaning of the genuine content is different than intended.

Imposter Content- When authentic sources are impersonated.This type of information is very harmful because it is done under the name of authentic media but is spread by false media. These imposter content creators take advantage of the trust that has been held by the news agencies and use their reputation to spread disinformation to consumers who may be uninformed about the validity of the fake news agencies.

Misleading Content - Misleading or misrepresented information is when the information is being provided by the media, which does not directly say the things, but it is a matter of what people gain out of it.

False Context- When legitimate content is distributed alongside fake contextual information. Here, an example might be an image that has been shared to fit a different story. Here, the

[9] Ibid
[10] *Disinformation and 7 common forms of information disorder*, HIVE MIND, (Oct. 30, 2022, 3:55 PM), https://en.hive-mind.community/blog/169,disinformation-and-7-common-forms-of-information-disorder

content used is authentic, so it cannot be refuted but is reframed in a harmful way to promote a specific point.

Propaganda- In propaganda, the facts are represented in a way to provoke a certain feeling or the desired response.[11]

DISINFORMATION - WHO IS SPREADING IT AND WHY?

Disinformation and manufactured content are being created, shared, and consumed on social media at an alarming rate, especially given how simple it is to access these platforms and how little people are aware of the availability of such false information. It has been substantially expanded by the internet and social media, making it possible for everyone, from teenagers to tyrants, to propagate false information. Deception now casts into doubt everything from corporate brands to individual citizens and public health to election results.[12]We have recent examples of COVID-19 disinformation tactics and the 2016 American election disinformation campaign to substantiate this claim. Understanding who is behind such operations and the motivations behind the dissemination of disinformation is crucial.

Today, social media and technology have also facilitated the spread and expansion of disinformation and so-called disinformation campaigns.Disinformation is primarily spread by those who want to *sway public opinion and further specific agendas*. It includes false and out-of-context information that is disseminated with the intent to deceive or mislead.Disinformation campaigns, is usually propagated for political gain by state actors, party operatives, or activists, deliberately spread falsehoods or create fake content, like a video purporting to show the Chinese Govt executing residents in Wuhan with COVID-19 or "Plandemic," a film claiming the pandemic is a ruse to coerce mass vaccinations, which most major social media platforms recently banned.[13]Disinformation can also be propagated by a host of online actors, including governments, state-backed entities, extremist groups and

[11]*Fake News and its intents: Propaganda, Disinformation & Misinformation*, WAYNE STATE UNIVERSITY LIBRARY SYSTEM, (Sep 1, 2021 3:05 PM), https://guides.lib.wayne.edu/c.php?g=401320&p=2729574
[12]John Romeo, *Disinformation is a growing crisis. Governments, business and individuals can help stem the tide*, WORLD ECONOMIC FORUM, (Oct 11, 2022), https://www.weforum.org/agenda/2022/10/how-to-address-disinformation/
[13]Christina Pazzanese, *Battling the 'pandemic of misinformation'*, THE HARVARD GAZZETTE, (May 8, 2020), https://news.harvard.edu/gazette/story/2020/05/social-media-used-to-spread-create-covid-19-falsehoods/

individuals.[14]These governments, state-backed organisations, and extremist groups now have unrestricted access to social media and the internet, allowing them to conduct national and international disinformation campaigns.Sometimes it can be linked back to them; sometimes, it might not. In the case of an Individual, it can be quite challenging to identify the precise offender when someone is disseminating false information across borders because they may be sitting far away and using the internet.However, it is illegal to propagate false information within one's own country. During COVID-19, we witnessed numerous cases of this happening in various nations, as well as the response of the authorities in each case. India, Kenya, Morocco, and Palestine are a few countries that have taken action against individuals spreading disinformation about the coronavirus. One such arrest included a woman who had been distributing false information about the COVID-19 condition via her YouTube channel.

WHAT IS ESPIONAGE? WITH EMPHASIS ON PEACETIME ESPIONAGE

Espionage poses a massive threat to national security. Espionage between states is a long-standing and widespread human activity that occurs in various areas. In the international arena, espionage is prevalent not only between countries that are political rivals but also between allies and neighbours. The subject of espionage during times of war has long been addressed by international law, but that of peacetime espionage has not.Firstly, let us see what espionage means. It is generally defined as "*the process of getting information that is not typically publicly available, using human sources (agents) or technical means (such hacking into computer systems)*."[15]

Espionage has many different aspects, including its goal, techniques, and application, but it is crucial to remember that, in the absence of war, espionage during peacetime is strangely absent from international law.Even though international law has developed into many different areas that cover anything from business to health to the environment to war, it is still unclear concerning espionage, especially in times of peace. Gathering intelligence through covert techniques presents a problem for international law because it affects the national security of target countries. This comprises gathering information inside the borders of another country without that country's knowledge or agreement using a variety of sneaky, intrusive methods.

[14]Spencer Feingold, *The four key ways disinformation is spread online*, WORLD ECONOMIC FORUM, (Aug. 9, 2022), https://www.weforum.org/agenda/2022/08/four-ways-disinformation-campaigns-are-propagated-online/

[15]*Counter-Espionage*, SECURITY SERVICE MI5, (Nov. 6, 2022, 4:14 PM), https://www.mi5.gov.uk/counter-espionage

For a long time, it was believed that nation-states had the authority to conduct these kinds of intelligence operations, especially when there was conflict. Some of the concerns surrounding information collecting during times of conflict, particularly the treatment of spies, are already covered by the *Geneva Conventions of 1949 and 1977* and the *Vienna Convention on Diplomatic Relations (1961*). In contrast, peacetime espionage is never explicitly addressed under the ambit of international law.

Peacetime espionage is often employed by states as a means of acquiring information about competitor states in the international system.[16]Further, such actions are not limited to hostile states, as even allied countries regularly spy on each other.[17]Acts of espionage often designated for use against enemies are also used against ally states in a world where security concerns are an ever-present factor for state activity. The fundamental tenet is that while alliances can promote mutual trust and collaboration, they do not necessarily imply that an ally will always be trustworthy and loyal, particularly when it comes to matters of national importance. Due to the international system and the necessity to protect one's interests and population, espionage, even against allies, will always be a vital state function. As a result, all states should be on the lookout for attempts to steal their state secrets.Typically, States engage in espionage to gather data about the political plans, economic goals, and military prowess of other States.

Kulbhushan Jadhav is a claimed suspect in such an act.On March 3, 2016, Pakistan detained Jadhav on the pretext that he was an Indian spy deployed there to engage in subversive activities. After an odd 22-day wait, India was informed of Jadhav's arrest on March 25, 2016. India said that Jadhav was kidnapped and prosecuted on concocted allegations of terrorism and espionage when he was running a business in Iran after retiring. India subsequently requested Jadhav's consular access on many occasions in order to meet him and set up his legal counsel. Pakistan not only refuted this but also made it clear that it would only do so if India helped with the inquiry into Jadhav.India filed a case before the ICJ on 8 May 2017, accusing Pakistan of egregious violations of the VCCR.[18]If Jadhav really did serve Indian intelligence, as Pakistan

[16]LereAmusan&Siphiwe Mchunu, *Adventure into Peacetime Intra-Alliance Espionage: Adventure into Peacetime Intra-Alliance Espionage: Assessment of the America-Germany Saga*, (33), LITHUANIAN FOREIGN POLICY REV. 64, 64, (2015), https://www.researchgate.net/publication/291835350_Adventure_into_Peacetime_Intra-Alliance_Espionage_Assessment_of_the_America-Germany_Saga

[17]Jared Beim, *Enforcing a Prohibition on International Espionage*, 18, Chi. J. Int'l L. 647, 651, (2018), https://chicagounbound.uchicago.edu/cjil/vol18/iss2/6

[18]AarshiTirkey, *The Kulbhushan Jadhav verdict: A certain win, with uncertain outcomes*, OBSERVER RESEARCH FOUNDATION (July 19, 2019), https://www.orfonline.org/expert-speak/the-kulbhushan-jadhav-verdict-a-certain-win-with-uncertain-outcomes-53188/?amp

alleges, he would not enter Pakistani territory but rather conduct his operations from Iran. A spy seldom risks being captured by entering the lion's den.Intelligence operations involve two types of professional profiles -- intelligence officers who are officially part of an intelligence organisation; and agents -- outsiders who undertake assignments due to their access to a particular person, area or organisation.[19] And, Jadhav, a former navy captain who now runs a company in Iran, was neither an intelligence agent nor an officer.

Peacetime intelligence gathering enables nation-states to judge potential threats more accurately and to choose between peaceful or hostile courses of action. Intelligence gathering often provides the basis for the *jus ad bellum* or criteria to go to war.[20]Gathering intelligence during peacetime is always intended to confirm a target nation's intentions and capability for wartime. In light of this, the nation in question that authorises intelligence collecting operations against another country only does so in order to prepare militarily to defend against the possibility of a surprise invasion.

The disinformation as a tool for peacetime espionage comes into the picture when the spies transform themselves into clandestine violent non-state actors.[21]They now actively engage in terrorist or violent political incitement in the host nation rather than only collecting intelligence in a passive manner.

TOOLS OF ESPIONAGE

Espionage typically conjures images of spies breaking into a business's secure vaults and stealing or copying formulas or goods. National spies, typically shownlike James Bond, retrieve government secrets while working in opulent environments. The reality is a little different, though, and espionage is becoming a bigger issue in a world of escalating business rivalry and computer-based data storage. The tools to spy have evolved to include computers and other high-level technology."*Modern spy tools are faster, smaller, more accurate and more easily concealed*," says Peter Earnest, a retired senior CIA official and the executive director

[19]BidandaChengappa, *Peacetime spying is legitimate*, DECCAN HERALD (Aug. 31 2019, 09:39 IST), https://www.deccanherald.com/opinion/in-perspective/peacetime-spying-is-legitimate-758209.html
[20]Ibid.
[21]Supra note 19.

of the International Spy Museum. "But they're the same basic idea as the old ones."[22]

Throughout the course of human history, several incredibly inventive and complicated tools have been made.Recently, the advancement of unmanned spy planes (they can monitor targets from above), satellites, and electronic surveillance has received more attention than the work of human agents. However, despite the end of the Cold War and less well-defined security concerns, the role of the individual spy is still important in learning what the enemy is truly thinking. They will need those cool James Bond tools as long as they are still on the ground.

DISINFORMATION IN INTERNATIONAL RELATIONS

Disinformation in the context of international relations concerns the deliberate spread of false or unbalanced information by foreign states with the primary objective to confuse and mislead to sow disagreement and discord among parts of the population in other countries.[23]The aim of the disinforming state is to strategically gain from other governments' decisions that come from these conflicts and, in the end, to expand one's relative international power. Disinformation or information manipulation is a tool used by the foreign policy in international relations.Disinformation as a tool for foreign policy can be a component of a far more extensive and deadly network of international state-led activities, such as espionage, cyber-attacks, and other subversive actions.Concerns over International disinformation have recently intensified. Policy-makers, pundits, and observers worry that countries like Russia are spreading false narratives and disseminating rumours in order to shape public opinion and, by extension, government policies to their liking.[24]

DISINFORMATION AS AN ESPIONAGE TOOL

Disinformation, in simple words, is false/fake information deliberately spread to deceive people. On the other hand, espionage is the practice of spying or using spies to obtain information about the plans and activities, especially of a foreign government or a competing

[22]*The Evolution Of Spy Tools*, FORBES (Apr 19, 2006, 09:00am EDT), https://www.forbes.com/2006/04/15/intelligence-spying-gadgets_cx_lh_06slate_0418tools.html?sh=6cd91d6d65c0
[23]André W.M. Gerrits, *Disinformation in International Relations: How Important Is It?,* BRILL (Dec. 12, 2018), https://brill.com/view/journals/shrs/29/1-4/article-p3_3.xml
[24]Alexander Lanoszka, *Disinformation in International Politics*, SSRN (May 4, 2018), https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3226258_code1511778.pdf?abstractid=3172349&mirid=1&type=2

company.[25]The state governments obtain the information of other states by spying or using spies and then deliberately spread false information with the main objective to confuse, mislead or to sow discord among the population in other states. Conventionally, this tactic was used only when the countries were at war with each other. However, it is currently practised even when the countries areat peace with each other. This paper provides a brief overview of some of the worldwide disinformation cases-

Pakistan's coordinated disinformation campaign against India

The Ministry of I&Bhas mandated the shutdown of 35 channels on the online video-sharing platform YouTube and 2 websites as part of strict measures to combat fake news on the Internet. These websites were actively involved in the coordinated propagation of disinformation and anti-Indian propaganda online**.**The channels and websites belong to a coordinated disinformation network operating from Pakistan and spreading fake news about various sensitive subjects related to India. The channels were used to post divisive content in a coordinated manner on topics like Kashmir, the Indian Army, minority communities in India, Ram Mandir, General Bipin Rawat, etc.[26] Apart from this, it is pertinent to mention that their social media presence expanded to Twitter, Instagram, and Facebook, wherein the Government blocked two Twitter accounts, two Instagram accounts, and one Facebook account for participating in the coordinated online propagation of disinformation about India.

The *modus operandi* of the anti-India disinformation campaign involved The Naya Pakistan Group (NPG), operating from Pakistan, having a network of YouTube channels, and some other standalone YouTube channels not related to NPG. The channels had a combined subscriberbase of over 35 lakh, and their videos had over 55 crore views. Some of the YouTube channels of the Naya Pakistan Group (NPG) were being operated by anchors of Pakistani news channels.[27]

These YouTube channels also published content on topics like the farmers' protest, the Citizenship (Amendment) Act protests, and attempts to instigate minorities against the Indian

[25]Merriam-Webster. https://www.merriam-webster.com/dictionary/espionage, (last visited Oct. 30, 2022)
[26]PIB Delhi, *Delhi India dismantles Pakistani coordinated disinformation operation*, PRESS INFORMATION BUREAU GOVERNMENT OF INDIA (Dec. 21, 2021, 2:45 PM), https://pib.gov.in/Pressreleaseshare.aspx?PRID=1783804
[27]Ibid.

Government. The democratic process of the approaching elections in five states was also thought to be compromised by the usage of these YouTube channels to upload content.

The Ministry of Information & Broadcasting has issued an order to block these Pakistan-based social media accounts and websites pursuant to Rule 16 of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. The majority of the content deals with topics that are sensitive from the standpoint of national security, is factually incorrect, and is primarily posted from Pakistan as part of a coordinated disinformation network (as in the case of the Naya Pakistan Group) against India.

These social media profiles and websites were being actively watched by Indian intelligence agencies, who flagged them to the Ministry for prompt action.

Disinformation spread by China regarding Covid 19 quarantine in the US

In the middle of March 2020, disturbing news erupted on cell phones all around the United States. According to a source in the US Department of Homeland Security, a series of ominous messages claimed that the Trump administration was putting armed US soldiers on the streets to enforce a lockdown in reaction to COVID-19. "*They will announce this as soon as they have troops in place to help prevent looters and rioters*," said one text. The anonymous sender noted that his friend "got the call last night and was told to pack and be prepared for the call today with his dispatch orders."[28]It implores readers to spread the message to friends and family. Similar communications alerted recipients to an impending federal quarantine.The Nationwide Security Council responded promptly, tweeting on March 15 that "*text message claims of a national quarantine are FAKE*." '*There is no nationwide lockdown*." It did nothing to calm some receivers, who hurriedly contacted their friends and relatives.According to the US government, the messages were a component of a disinformation operation designed to cause chaos and uncertainty during the early phases of the COVID-19 issue.

According to six American officials who spoke on the condition of anonymity in order to publicly discuss intelligence issues, the US intelligence community has determined that Chinese operatives assisted in spreading the information since that wave of fear. The

[28]Seth G. Jones, *The New Weapons of War: Disinformation, Economic Coercion, and Online Disruption*, LIT HUB (Sep. 28, 2021), https://lithub.com/the-new-weapons-of-war-disinformation-economic-coercion-and-online-disruption/

disinformation appeared as SMS on numerous Americans' smartphones, a method that some of the officials claimed they had never seen before, which alarms them about the amplification techniques. According to them, this has prompted organisations to examine fresh methods that China, Russia, and other countries are utilisingto promote disinformation during the epidemic.

However, the origin of the messages remains murky. American officials declined to reveal details of the intelligence linking Chinese agents to the dissemination of the disinformation, citing the need to protect their sources and methods for monitoring Beijing's activities.[29]

US Attempt of Espionage in Pakistan

Early in 2011, Shakil Afridi, a Pakistani Doctor, went door-to-door in Abottabad, Pakistan, promising to deliver Hepatitis B vaccines. In reality, the Central Intelligence Agency (CIA) had recruited Dr. Afridi to gather DNA samples as a prelude to the assassination of Osama bin Laden, the Al Qaeda leader.[30]In the garb of these vaccination campaigns, the US and its allies are running their spying networks.[31] This deception fueled widespread suspicions of vaccine campaigns, severely undermining the global polio eradication effort. It led to public backlash; polio vaccinators were attacked and threatened. Salma Farooqi, a mother of four, was kidnapped, tortured, and killed in March 2014 for providing polio vaccines. Many other such health workers were murdered. Therefore, the Obama administration formally ended its use of vaccine campaigns as a ruse for spy operations on May 20, 2014.

The CIA's ruse provided political cover for militants looking to capitalise on pre-existing fears. For example, disinformation campaigns have linked polio vaccination campaigns to Western plots to sterilise Muslims. Rumours have also circulated that the vaccines contained porcine contaminants, which are prohibited by Islam. Indeed, the interplay of immunisation, ideology, and religion has resulted in a toxic mix, with poor children bearing the brunt of the consequences.

[29]Edward Wong, Matthew Rosenberg, &Julian E. Barnes, *Chinese Agents Helped Spread Messages That Sowed Virus Panic in U.S., Officials Say*,THE NEW YORK TIMES (April 22, 2020),https://www.nytimes.com/2020/04/22/us/politics/coronavirus-china-disinformation.html
[30]Lawerence O. Gostin, *Global Polio Eradication: Espionage, Disinformation, and the Politics of Vaccination*, THE MILBANK QUARTERLY (Sep. 2014), https://www.milbank.org/quarterly/articles/global-polio-eradication-espionage-disinformation-and-the-politics-of-vaccination/
[31]Jon Boone, *Taliban leader bans polio vaccinations in protest at drone strikes,* THE GUARDIAN (Jun. 26, 2012, 08.42 BST), https://www.theguardian.com/world/2012/jun/26/taliban-bans-polio-vaccinations

Pegasus Spyware- Who is spreading disinformation?

In July 2021, Amnesty international and other organisations released a report investigating the software which was used to infiltrate the phones of human rights activists and journalists across the globe. The investigation revealed a spy software called 'Pegasus' which was used to strategically hack phones. The software was created by the NSO group, an Israeli surveillance firm.[32]It is a kind of malicious software that hacks into smartphones to collect the stored data and sell the same to third parties without the consent of the concerned parties. The malware becomes activated when it enters the phone and gets all access to keep track of the activity of the phone, including contact list, SMS, gallery, files, and location.[33]The revelations concerning its widespread use, including by India's Government, came to light earlier this month after Amnesty International and the Paris-based media nonprofit Forbidden Stories got access to leaked records of thousands of phone numbers that NSO Group clients had selected for potential surveillance.[34]In accordance with the aforementioned report, Israeli spyware has targeted more than 300 Indian mobile phones, including those of three opposition leaders, two central ministers of the Union Cabinet who are still in office, as well as judges, politicians, journalists, lawyers, human rights activists, and businesspeople. According to the report, the Pegasus spyware company illegally and forcibly gained access to Indian cell phones in order to access all of the handsets' data, which they then sold to government officials.

However, NSO refuted the allegations made by the report in its statement. It stated that "the report by Forbidden Stories is full of wrong assumptions and uncorroborated theories that raise serious doubts about the reliability and interests of the sources. It seems like the unidentified sources have supplied information that has no factual basis and are far from reality."[35]The Company said"after checking their claims, we firmly deny the false allegations made in their report. Their sources have supplied them with information that has no factual basis, as evident

[32]ShreshthaMenon , *Surveillance Laws in India in light of the Pegasus Project*, 4 (5) IJLMH 1011, 1011 (2021) https://doij.org/10.10000/IJLMH.112002
[33]Gaurav Kumar, *An Analysis of the Pegasus Spyware issue in light of Surveillance Laws and the Right to Privacy in India*, 2 (3) JUS CORPUS LAW JOURNAL 394, 396 (2022), https://www.juscorpus.com/wp-content/uploads/2022/04/81.-Gaurav-Kumar.pdf
[34]WasanthaRupasinghe, *Modi government calls exposure of its use of Pegasus to spy on political opponents "fake news",* WORLD SOCIALIST WEB SITE (July 31, 2021), https://www.wsws.org/en/articles/2021/07/31/pega-j31.html
[35]*Pegasus spyware: Reports of hacking "false, misleading", says Israeli firm,* THE TIMES OF INDIA (Nov. 10, 2022, 14:48 IST), https://timesofindia.indiatimes.com/india/pegasus-spyware-reports-of-hacking-false-misleading-says-israeli-firm/articleshow/84547543.cms

by the lack of supporting documentation for many of their claims. In fact, these allegations are so outrageous, and far from reality, that NSO is considering a defamation lawsuit."[36]

In the statement, it is said that NSO Group has reason to think that the assertions made by the unidentified sources to Forbidden Stories are based on an inaccurate interpretation of information from readily available and obvious sources, such as HLR Lookup services, and have no influence on the list of consumers that Pegasus or any other NSO product is intended to target.

The organisation contends that these services are freely accessible to everyone, everywhere, and at any time, and are frequently used by both private businesses and governmental organisations around the world for a variety of objectives.

Though the NSO Group insists the leaked database is "not a list of numbers targeted by governments using Pegasus", it told *The Wire* and Pegasus Project partners in a letter from its lawyers that it had "good reason to believe" the leaked data "may be part of a larger list of numbers that might have been used by NSO Group customers for other purposes". Asked what these "other purposes" could be, the company changed tack and claimed that the leaked records were based on "publicly accessible, overt sources such as the HLR Lookup service" – and that it had no "bearing on the list of the customer targets of Pegasus or any other NSO products."[37] However,NSO insists that if someone misused Pegasus or other products, they did so on their own accord.[38]

The Indian Government also unequivocally denied all 'over the top allegations' of surveillanceusing Pegasus Spyware. The Union government called the story "sensational, " seeming to be an attempt "to malign Indian democracy and its well-established institutions".[39] The Ministry of Electronics and Information Technology said that "India is a robust democracy that is committed to ensuring the right to privacy to all its citizens as a fundamental right" and that the "allegations regarding government surveillance on specific people has no concrete

[36]*Ibid.*
[37]Siddharth Varadarajan, *Pegasus Project: How Phones of Journalists, Ministers, Activists May Have Been Used to Spy On Them*, THE WIRE (Jul. 18, 2021), https://m.thewire.in/article/government/project-pegasus-journalists-ministers-activists-phones-spying
[38]Ariel Kahana, '*NSO accusations were part of international disinformation campaign'*, ISRAEL HAYOM (Feb. 09, 2022, 12:42 PM), https://www.israelhayom.com/2022/09/02/the-accusations-against-nso-were-part-of-a-disinformation-campaign/
[39]Express Web Desk*, A timeline of the Pegasus snooping scandal,* THE INDIAN EXPRESS (Oct.27, 2021, 1:56 PM), https://indianexpress.com/article/india/a-timeline-of-the-pegasus-snooping-scandal/

basis or truth associated with it whatsoever."[40] The Indian Government labelled it as a disinformation campaign to destabilise the Government.

HOW TO EFFECTIVELY COUNTER INTERNATIONAL DISINFORMATION?

Disinformation is by no means a new concern; it is a global threat to freedom and democracy.To effectively counter international disinformation, one needs to first recognise it, then to identify its origins and to prove intent, and finally to effectively neutralise it.[41]The entire process is challenging. The best political counter-strategy would be to address the root causes of these issues, given that international disinformation primarily aims to exploit already-existing rifts and tensions. Otherwise, there is no magic solution to combating global disinformation.

There are four different approaches to countering information manipulation. Nobody knows which strategy, or a mix of approaches, works best. The approach may be essentially "educational," strengthening people's resistance to false information. They can be "protective," utilising cutting-edge tools to identify and combat disinformation. They have the potential to be "repressive," utilising technology to prevent information tampering. Additionally, they can be "political," seeking to 'tame' disinformation by getting governments to grasp the potentially destabilising effects it may have on international security and trust.

These approaches fall into a variety of categories, depending on whether they are focused on disrupting the flow of disinformation, exposing it, or competing with it.[42] The major examples of a protective approach can be regulating social media platforms, creating norms and standards for online conduct, and restricting material or platforms. The educational method tries to increase media literacy, define criteria of information authenticity, and promote a clear, logical, entertaining, and persuasive counter-narrative in order to refute information manipulation and raise awareness of information manipulation. For example, during the pandemic, there was a lot of disinformation floating about the origin of the virus, such as the corona virus was created by the Chinese Government as a biological weapon,[43] symptoms of the virus, testing methods,

[40]Supra note 37
[41]Supra note 23
[42]Laura Jewett & Andriy Shymonyak, *Good Governance as a good counter-disinformation tool,* NDI (April 29, 2021), https://www.ndi.org/our-stories/good-governance-counter-disinformation-tool
[43] Daniel Romer & Kathleen Hall Jamieson,*Conspiracy theories as barriers to controlling the spread of COVID-19*, 263, 113356 SOCIAL SCIENCE & MEDICINE, 4 (2020),

prevention methods and how vaccination was a ploy to spy on citizens. These approaches countered the spread of such type of disinformation. Verification methods like fact-checking and debunking efforts and labelling systems for "whitelisting" or "blacklisting" sources or platforms are examples of repressive approaches. The political approach often entails business or governmental strategic communications initiatives intended to dispel false myths.

Along with these approaches, the response of international organisations in combating disinformation is particularly pertinent in the framework of international relations, and in this area, the European Union has unmistakably taken the lead. To gain a more comprehensive, regular and reliable picture of Russia's disinformation campaignis the main objective of European Union's East StratCom Task Force, established in 2015 on the initiative of the European Council. The Task Force arguably is the EU's most important initiative in its counter-disinformation efforts, especially also in the countries of the Eastern Partnership.[44]

The most effective countermeasure against disinformation, according to *Stanislav Levchenko* (A Soviet Defector), is to "train yourself to read the front pages of your newspapers and read them every day. Read news magazines."[45]The recommendation made by Levchenko for dealing with misinformation is still relevant today.

CONCLUSION

The problem of disinformation campaigns has drawn much attention since the 2016 U.S. presidential election, not just from the news media but also from governmental, academic, and corporate platforms eager to recognise and comprehend it.It has been observed that disinformation campaigns are expanding internationally and that the number of incidents is increasing. Additionally, state actors are now focusing on voters or ordinary civilians rather than the infrastructures or mechanisms that support democratic events like elections. Disinformation cannot be eradicated with a single remedy. Instead, a variety of legal and regulatory measures must be put in place to counter the escalation and propagation of disinformation.The best remedy would be to encourage public education to build

https://www.sciencedirect.com/science/article/pii/S027795362030575X/pdfft?md5=d835f3e940752bae4f4f39078888b1ed&pid=1-s2.0-S027795362030575X-main.pdf

[44]Supra note 23

[45]Calder Walton, *Spies, Election Meddling, and Disinformation: Past and Present*, 26 (1) Brown Journal of World Affairs 107, 121 (2019), https://bjwa.brown.edu/26-1/spies-election-meddling-and-disinformation-past-and-present/

resilience.However, since international law is insufficient on disinformation and espionage, to be more specific, peacetime espionage, it is important for several nations to work together to develop new international laws, conventions, and regulations. Therefore, it is essential to implement countermeasures in the form of national legislation to safeguard each nation's democracy.