Cold War 2.0 and Espionage

Dr. Devender Kumar[1]

ABSTRACT

The contemporary global politics has been marked by the Cold War 2.0 between the United States (US), China, and Russia, which are competing, rivalling, forming alliances, fighting proxy wars, expanding military might, influencing global politics, and forming blocs. The ideological struggle is missing, but the world is being divided between the US-led West (US, NATO, G7, and European Union) and the Anti-American-Axis comprising of CRINK (China, Russia, Iran, and North Korea). Hence, a few scholars have noted the Cold War dynamics and termed it "Cold War 2.0," involving many aspects, including espionage, which has been a major feature of the Cold War. As the world has changed and competition has been witnessed in technical, defence, etc., sectors for superiority in domains such as land, air, water, outer-space, and cyberspace. Meanwhile, no country has abandoned its espionage agencies while they have enhanced dependence on the domain to extract first-hand information to ensure superiority in the interplay of power politics that has been the major feature of global politics as outlined by the realist thinkers of international relations. This paper seeks to examine the changing nature of espionage in contemporary global politics (Cold War 2.0).

***Keywords**: Cold War 2.0, Espionage, CRINK, United States of America, Russia, and China.*

The Cold War is multi-dimensional and has various aspects like the "absence of direct war", "political instability", "world division into two blocs", "threats, rivalry, alliances, hard power", etc. Similarly, espionage is yet another dimension of the Cold War (Westad, 2018). In Cold War 2.0 various new things have been added to the domain such as technology, apps, fiber-optic cables, software, cyber, hacking, geospatial intelligence (GEOINT), signals intelligence (SIGINT), electronics, open-source (OSINT), "Foreign Instrumentation Signals Intelligence" (FISINT), communications intelligence (COMINT), human intelligence (HMINT), and social networking for monitoring and surveillance. However, the traditional character of espionage and spying has not changed and is utilizing tools of the 21st century. One example is many countries have not renounced or abandoned their intelligence

[1]Assistant Professor, Center of Excellence for Geopolitics and International Studies, REVA University, Bangalore

agencies and are still working to gather inputs on strategic and security issues even though the actors have changed in the Cold War 2.0 i.e. Soviet Union has been replaced by the Russian Federation, while China and the US have become major 'protagonists' (Nalapat, 2023).

The traditional Cold War espionage depended on diplomatic missions, agents, double agents, and underground operations for intelligence and spying (Andrew, 1998). In Cold War 2.0, the traditional mechanisms have transformed and opted segments like technical and electronic to incentivize and help the operations. Espionage and spying agencies are now using digital applications, which have become App-based. The new spy Apps are 'Pegasus', 'Shameware', 'Pinduoduo', 'Tik-Tok', 'Storm-0156', 'Turla', 'TwoDash', and 'Statuezy' etc (Gan & Xiong, 2023). These applications steal data, download harmful files, copy information from phones and computers to monitor activities, and read private messages without authorization and consent from the users (Gan & Xiong, 2023). These Apps sell data to the government like recently Pinduoduo sold to the Chinese government (Gan & Xiong, 2023). These companies also gather data to predict preferences, interests, locations, photos, notifications, calendars, and habits of the users to allow the machines to predict and influence behavior (Gan & Xiong, 2023). Cold War 2.0 can be defined as " a state of intensive competition, political and economic, which yet fall below the threshold of armed conflict between states" (Luard, 1964). It is measured as 2.0 since the world is still in a state of constant conflict and strife while agencies are involved in maintaining perpetual peace without a direct armed conflict between the antagonists but the agencies fighting silently.

UNDERSTANDING ESPIONAGE

Espionage is an old practice of extracting state secrets using technical means and human resources to procure information (Beim, 2019). Few scholars look at it as "information and an organized system for collecting and exploiting it, is both an activity and a product of that activity" (Warner, 2002). It is an 'organization collecting information' while the US Congress defines it as a mechanism to acquire information on "people, places, things, and events —in foreign lands" (Andrew and Wark, 2020). Which are required "by the government for the conduct of its functions" (Andrew and Wark, 2020). John Ferris (1995) argued that "spying came to rival money, sex, and war" (Ferris, 1995, p. 88).

According to intelligence historian Christopher Andrew (2019), it is the 'second oldest profession' (Niruthan, 2019). The references to it are found in '*Rig Veda*' (spies were known as *Spasa*), *Ramayana*, *Mahabharata*, and *Arthashastra*. These inscriptions have outlined how the spies should be used and build strategies through their network. In ancient Indian traditions, espionage had been a major organ of the State to help the king in warfare, administration, policies, strategic planning, and diplomatic strategies (Niruthan, 2019).

Espionage and spying agencies play a significant role in the country's defence and national security since countries maintain secrecy about their real capabilities. Secrecy is about certain 'secrets' —that is information confined to certain 'subjects' —which for the one in intelligence to be extracted and shared like a 'currency' that needs to be 'traded' (Lundborg, 2021, p. 444). Even though countries can make good relations with each other but intelligence agencies are always suspicious of each other's activities related to security and defence— as "there are friendly states but there are no friendly intelligence services" (Bennet, 2000). Many countries are still spying to extract information on domains such as military, finance, politics, etc to develop counter capabilities. Globalization and digitization have added new elements to national security, defense strategies, and espionage for gathering classified information. However, the profession of espionage violates Article 2 of the United Nations (UN) Charter as it calls for the 'respect for sovereign equality of all states and prohibits the use of threat against territorial integrity' (United Nations, 2025). In Cold War 2.0, agencies of the US, Russia, and China violate Article 2 of the UN Charter by undermining the principles of this article to extract information via espionage on other states by compromising their sovereignty and territorial integrity (BBC, 2014).

CHANGES IN ESPIONAGE FROM TRADITIONAL COLD WAR 1.0 TO 2.0

Espionage and spying have continued from Cold War 1.0 to 2.0. The world's most spying agencies emerged during the Cold War; for example, Central Intelligence Agency-CIA (USA- 1947), Inter-Services Intelligence (Pakistan-1948), *Aman* (Israel-1948), *Mossad* (Israel- 1949), *Shin Bet* (Israe-1949), '*Komitet Gosudarstvennoy Bezopasnosti*'-KGB (Soviet Union-1954), The *SAVAK*-Bureau for Intelligence and Security of the State (Iran-1957), RAW (India- 1968), *Mukhabarat* (Iraq-1973), *Teke* later 'Ministry of State and Security'-MSS (China- 1983) emerged during this

period (Clawson, 2020 & The Economic Times, 2024). The traditional way of espionage has not changed and remains a fundamental national security and policy instrument. The relevance of espionage is the same as earlier and dependence on this has increased with substantial changes in character but the tactics remain the same. Nevertheless, the earlier Cold War marked the conventional way of spying via agents, double agents, and diplomatic missions that facilitated the profession of surveillance, monitoring, and infiltration to collect information using different techniques and gadgets (Braat and Jong, 2022).

The operations conducted during Cold War 1.0 were more clandestine unlike 2.0 where most information is available on the internet. The 1.0 saw the phase of ground operations via agents with language expertise unlike the 'Open Source' of the 2.0. The Cold War 1.0 was sophisticated as secrecy was highly maintained due to the lack of information on so many aspects; much of the information came at the risk of human life. This cost is similar to the 'coercive operations' conducted in Cold War 2.0. During Cold War 1.0 diplomatic missions functioned as bases for collecting information while recruits were ideologically driven and had language expertise (Lee and Lederman, 2018). A lot of features of Cold War 1.0 are still visible in Cold War 2.0—as one analyses the 'Manhattan Project' which originated during the Cold War and demonstrated the nuclear capabilities— can be understood as the hypersonic project of Cold War 2.0. Also, during 1.0, the AK47 rifle was the symbol of modern advancement in military technology along with outer-space initiatives; similarly, drone technology, hypersonic projects, and satellites symbolize the hard power conundrum of Cold War 2.0 i.e. Armenia-Azerbaijan War and Russia-Ukraine War. And now many agencies in the US, Russia, China, Türkiye, and Iran are working to develop a 'mini air force of drones' (Malhotra, 2021).

Apart from this, there were many agents during the Cold War 1.0 like Melita Norwood popularly known as Granny Spy, Ursula Kuczynski (Agent Soniya), Klaus Fuchs that worked in nuclear projects such as Tube Alloys, and Manhattan (Szasz, 1992 & Rossiter, 2017 & Macintyre & Valle, 2020). These agents passed on crucial information on nuclear to the Soviet Union for making a nuclear bomb (Rossiter, 2017). And helped in building the espionage network of KGB (Burke, 2013). The Granny Spy was later awarded the 'Order of the Red Banner' by the KGB (Burke, 2013). These agents wanted to establish a balance between the nuclear US and the Soviet Union as they believed that —a sole military power would become a dictatorship

like Germany hence there has to be another nuclear power to balance the equilibrium (Thorndike, 2020 and Rossiter, 2017).

During Cold War 1.0, soft power tools were also utilized by espionage agencies like the CIA for the evacuation of American diplomats during the Iranian Hostage Crisis. The Two CIA agents posed as filmmakers and smuggled six American diplomats out of Iran (Debusmann, 2023). Moreover, after the dissolution of the Soviet Union, the world was aware of the strategic significance of espionage as many countries had already established spying agencies. The US during the Unipolar stage strengthened itself in different regions and undermined many strategic considerations to consolidate its position and influence worldwide— whereas its rival Russia dismantled the KGB (Azrael and Rahr, 1993). American influence in the former Soviet territories and "NATO's eastward expansion" brought Russia into the old espionage era to secure its interests (Mehrotra, 1998 & Shifrinson, 2023).

RUSSIA AND ESPIONAGE

During the Cold War, the KGB regarded the US as the 'main opponent' of the Soviet Union. Even after the dissolution of the Soviet Union, the situation remained the same despite the Russian dissolution of the KGB (Bennet, 2000). Moreover, after the US and NATO expansion in the former Soviet territories, Russia replaced the KGB with 'Foreign Intelligence Service' (SVR) and 'Federal Security Service' (FSB). These agencies consisted of various state agencies for foreign intelligence and defend the Russian Federation from 'external threats' (Government of the Russian Federation, 2025). In the post-Cold War— both SVR and FSB remained anti-west and anti-American and focused more on 'psychotropic means' instead of coercive recruitment (Bennet, 2000). The FSB is a major agency for the national security of Russia and implements policies to defend and protect the state (Government of the Russian Federation, 2025a). Both agencies gather information on security, territorial water, technology, seas, innovations, internal sea water, natural resources, continental shelf, and exclusive economic zones while also being responsible for initiating counterintelligence (Government of the Russian Federation, 2025a).

Currently, Russian agencies see all activities in the former Soviet territories as propaganda of the CIA —to create influence against Moscow and its military capabilities (Bahm and Rice 2018, p. 9). For example, the removal of Viktor Yanukovych a pro-Russian president from Ukraine (Enraged Protesters Storm Ukraine Government Offices, 2014). Such

episodes have strengthened Russian espionage and made it have the same numbers of agents in SVR and FSB as were during the Soviet era (Bahm and Rice, 2018, p. 10).

US AND ESPIONAGE

It was the Cold War 1.0 that outlined the strategic significance of intelligence due to nuclear detonations, strategic alignments, surprises, and deterrence. For a very long US kept its espionage activities secret and did not declassify many materials until recently. The records of American intelligence activities came from the congressional committees, leaks, and when people involved spoke about their engagement and operations in old age, and released sensational facts of their involvement. They outlined that since the Second World War, the US and Western allies had access to "German codes", which they "read" and utilised (Ferris, 1995). The intelligence agency (CIA) of the USA conducted clandestine operations in Iran, Albania, Guatemala, and Cuba. During this era, the US National Security Advisor had more influence on US strategy and diplomacy. The US Department of State released "Foreign Relations of the United States" in 1989, the paper (FRUS) which did not refer to the involvement of CIA in the overthrow of Mohammed Mossadeq (the then prime minister of Iran from 1952-54) such omission raised concerned in the US Congress and academia hence orders were issued to release materials even related to CIA. As a result, thousands of documents were released that elaborated on the role of US intelligence in different countries (Garthoff, 2004).

During Cold War 1.0, the CIA of US intervened in Albania under Operation BGFiend to counter the rise of communist influence in Albania and decided to overthrow the government of Enver Hoxha via several mechanisms of actions (military), propaganda, collection of intelligence to initiate a revolt against his government (Savich, 2023). In Iran, it removed the democratically elected prime minister (Mohammad Mossadeq) since he nationalised the Iranian oil, which was a major blow to the British and American companies. The CIA denied these allegations but "publicly admitted its involvement" in 2013 (Wu and Lanz, 2019). During this era, the CIA destabilized the Iranian government after Mossadeq's nationalization move and turned his image from economic and social reformer. The US bought the Iranian press and convinced the Shah of Iran by telling him that Mossadeq posed a threat to his regime, which instigated trials against Mossadeq, and he spent his life in house arrest (Wu and Lanz, 2019).

The US used espionage as a foreign policy tool to fulfil its national interest and secured the interest of 'United Fruit Company' (UFC) based in the US and removed the democratically elected government of Jacobo Árbenz Guzmán (the then president of Guatemala). The CIA launched "Operation Success" under the administration of John Foster Dulles and Richard Nixon to get rid of Arbenz (Schlesinger and Kinzer, 1999: XII-XIII). The reason for this was, the Guatemalan president had introduced land reforms which offered land to the landless people of Guatemala. Such initiatives threatened the US as they could ignite a wave of social movements in Latin America and posed challenges to UFC, an American company that exploited labor in Guatemala, since land reform could potentially affect their business. The company persuaded the U.S. government to change the government in Guatemala, with the CIA deemed most suitable to fulfil American foreign policy objectives.

The CIA declassified a document in 1995 on "CIA and Guatemala Assassination Proposal 1952-1954," which highlighted that the CIA had "directed covert operations" which aimed to "remove the government of Jacobo Arbenz Guzman from power in Guatemala," and efforts were made for the "disposal of key Arbenz government officials and Guatemalan Communists" (CIA, 1995). The CIA also "drew up a list of individuals for assassination" and held 'trainings' for 'assassinations' in Guatemala, and "conducted intimidation programs against prominent Guatemalan officials" (CIA, 1995). Another incident in which the US pursued its interests through espionage occurred during the 1960s when Dwight D. Eisenhower, then US President, instructed the CIA to "develop a plan for the invasion of Cuba and overthrow of the Castro regime" (US State Department, 2025). For which the CIA maintained a 'Station in Havana' and trained and recruited agents to procure secret communications (NAJFKLF, 2025: 1). It established a mechanism for delivering intelligence reports on Cuba after the breakdown of diplomatic ties.

A Brigade of '2506' was sent to the Bay of Pigs in Cuba on 17 April 1961 and was defeated by Fidel Castro in two days. The Cuban government openly sought ties with the Soviet Union, but despite this defeat, the espionage apparatus continued to operate in Cuba and provided reports about Cuba through US diplomats in Latin America and radio communications (NAJFKLF, 2025: 1). To continue its operations against Cuba, the CIA established a station in Miami and orchestrated 'Operation Mongoose' to remove Fidel Castro from power through military, psychological, intelligence,

propaganda, and political campaigns aimed at assassination (Castro) and undermining the communist regime in Cuba (US State Department, 2025). Nevertheless, both of these expeditions by the US failed, and Cuba enhanced its procurement of Soviet arms, which created dangerous tensions for both superpowers during the Cold War 1.0.

Throughout the 1960s and 1970s, the US also conducted espionage in Vietnam with operations such as 'Op-34 A', and the CIA collaborated with the Saigon government. It kidnapped individuals from North Vietnam to recruit them for spying and undermine the communist-backed country (CIA, 1974). The CIA worked tirelessly to eradicate the influence of Communism worldwide, and after the Soviet Union invaded Afghanistan in 1979 and occupied it, the CIA created the biggest intervention effort to drive the Soviets out of Afghanistan. It created '*Mujaheeds*' and '*Alqaeda*' through Pakistan and created a phenomenon of 'terrorism' (Feroz, 2021). Which later became the foreign policy element of Pakistan to secure monetary support from the US for the services.

ESPIONAGE IN COLD WAR 2.0: USA, RUSSIA, CHINA, ISRAEL AND TAIWAN

In the US during the Cold the number of civilians and military personnel in espionage was equal. Katherine L Herbig has stated that in the post-Cold War era in the US, "67 percent of spies have been civilians and only 33% have been members of the uniformed military" (Herbig, 2008). According to her, in the post-1990s 1990s more individuals in the US, not classically linked with espionage jobs like truck drivers, housewives, boat pilots, translators, have engaged in spying. More people had 'secret-level access' and only a few had 'top secret access' in comparison to Cold War 1.0 period. According to the World Economic Forum, Cold War 2.0 showcases two aspects i.e. cyber espionage and economic espionage between the US, Russia, and China (World Economic Forum, 2023). Global powers such as the US, China, and Russia are competing with each other to mark their influence in global policies and world order (Kumar, 2025a). And giving rise to competition and conflict globally by dividing the world into blocs, alliances and proxies for influence (Kumar, 2024 & Kumar, 2025a).

There are various espionage activities that the countries are undertaking in Cold War 2.0 to counter each other and create influence. The US as a great power has conducted spying activities on many countries. It was also the first to enact 'The Espionage Act' which made the gathering of defense

information illegal and prohibited backing of the enemy for its citizens. The US has given huge importance to spying and created the 'Office of Strategic Service'- the first intelligence agency of the country to recruit people from academia, libraries, journalism, and scholars with language expertise to get documents, reports, records, and enemy publications to obtain information for intelligence analyses (Peiss, 2020, p. 1-4). The US intelligence apparatus consists of various agencies among them are the Defense Intelligence Agency (DIA), the National Security Agency (NSA), and the Central Intelligence Agency (CIA). They are very active overseas in building American perception for securing interests and operations for collecting information on technical, cyber, outer-space, military, and scientific developments worldwide (Office of the Director of National Intelligence, 2025).

The US launched 'Operation Ivy Bells' against the Soviets which lasted decades until Russian intelligence found the cable recording devices at various underwater Soviet channels (Swink, 2018). The US military intelligence stationed numerous devices at the Sea of Okhotsk to record communication and were supported by a "mini nuclear reactor" until the Soviets captured these devices in 1981 (Swink, 2018). With this operation the US wanted to know the real capabilities of the Soviets, not what they portrayed to the world. Nevertheless, the information gathered under this operation helped the US in negotiation for Strategic Arms Limitation Talks (SALT-II) (Swink, 2018).

The US agencies also target Fiber-optic cables to get strategic and communication inputs. These cables work as a "highway of global communication" and play a central role in global telecommunication, internet, data, financial stability, and energy supplies (Sakhuja, 2025 & Bhardwaj, 2024). Globally there is a '1.6 million kilometres' —long network of fiber-optic cables comprising 600 wires worldwide (Sakhuja, 2025). This network is important for the internet and telecommunication while crucial for extracting information, surveillance, international communication, data, and gaining control over network infrastructure. In Cold War 2.0, spy agencies of the UK, US, China, and Russia target the Fiber-optic cables to access data that these cables carry (BBC, 2014 & Firstpost, 2024). Chinese agencies through the ship 'Yi Peng 3' recently voyaged to the Baltic Sea in order to access cables in the channels such as Estlink 2 (between Lithuania and Sweden) and C-Lion1(between Germany and Finland) to extract data (Sakhuja, 2025). On the other hand, with the destruction of the 'Nord Stream' infrastructure, the West fears that Russia might destroy underwater cable communications as

underwater submarine cable infrastructure carries nearly 95 percent of global data (Sakhuja, 2025). Due to this NATO and other countries have decided to strengthen their Fiber-optic cable infrastructure. According to a report US has tapped nearly 200 Fiber-optic cables to obtain data of nearly 600 million citizens every day (BBC, 2014). Taiwan recently also warned about the Chinese espionage on its underwater cable that led to an 'internet blackout' in the country— as a Chinese ship near Matsu Island damaged underwater cables belonging to Taiwan (Change and McCarthy, 2025).

In Cold War 2.0, the CIA spied on partners such as the EU and interrogated its internal computer networks and buildings to get information on its position on military and trade (BBC, 2014). At the same it did surveillance on citizens by going inside the servers of companies such as Google, Facebook, Yahoo, and Microsoft to obtain records of phones— to track communications (The Guardian, 2014 & BBC, 2014). It also intercepted phone calls of diplomatic missions, as per a report it targeted nearly 38 missions and conducted continent-wide surveillance (BBC, 2014). Moreover, US agencies also conducted nearly '61000' hacking operations worldwide and targeted China (BBC, 2014). The major targets of its attack were Chinese businesses, public officials, and universities (BBC, 2014).

China meanwhile conducted 'Operation Salt Typhoon' against the US in 2022 whereby hackers from China conducted cyber espionage against nearly nine US telecommunication companies to intercept calls, messages, data, and information of various high-level economic, political, and government officials (Kapko, 2024 & Vicenza, 2024). This group hacked nearly '100,000 routers' handled by major companies in the US such as Lumen, Verizon, and AT&T (Kumar, 2024 & Kapko, 2024). The Intelligence Committee of the US Senate considered this attack as the "most significant telecom hack in US history" (Kumar, 2024). Through this Chinese agency (MSS) got access to crucial infrastructure and data of millions of American citizens (Vicenza, 2024).

The intelligence agencies in the Cold War 2.0 have silently committed cyber espionage and counterintelligence on each other. The Israeli intelligence apparatus such as *Mossad, Shin Bet, Aman, 'Lekem* (a science liaison office and intelligence-gathering unit), and the Center for Political Research under the Ministry of Foreign Affairs, Israel has added new segments to the domain of espionage in the Cold War 2.0—through their operations. These agencies recently came with 'Pegasus software' and showcased their military, scientific, strategic, and technical superiority in the recent pager attack

against the supporters and affiliates of Hezbollah and Iranian Revolutionary Guards Cooperation (IRGC). The Pegasus software is powerful spyware for surveillance and monitoring of individuals without the consent of the user. It also sent malware to nearly 1400 thousand users to 'extract information, emails, files, messages, etc (Pegg and Cutler, 2021). These agencies also conducted a cyber-physical attack against the Hezbollah affiliates in Lebanon by causing nearly 3000 casualties via a series of blasts in pagers, radios, laptops, cell phones, and car stereos (Bhattacharjee, 2024 & D'Cruze, 2024). Such instruments were used to dodge Israel's detection technologies but Israeli agencies deployed nearly '5000 devices' from suppliers in Hungary and Taiwan to attack Hezbollah meanwhile both supplier countries denied the involvement (Bhattacharjee, 2024 & D'Cruze, 2024).

In Cold War 2.0, China's intelligence agency MSS is creating propaganda and preparing the citizens through campaigns highlighting that the 'foreign spies' are increasing in China and are 'infiltrating' the country (Under Xi Jinping, China's Powerful Spy Agency Drastically Raises its Public Profile, 2024). It has blamed the US and the West for recruiting citizens for espionage in the country. In 2016 the country had already executed various citizens that it believed sold secrets to foreign countries (Under Xi Jinping, China's Powerful Spy Agency Drastically Raises its Public Profile, 2024). Such discourse highlights the worldwide espionage and spying for surveillance, information, monitoring, data, cyber-attacks, hacking, and underwater espionage conducted by intelligence agencies to ensure their countries access to data and information for further ensuring the influence and dominance worldwide.

EFFECTS OF ESPIONAGE IN COLD WAR 1.0 TO 2.0 AND TRUMP

The access to information has provided an edge to countries in the power politics, military strength, and strategic considerations to outsmart each other in soft and hard power assets. The case studies above have highlighted how espionage has impacted different regions worldwide. As plots and propaganda were arranged for the removal of governments not in line with the ideology of the superpower. The 1967 Six-Day War between the Arabs (Egypt, Syria, Lebanon, and Jordan) and Israel was fuelled by the intelligence shared by the Soviets and the US, which passed information that worked as an antagonism for the preventive strike by Israel (Ro'i and Morozov, 2008). This episode started the process of war and peace between Israel and the Arabs, with the Camp-David Accords. The Arab-Israeli issue is still not resolved because

of the intricacies involved following the information of the Soviet and US, and created distrust because of which so many actors from the region and the world got involved in the bilateral issue of Arabs and Israel. And now transformed into a spider-web of intelligence agencies, commanding the everyday life of the residents on both sides.

Another impact of espionage is visible on Iran-US Relations due to the hatred that the US attained after the document release of its involvement, especially its agency CIA, along with the MI6 of Britain, in Mohammad Mossadeq's removal from Iran. The US faced strong criticism, and the puppet regime backed by the US was removed under the Iranian Revolution by the people of Iran in 1979 and paved the way for theocracy in the country (Ansari, 1999). The US encountered the 444-day blockade of its embassy in Tehran and finally got the embassy officials and diplomats released with the help of Hollywood (Explained The storming of the US embassy in Iran, 2024). But the trust deficit has not been filled between Iran and the US till today and both are struggling with distrust over the nuclear aspirations of Iran.

The menace of terrorism also traces its route from the espionage operations of the US in Afghanistan via Pakistan in the 1980s, and the effects of which are still available today. As the US failed to control Afghanistan and, after 20 years of occupation, left the country and Kabul remains a "graveyard of empire" as US, with all its might, could not control Afghanistan and gave control to non-state actors before leaving the country. but the creator of Mujaheeds and terrorist, Pakistan has started using terrorism as a policy to fulfil its interests and secure funding from the global institutions. Its intelligence agency, ISI, protects terrorists, i.e., provided refuge to Osama Bin Laden for nearly 10 years until he was assassinated by the US (US State Department, 2011). ISI shares information and uses terrorism as a policy to receive funding from the US and also from international organizations such as the IMF (IMF Loan to Pakistan Why the Latest Tranche Was Passed, 2025). The US, despite facing the 9/11 Terror Attack, has backed such funding at the crucial juncture. So, states Pakistan and the US, with their agencies such as ISI and CIA, are using espionage to fulfil their interest at the cost of morals, ethics, and humanity.

From ideological groups to multilateral groups the espionage has found its space as countries have not given up alliances and groupings. The continuity of the North Atlantic Treaty Organization (NATO) has created tussles and

wars in the world, as nations still compete with each other. For example, the Ukraine-Russia War since 2022 has highlighted the bloc politics and the role of espionage. Despite changes of administrations in the US from Barack Obama, Joe Biden, and Trump, the competence for forming groupings has evolved, and NATO has retained a special place in the security considerations of countries, as the rise of its membership has created a national security threat to countries, especially Russia. But Moscow has used espionage clandestinely to sustain its power and advantage, and the Russian agencies attacked the crucial data centres for information to know the real capacity and capabilities by weaponizing the information for warfare. In the Russia-Ukraine War, the "Unit 26165", largely known as the "Fancy Bear" a military intelligence of the Russian Army has targeted IT sector, emails, internet connectivity, defence, cameras, transport etc of Ukraine, US, Romania, Poland, Netherlands, Greece, France, Czech Republic and Bulgaria (Western Countries Reveal Major Russian Cyber-Espionage Campaign, 2025).

The US under Donald Trump had understood the information and he himself kept many documents related to government despite leaving office, and became the first president in the US to be charged under the 'Espionage Act', as he kept 31 documents related to the national security of the US (Trump Faces 31 Charges Under the Espionage Act the Law Regulating Government Secrets, 2023). The world has changed but the war of agencies continues, and even leaders have realised the importance of information, but access to crucial information in the information era also creates problems for the leaders, as Donald Trump was accused of spying for Russia by "sharing crucial information with the Russian counterpart" (Trump Revealed Highly Classified Information to Russian Foreign Minister and Ambassador, 2017).

CONCLUSION

In contemporary times, the mechanism for procuring information has drastically changed as the world witnesses Cold War 2.0 between the US-led West and the anti-American axis. Both sides have avoided direct confrontation but have engaged through espionage agencies and proxies to balance power and gain the upper hand in this strategic rivalry. Meanwhile, reliance on technology and electronics for intelligence gathering has increased. Espionage and spying exhibit continuity from the traditional Cold War 1.0 to 2.0, with few tactical changes in surveillance and monitoring. However, Cold War 2.0 is heavily characterized by cyber espionage, economic espionage, cyber-physical espionage, data exploitation, artificial intelligence, software

tampering, hacking, fiber-optic cables, the internet, open-source platforms, and communication devices. States are competing technologically to outsmart one another, and new lethal conventional setups have emerged due to the weaponization of communication devices, such as pagers, mobile phones, and telephones, as seen during the Pager attack by Israel against Hezbollah and the IRGC.

The growing dependence on technical devices in the digital era, including systems like facial recognition, fingerprint systems, electronic chips, artificial intelligence, and drone technologies, has further redefined the espionage domain. Major businesses worldwide have developed new technologies that are not only lethal in the espionage realm but also pose dangers to humanity, such as neurochips (brain-computer interfaces) that can control human actions. The rise of technology has not deterred conventional setups from obtaining information, as data related to military operations is not available in the public domain. There is a significant data crunch in the sector because governments conceal their true capabilities. Consequently, countries continue to rely on traditional espionage methods through direct recruitment by agencies to gather intelligence from individuals, including ordinary civilians, through honey traps, social networks, favours, brainwashing, and social gatherings. In many cases, individuals are unwittingly recruited and share crucial details regarding locations, places, files, data, reports, and sensitive information with adversaries.

REFERENCES

Andrew, C. (1998). Intelligence and International Relations in the Early Cold War. *Review of International Studies*. 24 (3), 321-330.

Andrew, C., & Wark (2020). *Secret Intelligence A Reader*. London: Taylor and Francis.

Ansari, A. (1999). *Iranian Revolution of 1979*. Retrieved from https//web.stanford.edu/class/e297c/war_peace/middleeast/hiranianrev.html.

Azrael, R J., & Rahr A G. (1993). *The Formation and Development of the Russian KGB, 1991-1994*. Retrieved from https//www.rand.org/content/dam/rand/pubs/monograph_reports/2007/MR355.pdf.

Bahm, Karl & Rice Dakota, S. (2018). *The Nature of Russian and Soviet Intelligence Agencies*. Retrieved from https//minds.wisconsin.edu/bitstream/handle/1793/79280/The%20Nature%20of%20Russian%20and%20Soviet%20Intelligence%20Agencies.pdf?sequence=9&isAllowed=y.

Bennett, G. (2000). *The SVR Russia's Intelligence Service. Conflict Studies Research Center*. Retrieved from https//irp.fas.org/world/russia/svr/c103-gb.html.

Beim, J. (2019). *Enforcing a Prohibition on International Espionage 182*. Retrieved from https//cjil.uchicago.edu/print-archive/enforcing-prohibition-international-espionage.

Bhardwaj, A. (2024). *Sub Sea Fibre Optic Cable Network Safety and Security*. Retrieved from https//bharatshakti.in/sub-sea-fibre-optic-cable-network-safety-and-security/.

Bhattacharjee, S. (2024). *Pager Attack in Lebanon Can Nations be Allowed to Cause Violence and Death Using Digital Techniques?*. Retrieved from https//indianexpress.com/article/opinion/columns/pager-attack-in-lebanon-violence-digital-techniques-9576343/.

Braat, E., & Jong, Ben de. (2022) Between a Rock and a Hard Place The Precarious State of a Double Agent during the Cold War. *International Journal of Intelligence and Counter Intelligence*. 36(1), 7-108.

British Broadcasting Corporation (BBC). (2014). *Edward Snowden Leaks that Exposed US Spy Programme*. Retrieved from https//www.bbc.com/news/world-us-canada-23123964 accessed 4 January 2024.

Burke, D. (2013). *The Spy Who Came in from the Co-Op Melita Norwood and the Ending of Cold War Espionage History of British Intelligence*. New York: Boydell Press.

Central Intelligence Agency (CIA). (1974). *Vietnam War, the Role of CIA*. Retrieved from http//cia.gov/readingroom/docs/CIA-RDP90-01208R000100190023-8.pdf.

Central Intelligence Agency (CIA). (1995). *CIA and Guatemala Assassination Proposals 1952-1954*. Retrieved from https//www.cia.gov/readingroom/docs/DOC_0000135796.pdf.

Chang, W., & McCarthy, C Simone. (2025). *A Cut Undersea Internet Cable is Making Taiwan Worried about 'Gray Zone' Tactics from Beijing*. Retrieved from https//edition.cnn.com/2025/01/09/china/undersea-cable-taiwan-intl-hnk/index.html#~text=In%202023%2C%20Taiwanese%20authorities%20blamed,saying%20they%20were%20deliberate%20acts.

Clawson, P. (2020). *How to Build a New Iraq After Saddam.* Washington DC: The Washington Institute for Near East Policy.

Danish Military Tracking Chinese Vessel after Undersea Cable Damage Why Are These Fiber-optics so Important. (2024, November 20). *Firstpost.* Retrieved from https//www.firstpost.com/world/danish-military-tracking-chinese-vessel-after-undersea-cable-damage-why-are-these-fiber-optics-so-important-13837069.html.

Dheeraj, P. (2024). No BFFs in Geopolitics. Spying on Friends is a Symbol of Power. *The Times of India*. Retrieved from https//timesofindia.indiatimes.com/blogs/voices/no-bffs-in-geopolitics-spying-on-friends-is-a-symbol-of-power/.

D'Cruze, D. (2024). Hezbollah's Pager Explosions Could Smartphones Face Similar Explosive Cyber Attacks?. *The Bussiness Today*. Retrieved from https//www.businesstoday.in/technology/news/story/hezbollahs-pager-explosions-could-smartphones-face-similar-explosive-cyber-attacks-446397-2024-09-18.

Debusmann, B. (2023). CIA Identifies Second Officer Involved in 'Argo' Mission CIA Identifies Second Officer Involved in 'Argo' Mission. *British Broadcasting Channel*. Retrieved from BBC.

Enraged Protesters Storm Ukraine Government Offices. (2014, January 23). *CBS News*. Retrieved from https://www.cbsnews.com/news/ukraine-protesters-storm-government-offices-as-protests-against-president-viktor-yanukovych-intensify/.

Explained The storming of the US embassy in Iran. (1979, November 04). *The Indian Express*. Retrieved from https//indianexpress.com/article/explained/explained-global/1979-storming-us-embassy-iran-9652964/.

Ferris, John. (1995). Coming in from the Cold War The Historiography of American Intelligence. 1945–1990, *Diplomatic History*, 19(1), 87-115.

Feroz, Emran. (2021). What the CIA Did (and Didn't Do) in Soviet-Occupied Afghanistan. Retrieved from https//newlinesmag.com/argument/what-the-cia-did-and-didnt-do-in-soviet-occupied-afghanistan/.

Gan, Nectar & Juliana, X. (2023, April 3). I've Never Seen Anything Like This' One Of China's Most Popular Apps Has The Ability To Spy On Its Users, Say Experts", *CNN Business*, Retrieved from https//edition.cnn.com/2023/04/02/tech/china-pinduoduo-malware-cybersecurity-analysis-intl-hnk/index.html

Garthoff, Raymond L. (2004). Foreign Intelligence and the Historiography of the Cold War. *Journal of Cold War Studies*. 6 (2), 21-56.

Gan, Nectar & Juliana, X. (2023, April 3). I've Never Seen Anything Like This' One Of China's Most Popular Apps Has The Ability To Spy On Its Users, Say Experts", *CNN Business*, Retrieved from https//edition.cnn.com/2023/04/02/tech/china-pinduoduo-malware-cybersecurity-analysis-intl-hnk/index.html

Government of Russian Federation. (2025). *Foreign Intelligence Service*. Retrieved from http//archive.government.ru/eng/power/112/.

Government of Russian Federation. (2025a). *Federal Security Service of the Russian Federation*, Retrieved from http//government.ru/en/department/113/.

Herbig, K.L. (2008). Changes in Espionage by Americans 1947-2007. Retrieved from https//sgp.fas.org/library/changes.pdf.

IMF Loan to Pakistan Why the Latest Tranche Was Passed. (2025, May 12). *The Indian Express*. Retrieved from https//indianexpress.com/article/explained/explained-economics/imf-loan-to-pakistan-why-passed-9995800/.

Kapko, M. (2024). *White House Says 9th Telecom Company Hit in Salt Typhoon Spree*. Retrieved from https//www.cybersecuritydive.com/news/salt-typhoon-telecom-attacks-lax-security/736233/.

Kumar, A. (2024). *What is Salt Typhoon, the China-linked cyberattack shaking US telecom?*, Retrieved from https//www.business-standard.com/world-news/china-salt-typhoon-cyberattack-us-telecom-network-hack-124121700683_1.html.

Kumar, D. (2025a). *Chiefs of Defence of NATO Members Meet*, Retrieved from https://www.geopolitics.reva.edu.in/chiefs-of-defence-of-nato-members-meet.html.

Kumar, D. (2025). *Iran's 'Comprehensive Strategic Partnership Agreement With Russia*. retrieved from https://www.geopolitics.reva.edu.in/Irans-comprehensive-strategic-partnership-agreement-with-russia.html.

Lee, M., & Lederman, J. (2018). Spies Posing as Diplomats have a Long History. Retrieved from https//apnews.com/article/985f444da7dd42c5b3b8abc422a977b8.

Luard, E. (1964). *The Cold War, a Re-appraisal*. London: Thames & Hudson.

Lundborg, T. (2021). Secrecy and Subjectivity Double Agents and the Dark Underside of the International System. *International Political Sociology*. 15 (4), 443–459.

Macintyre, Ben & Valle, Efrén, del. (2020). *Agent Sonya Lover, Mother, Soldier, Spy*. New York: Viking.

Malhotra, R. (2021). *Artificial Intelligence and the Future Power*. New Delhi: Rupa Publication.

Mehrotra, O N. (1998). *NATO Eastward Expansion and Russian Security*. Retrieved from https//ciaotest.cc.columbia.edu/olj/sa/sa_98meo02.html.

Microsoft, Facebook, Google and Yahoo release US Surveillance Requests. (2014, February 3). *The Guardian*. Retrieved from https://www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests.

Nalapat, M. D. (2023). *Cold War 2.0*, Haryana: Penguin Random House India.

National Archive John F. Kennedy Library Foundation (NAJFKLF). (2025). *CIA Operations Against Cuba Prior to the Assassination of President John F. Kennedy on 23 November 1963*. Retrieved from https//www.archives.gov/files/research/jfk/releases/104-10096-10145.pdf.

Niruthan, N. (2019). The Indic Roots of Espionage Lessons for International Security. *The SAIS Review of International Affairs*. Retrieved from https//saisreview.sais.jhu.edu/the-indic-roots-of-espionage-lessons-for-international-security/.

Office of the Director of National Intelligence. (2025). The U.S. Intelligence Community is Composed of the Following 18 Organizations. Retrieved from https://www.dni.gov/index.php/what-we-do/members-of-the-ic#content.

Peiss, K. (2020). *Information Hunters When Librarians, Soldiers, and Spies Banded Together in World War II Europe,* London: Oxford University Press.

Pegg, D., & Cutler, S. (2021). What is Pegasus Spyware and How Does It Hack Phones. *The Guardian.* Retrieved from https//www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones.

Polyakova, A. (2019). *Five years after the Revolution of Dignity Ukraine's progress and Russia's malign activities*. Retrieved from https//www.brookings.edu/articles/five-years-after-the-revolution-of-dignity-ukraines-progress-russias-malign-activities/.

Ro'i, Y., & Morozov, B. (2008), *The Soviet Union and the June 1967 Six-Day War*, California: Stanford University Press.

Rossiter, M. (2017). *The Spy Who Changed the World Klaus Fuchs, Physicist and Soviet Double Agent*, New York: Skyhorse.

Sakhuja, V. (2025a). *China, Russia, Iran and North Korea (CRINK) block gains foothold in Central America.* Retrieved from https//kalingainternational.com/Vijay-Sakhuja147.html.

Sakhuja, V. (2025). *Underwater Fiber Optic Cable Security and Gray Zone Operations*.

Retrieved from https//www.defstrat.com/magazine_articles/underwater-fiber-optic-cable-security-and-gray-zone-operations/.

Savich, C. K. (2023). *The CIA and a Greater Albania The Origins of the US Role in the Balkans*. Retrieved from http//global-politics.eu/cia-greater-albania-origins-role-balkans/.

Schlesinger, S., & Kinzer, S. (1999). Bitter Fruit: The story of the American coup in Guatemala, revised and expanded. Harvard University Press.

Shifrinson, J. (2023). *What Washington Got Wrong About NATO Expansion in the 1990s*. Retrieved from https//carnegieendowment.org/posts/2023/10/what-washington-got-wrong-about-nato-expansion-in-the-1990s?lang=en.

Swink, S. (2018). *The wiretapping that changed the Cold War*. Retrieved from https//thedefensepost.com/2018/08/16/book-wiretapping-changed-cold-war/.

Szasz, M.F. (1992). *British Scientists and the Manhattan Project*, New York: Palgrave Macmillan.

Trump Revealed Highly Classified Information to Russian Foreign Minister and Ambassador. (2017, May 15). *The Washington Post.* Retrieved from https//www.washingtonpost.com/world/national-security/trump-revealed-highly-classified-information-to-russian-foreign-minister-and ambassador/2017/05/15/530c172a-3960-11e7-9e48-c4f199710b69_story.html.

Trump Faces 31 Charges Under the Espionage Act the Law Regulating Government Secrets Explained. (2023, June 17). *ABC* News. Retrieved from https//abcnews.go.com/Politics/trump-faces-31-charges-espionage-act-law-regulating/story?id=100129183.

Thorndike, Greenspan, N. (2020). *Atomic Spy The Dar Lives of Klaus Fuchs*. New York: Viking.

Under Xi Jinping, China's Powerful Spy Agency Drastically Raises its Public Profile. (2024, April 22).*The Economic Times.* Retrieved from https//economictimes.indiatimes.com/news/defence/under-xi-jinping-chinas-powerful-spy-agency-drastically-raises-its-public.

United States Government. (2025). *Central Intelligence Agency*. Retrieved from https//www.usa.gov/agencies/central-intelligence-agency.

United Nations. (2025). *Charter of the United Nations*. Retrieved from https//legal.un.org/repertory/art2.shtml.

US State Department. (2025). *The Bay of Pigs Invasion and its Aftermath, April 1961–October 1962*, Retrieved from https//history.state.gov/milestones/1961-1968/bay-of-pigs.

US State Department. (2011). *Justice Has Been Done*. Retrieved from https//www.defense.gov/Multimedia/Photos/igphoto/2002009777/.

Vicenza, A. J. (2024). *US Adds 9th Telcom To List of Companies Hacked by Chinese-Backed Salt Typhoon Cyberespionage*. Retrieved from https//www.reuters.com/technology/cybersecurity/us-adds-9th-telcom-list-companies-hacked-by-chinese-backed-salt-typhoon-2024-12-27/.

Warner, M. (2002). *Wanted A Definition of "Intelligence" Understanding Our Craft*, *Studies in Intelligence*. Retrieved from https//www.cia.gov/resources/csi/static/Wanted-Definition-of-Intel.pdf.

Westad, O.A. (2018). *The Cold War A World History*, New York: Penguin.

Western Countries Reveal Major Russian Cyber-Espionage Campaign. (2025, May 21). *Politico News* Report. Retrieved from https//www.politico.eu/article/russian-cyber-espionage-campaign-ukraine-fancy-bear-hackers/.

World Economic Forum. (2023). *US Warns of Huge Cyber-Espionage Campaign, and Other Cybersecurity News to Know this Month*. Retrieved from https//www.weforum.org/stories/2023/06/us-china-cyber-espionage-campaign-cybersecurity-news/.

Wu, L., & Lanz, M. (2019). *How The CIA Overthrew Iran's Democracy In 4 Days*. Retrieved from https//www.npr.org/2019/01/31/690363402/how-the-cia-overthrew-irans-democracy-in-four-days.