Global Journal of human-social science: F
Political Science
Volume 23 Issue 1 Version 1.0 Year 2023
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-460X & Print ISSN: 0975-587X

Intelligence Challenges in Contemporary Geopolitical Discourse

By Zoran Ivanov

Introduction- Intelligence is critical in the state's decision-making process and national security strategy. Nevertheless, the contemporary regional and geopolitical complexity implies countless challenges to intelligence. Carl von Clausewitz said: "In the fast-moving complex environment, the target has changed by the time you adopt a plan." (Clausewitz, 1832) Today this sentence has more relevance. We live in an interregnum period where the domination of liberal democracy is challenged from the inside out through the war in Ukraine, a decline of trust in democracy, inequality, division of societies, decay of economic development, rising inflation, and geopolitical competition between great powers. Today we live in a hazy space where there is no clear line between war and peace. Further, we started our twenty-first century with a dangerous relationship between political leaders and their intelligence advisors, in which they are distorting intelligence information to justify their political decisions.

GJHSS-F Classification: DDC Code: 320.12 LCC Code: JC319

Strictly as per the compliance and regulations of:

Intelligence Challenges in Contemporary Geopolitical Discourse

Zoran Ivanov

I. Introduction

Intelligence is critical in the state's decision-making process and national security strategy. Nevertheless, the contemporary regional and geopolitical complexity implies countless challenges to intelligence. Carl von Clausewitz said: "In the fast-moving complex environment, the target has changed by the time you adopt a plan." (Clausewitz, 1832) Today this sentence has more relevance. We live in an interregnum period where the domination of liberal democracy is challenged from the inside out through the war in Ukraine, a decline of trust in democracy, inequality, division of societies, decay of economic development, rising inflation, and geopolitical competition between great powers. Today we live in a hazy space where there is no clear line between war and peace. Further, we started our twenty-first century with a dangerous relationship between political leaders and their intelligence advisors, in which they are distorting intelligence information to justify their political decisions. Both Prime Minister Tony Blair and President George W. Bush came under unprecedented public scrutiny in both Britain and the United States and were widely charged with purposefully distorting intelligence information to justify their decision to make war on Iraq in April 2003 (Scott and Jackson, 2004). The need for a better understanding of both the nature of the intelligence process and its importance to national and international security policy has never been more apparent.

Meanwhile, the so-called traditional threats such as terrorism, corruption, and organized crime are using every opportunity to gain their ground. Nevertheless, intelligence is not immune to myriad challenges created while the great powers learn how to share power. The interaction of the states in the geopolitical competition is changing the environment's conditions, which directly challenges intelligence. Hence, this article will examine the correlation between dynamic changes in the geopolitical environment and intelligence. The article will develop a model to recognize geopolitical environment variables. Interrelationships between variables produce changes in the geopolitical environment that directly affect intelligence. In recent years, where "nations have wrestled with economic, social, and geopolitical upheaval in recent years, the future of liberal democracy has come into question. In countries across the globe, democratic norms and civil liberties have deteriorated, while populists have enjoyed surprising success at the ballot box. Newly democratic nations have struggled, while more-established, once self-assured democracies have stumbled, exposing long-simmering weaknesses in their social fabrics and institutional designs." (Wike and Fetterolf, 2021).

The understanding ramification of geopolitical environment changes on intelligence in current conditions draws apparent necessity to consider the nature of intelligence study in correlations to geopolitics. It also examines the development of intelligence as an area of academic study and assesses its emerging need to widen the perspective of the study. It aims to explore implied critical challenges to intelligence from manifested geopolitical environment changes. We consider this analysis critical because each challenge of the geopolitical environment utterly influences the politicians to create politics according to their perceptions, thus directly influencing the intelligence.

II. The Study of Intelligence

The study of intelligence is more prominent than ever because intelligence has been playing a critical role in shaping political discourse from both sides of the world, West and East, resulting in tectonic changes in international politics, state relationships, and great power competition. Hence, understanding the intelligence role in not only in domestic affairs but more importantly in context of contemporary geopolitical environment is essential.

In their excellent work, Len Scot and Peter Jackson, "The Study of Intelligence in Theory and Practice," they recognized three different concepts that generally fit in the work done by many observers of intelligence studies. The first approach, favored among international historians in particular but also characteristic of theoretical approaches that seek to explain the relationship between organizational structure and policy making, conceives of the study of intelligence primarily as a means of acquiring new information in order to explain specific decisions made by policymakers in both peace and war. To this side belong authors O'Halpin (2005) and Perlman (2018), that gave a historical analysis of the role of British and American intelligence organizations. Second, strive to establish general models that can explain success and failure in the intelligence process. Additionally, authors such as

Author: *e-mail: zivanov@etu.edu.tr*

Hedley (2005), Fitzgerald and Lebow (2006), and Eiran (2016), by examining the intelligence failures and process of reforms, significantly contribute to the intelligence study. Decisive importance is attributed by adherents of this approach to structural and cognitive obstacles to the effective use of intelligence in the policy process. The aim is to identify and analyze the personal, political, and institutional biases that characterize intelligence organizations and affect their performance in the decision-making process. A third approach focuses instead on the political function of intelligence as a means of state control. Recently released archival material has enabled scholars to study the role of state security services in political and social life in the USSR and Eastern bloc states after 1945 (Scott and Jackson, 2004). Nevertheless, their research produced two critical observations that coincide with contemporary geopolitical shambles. First, the best writing about intelligence incorporates all three approaches differently. Second, at the heart of these divergences is disagreement concerning the extent to which political assumptions and culture shape the intelligence process at all levels. This is power, and power is shaping the environment in pursuing dominance in geopolitical competition (Scott and Jackson, 2004).

III. Intelligence Concept of Geopolitics

Common elements can be recognized in the work of other authors, philosophers, and experts scrutinizing geopolitics. Starting with the nineteen-century, geographer and philosopher Halford Mackinder described geopolitics as the use of politics in controlling territories, where certain geographical positions are more strategic than others, for resources, historical and socio-political reasons. In Walberg's work on geopolitics, he uses the concept of the "Great Game" to better describe the broader rivalry between nations and economic systems with the rise of imperialism and the pursuit of world power (Walberg, 2011). These are sufficient studies to see that geopolitics has common elements. Those are states, leadership, territory, and power. The same elements that intelligence is collecting information and accumulating knowledge about.

Hence, the intelligence concept of geopolitics must be holistic because these are various state elements under certain circumstances that must be examined to gain knowledge and understanding of the state's capabilities, limitations, behavior, and intentions. Intelligence is a state's function to collect information and gain knowledge for the state to achieve desired strategic goals. Michael Herman observes in his work that intelligence is an 'enabling' facility, helping the world of action to exercise national power and influence (Herman, 1996). Henceforth, intelligence and geopolitics are directly linked. In Flint's work on geopolitics, he examines that the state should be able to define the global geopolitical agenda (Flint, 2006). Intelligence has critical, if not central role and has capacity to integrate other resources and assets when gaining knowledge about other adversaries, states, non-state actors and global conditions to define the global geopolitical agendas. Following Gramsci, we would expect that the most powerful country would try to set a political agenda that the rest of the world would, more or less, follow (Gramsci, 1971). The intelligence function is one of the critical state's tool in establishing a connection with foreign leaders, building coalitions with countries, and/or setting conditions to provoke actions by target countries or individuals. The geopolitical environment can be broken down into variables to understand the interconnection between intelligence and geopolitics further. These variables are actors, conditions, relationships, and influences. We consider this concept of scrutinizing the geopolitical environment critical because it will open a different approach to understanding the dependent correlation between intelligence and geopolitics. Christopher Andrew's excellent work shows the critical role of intelligence in two significant perspectives.

First, intelligence played a critical role in the ideological competition between East and West, hunting and influencing the unlike-minded from both sides of the world and limiting space for its adversary. Second, the close relationship between political leaders and intelligence. The close mutual relationship has influenced the political discourse (Andrew, 2004).

In general, geopolitics is about the rivalry between nations, which means a struggle for power and power is shaping the environment in pursuing dominance in geopolitical competition. Therefore, our variables will enable what kind of events are produced. These events can be planned or the result of the second-order effect of mutual interaction. Planned events are manifests taken by states to change or influence elements of the geopolitical environment in their desired direction. Second-order manifests are the product of changes in any of the elements. Both are critical because they directly represent the changes in the geopolitical environment where some states will perceive them as a threat to national interests and benefit for some. The purpose of these events is to create conditions for actors to exercise their power. In such a complex milieu, intelligence has a critical role in identifying the actors' intentions and capability, recognizing changes in the conditions, understanding the relationships between actors and conditions, and creating specific influences to exercise their power. Any change in the geopolitical environment represents challenges to intelligence because these manifests can represent a limitation in collecting information or gaining knowledge. Also, some changes are very dynamic or require additional assets or technology. Therefore, it is

critical to understand the ramification of geopolitical shambles on intelligence.

IV. Scope and Focus

General understanding of intelligence study and geopolitics tend to keep their research into respective areas. Events such as September 11, the war on terror in Iraq and Afghanistan and their subsequent forces withdrawal, the color revolutions in Egypt, Syria, Libya, and Ukraine in 2014, and the reinvasion of Ukraine in 2022 desired much to understand about the relationship between intelligence and geopolitics. These events undoubtedly serve as an example of a direct connection between intelligence and geopolitical environment changes. Further, these events are directly connected to intelligence in two ways—Eighter as a challenge to face and adjust or as a generator of events. The events mentioned above are all researched and studied in detail by many observers from different perspectives. Thus, we will assume these manifests are the product of direct or indirect interconnection of intelligence and geopolitics. Consequently, they produce changes in the geopolitical environment that influence intelligence. The focus is to recognize what are the implied critical challenges to intelligence.

The observation recognized three central challenges to intelligence. First, technology implied structural changes in intelligence organization and process. States have used technology to protect national interests or use by malevolent states, nonstate, or individuals to harm our societies. The common denominator for these two types understands how, when, and in what context of the environment they will utilize technology.

Second is the geostrategic discourse by the rise of China and Russia. The intelligence focus in the past two decades was on the war on terror and counterterrorism. Therefore, intelligence must shift from a global war on terrorism to major rival or rouge states. Consequently, we must observe the intelligence shift from counterterrorism to great power competition and how to protect friendly information and capabilities from rival and rouge states.

Third, balancing the liberal democracy virtues in managing the former intelligence officer's activities related to security and intelligence. How to control the intelligence officer who leaves the service is one of the most understudied challenges to intelligence services. This issue can severely impact the trust among alliances and the credibility of the intelligence services. Thus, directly endangering the mutual state relationships, which might trigger international conflict or disputes. The manifest of the Raven project in the United Arab Emirates has much to learn from.

In the end, we will use NATO Intelligence Enterprise as an example of how the geostrategic environment's perception reflects on international intelligence cooperation that can create political disputes within the Alliance. Why observes NATO? NATO is one of the actors in the geopolitical environment that can shape and produce changes. It has built its intelligence structure that can be subject to further analysis because intelligence cooperation inside the Alliance is influenced by the state's perception of the geopolitical environment, thus representing the threat to maintaining the trust inside the Alliance.

V. Technological Challenges

The article disagrees with the authors who are perceiving technologies as the most critical challenges where the other challenges are related or products of them. Therefore, the article will assume that technology is a tool. States have used technology to protect national interests or use by malevolent states, non-states, or individuals to harm our societies. The common denominator for these two types understands how, when, and in what context of the environment they will utilize technology. Hence, we cannot consider technology the most crucial challenge to intelligence service because the human domain through developing knowledge is and will remain critical in developing and using technology.

"Technological advancements are heightening global instability in ways that extend far beyond the battlefield. New technologies enable increasingly powerful non-state actors to affect the answer. Power is shifting away from democratic states, and they must prepare for, and defend against, the potentially seismic consequences" (Cronin, 2020). Meanwhile, a recent re-emergence of major-power competition, particularly between the United States, Russia, and China, is likely to keep the focus of military planners on large-scale, high-end weapons systems rather than on building capabilities and strategies to defend against more pervasive and less obvious emerging threats. Major powers will be defined not only by the size of their military forces but also by how nimble and adaptive those forces are. Ukraine's ability to defeat or slow the advances of Russian forces has illustrated the priority of adaptive learning and the superior use of intelligence, surveillance, and reconnaissance to support kinetic operations (Korb, 2022).

Hence, the article recognizes two critical ways. First, identifying and understanding the threats to domestic security from cognitive warfare used by individuals, domestic and foreign organizations, and rouge states that promote anti-democratic agendas, extremism, tribalism, and division of societies. Second, understanding the strategy of how rouge states and malicious actors will employ technologies. Crafting scenarios of how the technologies may be deployed

and combined in innovative ways by rogue actors is crucial. (Cronin, 2020)

1. Cognitive warfare

Technological advances have created a new warfare domain besides the current military five domains of warfare land, sea, air, space, and cyber domain. The cognitive domain is a product of the present complexity of warfighting, geopolitical competition and contemporary technological connectivity. Communication interconnectivity and mass use of social media made the cognitive domain part of each of the current five domains and an emergent (more than the sum of the parts) separate sixth domain. Heartly and Jobson, in their book "Cognitive Superiority" are arguing that technology has created new forms of cognition, the unending exponential increase in the sum of human knowledge, new communities of knowledge, and information access. "It is intertwined with competing world views, grand strategies and metanarratives of power, diplomacy, commerce, education, science, metascience, and the necessity for lifelong learning. It molds trust, social membership, meaning, identity, and power." (Heartly and Jobson, 2021) Thus, forcing intelligence services to abruptly use technology to counter cognitive warfare to protect the state's decision-making system and to increase society's resilience to foreign influence and division. Since cognitive warfare integrates cyber, information, psychological, and social media capabilities to achieve its ends, the intelligence service must expend its expertise beyond traditional intelligence collection. The primary goal of cognitive warfare is to sow doubt, introduce conflicting narratives, polarize opinion and society, radicalize groups, and motivate them to act that can disrupt or fragmentize society's cohesiveness. In such a security milieu, besides traditional threats, the intelligence services will face emerging domestic violence, civil unrest, distrust in government institutions, homegrown terrorism, domestic sectarian violence, and rapid division of society.

Even the most advanced democracy in the world, the USA, is not immune to this cognitive warfare. It turns out to be its biggest weakness. The best example of one of the primary goals of cognitive warfare, sowing doubt, is the American Presidential election in 2021. Some may argue that this event is not connected to cognitive warfare, yet it falls into this category because whoever was the idea's generator (domestic or foreign forces) has reached the goal. Part of the American public perceives that the Presidential election was stolen. Millions of Americans believe that at the dawn of Biden's precedence, the election was stolen, and thousands turned to violence to "stop the steal." (Alter, 2021) Later, President Joe Biden, in his inaugural speech in January 2021, confirmed that American society is divided, and the division forces are real (Biden, 2021). In such an ambiance, the intelligence services quickly can become collateral damage from the battle between two major political parties. Thus, directly weakening the credibility and effectiveness of the intelligence services in protecting national interests. Soon after, the Jan 6 Committee in Capitol Hill started an examination of intelligence failure. Many experts and journalists in US security consider the Jan 6 riots in Capitol Hill as the most significant domestic security failure since 9/11 (Dilanian, 2022). Is it? It is arguable because too many reports from various US domestic intelligence agencies prior to Jan 6 produce actionable intelligence (Dahl, 2022).

The intelligence services are always between the hammer, political masters and the protection of the state's national interests, the anvil. Not always the politicians want to hear that something is wrong neither that they must take responsibility for some issues, or they must give money to intelligence services for something they rarely can win political benefit. In such ambiance the intelligence services must develop their expertise in how the technologies may be deployed, and combined, in innovative ways by rogue actors and especially rival states.

2. Strategy to employ technology

The technological revolution is open, and it will never stop, which means that new products will be invented or modified. Though, the product itself does not have relevance until it's been used for some purpose. Hence, the critical question remains how the technology will be used, where, when, and for what purpose. Military History teaches us that weapons and technological innovation impact war or conflict, but they are not decisive. A recent example is the latest war in Iraq and Afghanistan. The US started to use UAVs – unmanned area vehicles, and drones for targeting Al-Qaeda'sAl-Qaeda's high-value targets for a few years to successfully end the war on terrorism. The technological advancement, combined with ground military force, impacted tactical operations. (Bumiller, 2011) Nevertheless, the UAVs did not bring a strategic sustainable solution, an end to war on terrorism. Soon after, the US troops withdrew from Afghanistan in August 2021.

The strategy to employ technological advancement is vital because they represent a more significant challenge to intelligence services than just discovering their existence by rogue actors. The intelligence services should focus on understanding the adversary'sadversary's strategy of technology employment; if they do not, they can easily overestimate or underestimate of adversary'sadversary's power projection.

The strategy is defined as the application of means to achieve ends. Therefore, technological advancement means states can use it to attain political

outcomes. Depending on what kind of outcome they want, the reliance on technological advancement may or may not be sufficient. The overestimation or underestimation of the adversary'sadversary's power projection can come from limited intelligence analysis to the adversary'sadversary's technological capabilities. If the intelligence analysis does not consider in what context of the security environment technological advancement may or may not be used, it does not represent the adversary'sadversary's real power.

Further, the intelligence services must understand how the adversary will deploy the technology and how much time they need. Providing this knowledge will create decision points where decision-makers can decide when, where, and what preemptive actions can be used to achieve the desired political outcome. To illustrate, the US had technological and military superiority during the Vietnam War. Yet, they misjudged the North Vietnamese will to resist. During the Iraq and Afghanistan wars, the US'sUS's technological and military superiority was obvious. Yet, the US did not win the war on terrorism. Therefore, technology can shape war or conflict, but it is not decisive.

Here it is essential to observe the second-order effect on technological innovation because the grown insurgencies, terrorist organizations, and malicious individuals have used technological innovation to adapt to deadly use to counter the US and its allies at home. Due to the US and allies'allies' domination in Afghanistan and Iraq wars, the insurgents and terrorists used technological innovation to create more deadly weapons. Therefore, the Improvised Explosive Device – IED became the deadliest weapon against the westerners in the theater. Further, the terrorist organizations took the initiative and started the diffusion of anti-American rhetoric to inspire sympathizers globally. The case of the Boston Marathon bombings illustrates how technological innovation can become disruptive to the security and safety of our societies. In 2013, the Tsarnaev brothers, ethnic Chechens, followed Inspire'sInspire's magazine step-by-step instructions, turning two pressure cookers into IEDs using explosive powder from ordinary fireworks and detonators made from Christmas lights (Meek, 2014).

There are two critical learning points from these examples that impact intelligence. Frist, if it is engaged in political friction between the politicians and political parties, it most likely will be accused of intelligence failure, which was the case of a controversial report on Iraqi weapons of mass destruction – WMD in 2005 (Kessler, 2019). Second, their action, in this case producing a report that Saddam Hussein had WMD that initiated the Iraqi invasion, produced a reaction that directly changed the security environment. The insurgents and terrorists modified technological innovation into deadly weapons. ISIS and Hezbollah have used armed drones in their operations (Sims, 2018). Accessible lethal technologies empower a much broader range of actors to challenge major powers, where they are losing the capacity to counter them (Cronin, 2020 p.159). Therefore, intelligence services must adapt fast and acquire new skills to identify and counter these threats.

VI. Geostrategic Discourse by Rise of China and Russia

In the following years growing specter of great power competition and conflict will dominate the global security environment (DNI, 2022). Therefore, intelligence must shift from a global war on terrorism to major rival or rouge states. There are two significant challenges for intelligence services. First, shift from counterterrorism to great power competition. Second, how can friendly information and capabilities be protected from rival and rouge states?

The shift to great power competition will require structural changes in collecting critical information because it is a different fight involving major combat forces and operations. Counterterrorism, for the most part, is reactive and allows one to choose a time, operations, and space with limited force.

These substantial differences in collection management and especially analysis can represent weakness for some intelligence services. Even the US intelligence system needs time to adjust to great power competition because counterterrorism intelligence is not focused evaluating combat power of the states, how and in what formations they will bring technological advances to bear, and how they will coordinate their weapons system in multi-dimension warfare. To illustrate, counterterrorism collects information to understand and prevent the next terrorist's attack. The intelligence developed models, network, and systems to learn about terrorist modus operandi and networks. In ongoing great power competition, the intelligence needs to change the taxonomy and mindset to understand how the rival state's "way of war" (Roberts, 2019). Meanwhile, they still need to focus on traditional threats because they will use security gaps or any weakness created by great power competition. The balance of military power among the United States, China, and Russia is an essential focus for all analysts seeking to anticipate future threats to the world order. The United States and its allies are facing sustaining severe threats. China's assertiveness in the South China Sea, Russia's intervention into the Syrian civil war and especially the invasion in Ukraine. They must not lose sight of these many threats or fail to plan for them and innovate to deter or meet them. But just as market disruptors can blindside dominant companies, militaries can be blindsided by non-state actors. In the past decades, Russia and China developed their military capability that can substantially challenge the western countries. China

has developed capabilities in area and space denial that can limit access and communication systems of the western allies. Russia holds the capability to use hypersonic missiles that can have critical impact on western allies' defense (Henley 2022). These capabilities can be used as power of influence to build potential new alliances against west.

Henceforth, intelligence analysis will play critical role in developing knowledge of how and when rouge states can apply their strategic weapons. Further, in the contemporary interconnected global environment, intelligence services will be challenging to protect critical friendly information.

Present-day great power competition, how to protect friendly information and capabilities remains essential. In the past few decades Russia and China could observe the US, NATO, and European countries fighting in two Desert wars, Bosnia, Iraq, Afghanistan, and other regional conflicts. Yet, there are two critical outcomes. First, during these military and security engagements western allies has exposed many of their military capabilities to name a few, the way of war, formations, maneuver, doctrine and tactics, and ability to adjust. Some may argue that these military and security engagements can have a second-order deterrence effect to keep balance of power. Yet, the rival states can gain significant knowledge about western warfare to counter or deny future activities.

Second, achieved successes in demonstrating a commitment to protect democracy and human rights without direct confrontation with Russia and China, yet can lead to fault assumption that global domination will deter from great power conflict.

The ongoing Russian reinvasion of Ukraine falls into this category. It is a result of a series of past eighter disregarded or underestimated events that Russia was engaged in. Article recognizes several critical events. First, NATO Summit in Bucharest in May 2008 where Georgia and Ukraine were allowed to be considered as future candidates. President Putin was invited to the Summit, where he directly opposed it. Second, soon after in August 2008, Russia initiated war with Georgia. Third, Russian Gazprom has halted gas export to Ukraine. Fourth, in November 2011, Russia vetoed the UN resolution on Syria (NATO Association of Canada, 2022). Fifth, in Feb 2014, Russia invaded Ukraine. Consequently, Russia reinvaded Ukraine in Feb 2022, engaging in massive military operations that still many Ukrainians are losing their lives. The analysis of these critical events of global affairs and international relations is subject for itself. Yet, the article recognizes the considerable amount of intelligence that could be used to prevent Russia from going rogue, save lives, and prevent future great power's direct conflict. From intelligence perspective there are two possible assumptions. First, intelligence services have failed to gain knowledge of Russia's global affairs intentions. It can be assumed that this is very unlikely because major intelligence services built up their intelligence skills during the Cold War period. Therefore, they are expected to continue monitoring rival state's intentions. Second, the politicization of intelligence. Tailoring intelligence reports for political purposes has been gaining roots in democratic societies. The biggest challenge for intelligence services is speaking the truth to power.

Nevertheless, politicians do not like to hear the truth because, usually, their focus is on winning the next elections. The conflict between politics and intelligence has a long history. In their book "Intelligence in an insecure world," Peter Gill and Mark Phythian scrutinize the politization of intelligence. Nevertheless, current trends of political polarization and tribalism in democratic societies represent the biggest challenge to balancing liberal democracy virtues.

VII. Balancing the Liberal Democracy Virtues

How to control the intelligence officer who leaves the service is one of the most understudied challenges to intelligence services. This issue can severely impact the state's relationship, trust among alliances, and credibility of the intelligence services. There are two crucial aspects to analyzing this issue. First, intelligence officers can become whistleblowers to expose the government's intentions in execution of their security policies. Second, they can become contractors for non-state or other state intelligence and security agencies that can damage state's mutual relationship.

The aspect of whistleblowers we will not examine because it is the most scrutinize topic since Snowden and Assange's cases appear in media. The focus will be on, directly influencing the trust between states and intelligence services. We consider the trust critical to resiliency from the rival state going, rogue.

At present intelligence service is still struggling to control the intelligence officers who will leave the service. To illustrate, we will look at "Project Raven," the American group of former intelligence officers from the National Security Agency – NSA has joined the United Arab Emirates in hacking operations against UAE's rival states and individuals. The project started in 2014 to assist the UAE's National Electronic Security Agency by US private cybersecurity contractor company "CyberPoint" to build cyber counterterrorism capability in fighting ISIS. Though, the project ended up hacking operations to spy on UAE's rival states, including American citizens and human rights activists (Bing, and Schectman, 2019). After exposing the case by a former member of this hacking group, Lori Stroud, many legal and procedural weaknesses of intelligence contractors emerged. Further, the Raven project eventually started to target foreign adversaries, such as Iran, Qatar, and

Turkey, and individuals who criticized the monarchy (Bing, and Schectman, 2019). It can be assumed that if these types of operations try to meddle in political processes in favor of the UAE, it can directly spark regional tension between states. Hence, having such an intelligence tool can become a risky asset and encourage states to go rogue in pursuing their interests.

This case was expose to the media due to the ethical and patriotic motives of the former NSA intelligence officer who was part of this project. Nevertheless, critical question remains what if there is no one with patriotic or ethical motives to report? Today our societies are experiencing losing trust in democracy, political polarization, tribalism, inequalities, rising inflation, where the middle and lower class very soon will be struggling for necessities. In such a complex milieu, it can be assumed that many intelligence officers or private intelligence companies do not agree with the government's decisions for various reasons, such as different political polarization perceptions or economic reasons.

Hence, the intelligence agencies need to maintain a relationship with their former officers and offer them roles where they can still be valuable resources for the intelligence and state rather, than make them targetrival or rouge states.

VIII. Challenges to nato Intelligence Enterprise

The North Atlantic Treaty Organization: NATO remains a critical actor in the current shambles ofglobal geopolitics and security. Therefore, the article recognized that maintaining trust among its members is a critical challenge that NATO and especially NATO intelligence enterprises, need to face.

Today, NATO is facing the fragility of democratic politics in a world tapestry of ideologies and communications technologies. The origin of the threat to trust, we can look into several characteristics of our societies, such as: the growth of nationalist parties with anti-democratic agendas; changes in Western political cultures that privilege extremism and tribalism; the adverse consequences of "globalization," including breakdowns in supply chains, the spread of pandemics, the disruption of markets, and the growth of an elite transnational class; and political coercion and military pressure from authoritarian regimes against democratic ones, within and outside of Europe (Korb, 2022) In the such complex milieu of domestic and international challenges will dominate self-preservation and national interests rather than NATO alliance's common interest. Hence, there are two critical ways that the trust among NATO members is challenged. First, sharing intelligence can severely damage the trust among NATO members because of the gradation of intelligence sharing. Second, different perceptions of interpretation of the implementation of counterterrorism policies.

Enforcing the gradation of intelligence sharing is directly damaging trust between member states. The chief of NATO Intelligence Enterprise, Arndt Freytag von Loringhoven recognized synchronizing efforts, reducing duplication, and fully optimizing resources ((Loringhoven, 2017). Thus, synchronizing efforts in sharing intelligence making the hardest task to NATO intelligence enterprise. Intelligence culture is an essential element that hinders the effort to increase intelligence sharing. This culture differs between civilian and military intelligence services within NATO. The military, focusing on planning and operations, is typically more inclined to the "need to share". Some civilian intelligence organizations adopt a much morerestrictive approach to their information, emphasizing the "need to know". Such deeply ingrained traditions are hard to overcome. Additionally, the gradation of intelligence sharing between members is a deeply rooted culture. To illustrate, even among allies, the United States employs gradations of intelligence sharing, having the most profound relationship with Britain, followed closely by Australia and Canada. Intelligence relations with other NATO allies are close, albeit less so than with the "Commonwealth cousins." (Lowenthal, 2009, p.37)

Counterterrorism appears to be where the differences in the threat perceptions of the allied countries are most evident. Although NATO creates counterterrorism action plans by continuing to define terrorism as "one of the principal threats against the Alliance." The differing viewpoints of the allies towards terrorist organization causes serious flaws within the Alliance in practice.

The most evident sign of these differences known to have created severe debates within NATO and tensionamong the allies. Tensions erupted in 2019 when the development related to NATO defense plans partially leaked to the public. The media reports stated the negotiations on the Graduated Response Plans (GRP) came to a deadlock due to the different viewpoints of the allies toward PYD/YPG (Aliriza, 2019). The problem could only be solved through intensive discussions at the level of the leaders.

Such tensions, which undoubtedly caused harm to NATO's image and its deterrence, are expected to remain as long as NATO members continue to have different perspectives regarding the issue. Nevertheless, it is considered that along with the Russian occupation of Ukraine, the skeptical approach toward NATO's presents and deterrence seems to have vanished with no likelihood to come on the agenda for a long time. NATO's deterrence is the most crucial weapon of the allies to protect themselves. To maintain its deterrence, NATO must create an "impression of unity" before its adversaries and rivals without leaving any room for doubt.

In this respect, it would be appropriate to develop, under the leadership of the NATO Intelligence Enterprise, an approach that considers the national sensitivities of the allies to avoid future disagreements that may come up in counterterrorism issues. Otherwise, the cost to be paid may be as high as to affect thewhole Alliance.

IX. Conclusion

The article has examined the challenges that emerged from current geopolitical shambles in intelligence. We recognized that technological, geopolitical discourse, balancing liberal democracy virtues, and challenges to NATO intelligence enterprise directly correlate to intelligence efficacy and efficiency. The intelligence function is the best tool states can use to define the political, economic, and security prioritiesin contemporary precarious geopolitical conflict. Nevertheless, if the state allows these challenges to overwhelm the importance of intelligence in the decision-making process, then at some point, they find themselves in a cloud full of unknowns. Current literature examines challenges and perspectives that are structural and organizational to intelligence. Hence, this article addresses perspectives that can seriously impair intelligence function's effectiveness and efficacy, thus making the state even more vulnerable to multi-dimensional threats.

Technological advancements are inevitable, and they make progress and development for our societies. Therefore, the article looks at technological advancement as a tool. Hence, we recognized two critical perspectives on how these tools can challenge intelligence. First, identifying and understanding the threatsto domestic security from cognitive warfare used by individuals, domestic and foreign organizations, and rouge states that promote anti-democratic agendas, extremism, tribalism, and division of societies. Second, it is crucial to understand how the rival states and rouge actors can employ technologies. The article finds that intelligence can easily fall into a trap set by cognitive warfare since the rival or rouge state can directly influence our societies and political processes without direct confrontation.

Further, geopolitical discourse brings two significant challenges for intelligence services. First, shift from counterterrorism to great power competition. Second, how can friendly information and capabilities be protected from rival and rouge states? The shift to great power competition will require structural changesin collecting information because this is a different fight involving major combat forces and operations. Counterterrorism, in the most part, is reactive and allows one to choose the time, operations, and space with limited force. These substantial differences in collection management and especially analysis can represent weakness for many intelligence services.

Additionally, the most significant vulnerability to intelligence services is balancing liberal democracy virtues and controlling the intelligence officer who leaves the service. This issue can severely impact the state's relationship, trust among alliances, and credibility of the intelligence services. Free intelligence officers have unique skills that can be used against our governments, thus damaging our societies. The results are emerging two crucial actions. To establish a control mechanism for using intelligence skills globally. Second, we cannot rely on the intelligence officers' luck, patriotism, and morale. They are ordinary people with beliefs and emotions that can be subject to influence by sophisticated communication technologies from rival or rouge states and non-state actors.

Finally, the article examines the challenges to NATO intelligence enterprise because it is the critical military Alliance that can play an essential rule in handling rival and rouge state's actions. Maintaining trust among member states is crucial. The results present that intelligence can have both negative and positive impacts. Sharing intelligence has always been a more significant challenge because of different political perceptions, intelligence capacities, and national priorities between NATO members. Further, counter-terrorism appears to be where the differences in the threat perceptions of the allied countries are most evident. The differing viewpoints of the allies towards terrorist organizations cause severe flaws within the Alliance, thus minimizing the trust among the members.

Scrutinizing intelligence challenges is a dynamic process. Intelligence can initiate changes in the geopolitical environment. Hence, the geopolitical environment influences intelligence by creating conditions, actions, and relationships between its actors outside intelligence reach. Therefore, having a continuous process of scrutinizing intelligence with a holistic approach will enrich our knowledge and assist professionals and politicians in adjusting and improving intelligence function.

Literature

1. Alter, C. (2021) How President Biden Handles a Divided America Will Define His Legacy, Time, Available at: https://time.com/5932022/joe-biden-divided-america/ (accessed on 01 Jun 2022)
2. Bumiller, E. (2011) Soldier, Thinker, Hunter, Spy: Drawing a Bead on Al Qaeda, New York Time, Available at: https://www.nytimes.com/2011/09/04/world/04vickers.html (Accessed on 03 Jun 2022)
3. Cronin, E. (2020). Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists. Oxford University Press

4. Dahl, E. (2022). January 6th Intelligence Failure Timeline, Just Security. Available at: https://www.justsecurity.org/81806/january-6-intelligence-and-warning-timeline/ (accessed on 02 Jun 2022)
5. Dilanian, K. (2022). Jan. 6 committee examines FBI, DHS documents for answers on intel failure, NBC NEWS, Available at: https://www.nbcnews.com/politics/national-security/january-6-committee-examines-internal-fbidhs-documents-seeking-answers-rcna11076 (accessed 02 Jun 2022)
6. O'Halpin, E. (2005). The Liddell diaries and British intelligence history. Intelligence and National Security, 20(4), 670-686.
7. Perlman, S. M. (2018). US intelligence and communist plots in postwar France. Intelligence and National Security, 33(3), 376-390.
8. Meek, J. (2014) FBI Feared Boston Bombers 'Received Training' And Aid From Terror Group, Docs Say. ABC NEWS, Available at: https://abcnews.go.com/Blotter/fbi-feared-boston-bombers-received-training-aid-terror/story?id=23819429 (accessed on 01 Jun 2022)
9. John Hollister Hedley (2005) Learning from Intelligence Failures, International Journal of Intelligence and CounterIntelligence, 18:3, 435-450,
10. Michael Fitzgerald & Richard Ned Lebow (2006) Iraq: The Mother of all intelligence failures, Intelligence and National Security, 21:5, 884-909.
11. Ehud Eiran (2016) The Three Tensions of Investigating Intelligence Failures, Intelligence and National Security, 31:4, 598-618.
12. Michael Herman (2003) Counter-Terrorism, Information Technology and Intelligence Change, Intelligence and National Security, 18:4, 40-58.
13. Abraham Wagner (2007) Intelligence for Counter-Terrorism: Technology and Methods, Journal of Policing, Intelligence and Counter Terrorism, 2:2, 48-61.
14. Michael Warner (2012) Reflections on Technology and Intelligence Systems, Intelligence and National Security, 27:1, 133-153.
15. Wike, R and Fetterolf, J (2021) Global Public Opinion in an Era of Democratic Anxiety, Pew Research Center, Available at: https://www.pewresearch.org/global/2021/12/07/global-public-opinion-in-an-era-of- democratic-anxiety/ (accessed on 20 May 2022)
16. Korb, L. (2022). How NATO can meet the challenges of the 21st century. National Interest. Available at: (https://nationalinterest.org/feature/how-nato-can-meet-challenges-twenty-first-century-202852) (accessed on 20 May 2022)
17. Heartly, D and Jobson, K. (2021) Cognitive Superiority: Information of Power, Springer
18. Biden, Joe, (2021) Inaugural Address by President Joe Biden, The White House, Available at: https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/01/20/inaugural-address-by-president-joseph-r-biden-jr/ (accessed on 01 June 2022)
19. Kessler, G. (2019) The Iraq War and WMDs: An intelligence failure or White House spin? The Washington Post, Available at: https://www.washingtonpost.com/politics/2019/03/22/iraq-war-wmds-an-intelligence-failure-or-white-house-spin/ (accessed on 05 Jun 2022)
20. Sims, A. (2018) The Rising Drone Threat from Terrorists. Georgetown Journal of International Affairs, Vol. 19 (Fall 2018), pp. 97-107 Available at: https://www.jstor.org/stable/pdf/26567532.pdf?refreqid=excelsior%3A82f475b44c0615a725697853fd410a16&ab_segments=&origin=&acceptTC=1 (accessed on 01 Jun 2022)
21. Roberts, P. (2019) The Future Conflict Operating Environment Out to 2030, RUSI Occasional Paper, Available at: https://rusi.org/explore-our-research/publications/occasional-papers/future-conflict-operating-environment-out-2030 (accessed on 05 April 2022)
22. Henley, J. (2022) What are hypersonic missiles and why is Russia using them? The Guardian, Available at: https://www.theguardian.com/world/2022/mar/20/what-are-hypersonic-missiles-and-why-is-russia-using-them-kinzhal-ukraine (accessed on 14 Maj 2022)
23. Korb, L. (2022) How NATO Can Meet the Challenges of the Twenty-First Century, National Interest, Available at: https://nationalinterest.org/feature/how-nato-can-meet-challenges-twenty-first-century- 202852 (accessed on 01 Jun 2022)
24. Lowenthal, M. (2009) From Intelligence: From Secrecy to Policy, CQ Press, USA
25. Aliriza, Bulent. (2019) Erdogan and Trump at the NATO Summit: Another Display of Solidarity, CSIS, Available at: https://www.csis.org/analysis/erdogan-and-trump-nato-summit-another-display-solidarity (accessed on 02 Jun 2022)
26. NATO Association of Canada (2022) A timeline of Russian aggression. Available at: https://natoassociation.ca/a-timeline-of-russian-aggression/ (accessed on 10 Jun 2022)
27. Bing, C. and Schectman, J. (2019) Project Raven, Reuters, Available at: