CENTRE FOR SECURITY STUDIES | **ISSUE BRIEF**

August 2022

An Assessment of the 2019 National Intelligence Strategy

Raghav Dua

Edited by: Aryan Gupta

About the author

Raghav Dua is a postgraduate student at the Jindal School of International Affairs and was Research Assistant at the Centre for Security Studies, JSIA.

About the Centre for Security Studies

The Centre for Security Studies (CSS) was established in 2020 as the Jindal School of International Affairs' first student-run research centre under the aegis of Prof Dr Pankaj K Jha. Researchers at CSS – through in-depth analysis briefs and events, reports, policy briefs and print publications – explore both regional and thematic topics in the broader field of international security studies. The concept of international security has been expanded to reflect not merely the study of state security, but also include topics like ethnic, sectarian and religious conflict; civil wars and state failure; cyber and space warfare; resource related security issues; the proliferation of weapons of mass destruction; defence economics and also the role of ethics or morality in the formulation of security policies. The complexity of these matters is what the Centre for Security Studies attempts to unfold. Please refer to www.cssjsia.com for further details, and follow the Centre's social media platforms for critical news and research updates:

www.linkedin.com/company/jindal-centre-for-security-studies/

www.instagram.com/css_jsia/

https://twitter.com/Css_Jsia

Important disclaimer

IB2208005

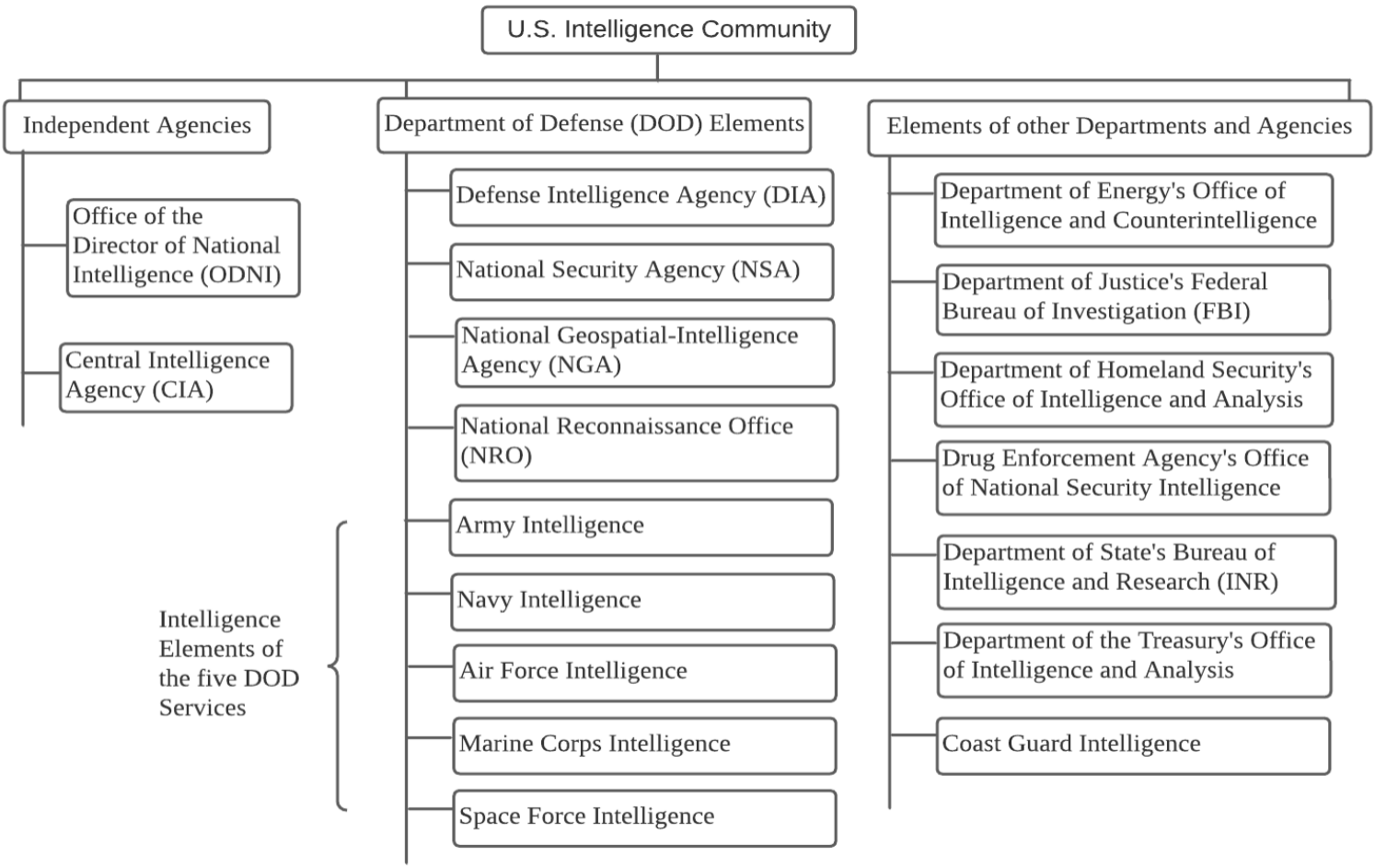
The National Intelligence Strategy (NIS) of the United States of America, prepared by the Office of the Director of National Intelligence (ODNI), is the principal guiding strategy for the Intelligence Community (IC) which provides it "with strategic direction from the Director of National Intelligence" (ODNI, 2019a, 2019b). It is a fully unclassified document that was first released in October 2005 by the then DNI John Negroponte (ODNI, 2019b).

Since then, the ODNI has regularly released the NIS every four to five years. The fourth, and the latest, iteration of NIS was released in January 2019 by the then DNI Daniel R. Coats. The next strategy is expected to be released in 2023. The NIS supports the IC mission, which is to "provide timely, insightful, objective, and relevant intelligence and support to inform national security decisions and to protect our [United States] Nation and its interests" (ODNI, 2019a, p. 2-3). The NIS outlines IC's mission and enterprise objectives and provides IC's assessment of the strategic environment.

The NIS 2019 has **seven components**: (1) the *Strategic Environment*; (2) the *Mission Objectives*; (3) the *Enterprise Objectives*; (4) *Factors affecting IC performance*; (5) *Organisation of the IC* section; (6) *Implementing the NIS;* and (7) *Principles of Professional Ethics for the Intelligence Community*. The aim of this paper is to summarize the points in the NIS and to provide an analysis of the key takeaways. Therefore, rest of this paper has been organised into five sections: (a) Intelligence Community: A Short Introduction (covers 4, 5, 6, 7 sections); (b) Mission Objectives; (c) Enterprise Objectives; and (d) Strategic Environment, for effective summarization and ease of understanding. Emphasis of this paper is on elaborating upon the three foundational mission objectives of the IC (Strategic, Anticipatory, and Current Operations Intelligence) which are critical support functions that it provides to the policy community.

INTELLIGENCE COMMUNITY: A SHORT INTRODUCTION

NIS 2019 describes the Intelligence Community (IC) as an "integrated enterprise" consisting of 18 agencies and organisations, which are also called **IC Elements** that "conduct a variety of intelligence activities and work together to promote national security" (ODNI, 2019a).



Source: ODNI Website

It should be noted that Space Force Intelligence, the 18th, and the newest member of the IC, was established in June 2022. NIS 2019 only mentions 17 IC elements.

These IC elements conduct a wide range of intelligence activities. For example: CIA is responsible for HUMINT collection, covert action, and foreign counterintelligence. It also conducts all-source analysis along with INR. Similarly, NSA is responsible for SIGINT. All these agencies, apart from CIA and ODNI, respond to their department heads.

The ODNI is the staff of the Director of National Intelligence (DNI), who is the leader of IC. The DNI has many responsibilities, such as: (a) acting as the principal intelligence advisor to the President, National and Homeland Security Councils; (b) ensuring proper coordination of intelligence activities; (c) providing strategic direction to the IC; (d) managing the National Intelligence Program (NIP) and contributing to the Military Intelligence Program (they together make-up the IC budget); (e) leading IC integration; and (f) enabling mission execution. The DNI also sets the strategic priorities for the IC through the NIS (ODNI, 2019a).

U.S. National Security policy depends on Intelligence. The raison d'être of the IC, also reflected in its *Mission*, is to "provide the best available information to the nation's senior civilian and military decision-makers" (George, 2020, p. 52). In this regard, DNI ensures that timely and objective intelligence is provided to its customers which include policymakers/ decision-makers such as the President of the United States (POTUS), National Security Council (NSC) principals, Congress, Heads of Departments and agencies of the Executive, Military, Diplomats, etc (ODNI, 2019a).

Further, for ensuring effective integration and coordination, heads of certain IC elements serve in other roles under the DNI. These roles include: **(a) Functional Managers:** coordinator of a specific intelligence discipline, for example: Director of CIA and NSA are functional managers for HUMINT and SIGINT respectively (ODNI, 2020); **(b) National Intelligence Managers (NIM):** principal intelligence advisors on all aspects of a certain area of concern, for example: Director of the National Counterterrorism Centre is the NIM for counterterrorism. As of 2019, there exist 17 NIMs (Lowenthal, 2020); **(c) Program Managers:** heads of IC elements responsible for mission execution, budget coordination and informing resource allocation of their organisation; **(d) Enterprise Managers:** responsible for aligning capabilities and business functions to enable

IC mission. Apart from these roles, it is vital that IC elements incorporate the NIS in their strategic plans for better synchronisation of IC activities.

Now, it is interesting to note that NIS 2019 also highlights the factors that affect IC performance. They are divided into: (a) *Accomplishments* regarding integration, workforce, partnerships, transparency and innovation; factors we will discuss in the enterprise Objectives section; (b) *Risks and challenges:* It identifies four kinds of risk- Strategic (affecting basic mission capabilities), institutional (affecting mission execution and business practices), Fiscal (unpredictable events affecting use of funds), and Technological. While these are not discussed in detail in this paper, they nevertheless remain important for IC management. In addition to this, NIS also features a *Principles of Professional Ethics for the Intelligence Community* section. It includes seven ethical principles that intelligence professionals must observe in their day-to-day activities: (1) Mission; (2) Truth; (3) Lawfulness; (4) Integrity; (5) Stewardship; (6) Excellence; (7) Diversity.

MISSION OBJECTIVES

The *Mission Objectives* outlined in NIS 2019 describe the "activities and outcomes necessary for the IC" to fulfil its mission of providing intelligence and support to inform national security decisions (ODNI, 2019a). These Mission Objectives "support customer success" (ODNI, 2014). NIS 2019 divides these **seven** mission objectives into **two categories**: **Foundational** and **Topical**.

Foundational Mission Objectives

The three **Foundational Mission objectives** are the most fundamental missions or basic support functions of the IC (ODNI, 2019a). Any permanent intelligence organisation must fulfil these support functions. They are not confined to any threat, topic or region. These are: *Strategic Intelligence*, *Anticipatory Intelligence* and *Current Operations Intelligence*. George (2020) refers to them as "critical support to the decision-maker" (p. 102).

(1) Strategic Intelligence: NIS defines *Strategic Intelligence* as "the process and product of developing the context, knowledge, and understanding of the strategic environment, required to support U.S. national security policy and planning decisions." Its foremost objective is to create in-depth knowledge of the strategic international environment. It includes the assessment of important trends and factors that U.S. national security decision-makers must be apprised of. It further involves the identification and assessment of "capabilities, activities, and intentions of state and non-state entities" to understand risk and opportunities for the U.S (ODNI, 2019a).

Strategic Intelligence is long-term analysis of issues of enduring interest opposed to basic (facts) and current (daily) intelligence. Although, both are important as they are included as static and new information respectively, in a much larger body of knowledge. George (2020) notes that virtually all intelligence analysis is strategic, as it focusses on achieving goals by available means. What distinguishes strategic intelligence is its focus on long-term analysis. The analysts working on Strategic Intelligence must become Subject-Matter Experts (SMEs) on countries like Iran, China, Pakistan, Russia, and others; and on transnational issues like terrorism, proliferation of Weapon of Mass Destruction (WMDs), drug and human trafficking, etc (George, 2020, pp. 111-115).

Strategic Intelligence is both a process and a product. The process of producing strategic intelligence is highly analyst centric. George (2020) emphasises that it is vital for policymakers to understand the strategic international environment in which the U.S. operates, in order to make informed national security decisions. He further adds that policymakers usually have rigid preconceptions about the strategic environment. It is therefore essential that analysts are objective in their assessments (understand the world as it is) in order to improve policymakers' understanding and apprise them of any changes in the strategic environment, enabling wise and informed decision-making. Sherman Kent argued in 1949 that this goal of "providing knowledge" and "raising the level of policy debate" is arguably the most crucial job of an analyst.

The National Intelligence Council (NIC) is "IC's premier strategic intelligence producer" (George, 2020, p. 121). Its strategic intelligence analysis represents the IC's collective judgement. It is

responsible for preparing the **National Intelligence Estimates (NIEs)**, which are strategic assessment reports, on behalf of the DNI. It comprises of a dozen National Intelligence Officers (NIOs) responsible for various regional and functional topics. They oversee the creation of NIEs and other assessments for senior policymakers. Another product of the NIC is the unclassified *Global Trends* strategic assessment report which discusses key trends that will shape the world over next 5-20 years. (George, 2020)

For the IC to produce effective strategic intelligence, NIS directs it to: (a) develop data acquisition and evaluation capabilities enabling better understanding of the strategic environment; (b) develop expertise in areas of enduring security interests for identifying risk and opportunities; (c) build academia and industry-wide partnerships for research collaboration; (d) develop advanced analytics and tradecraft for providing better assessment and context (ODNI, 2019a).

(2) Anticipatory Intelligence: NIS defines **Anticipatory Intelligence** as the process of "collecting and analysing information to identify new, emerging trends, changing conditions, and undervalued developments, which challenge long-standing assumptions and encourage new perspectives, as well as identify new opportunities and warn of threats to US interests." It mainly focuses on: **(a) foresight**: identification of new and emerging issues; **(b) forecasting:** development of potential scenarios; and **(c) warning:** alerting on potential issues of concern (ODNI, 2019a). It explores, both, the possibility of the occurrence of an event and the potential effects it might have on U.S. national security. "Predvideniye" or foresight, a similar concept to anticipatory intelligence, is part of the Russian military doctrine (Bowen, 2020). Anticipatory intelligence, like strategic intelligence, is highly analyst centric. A good analyst-policymaker relationship is vital for its success. Alerting does not guarantee that the policymaker will act on the intelligence assessment; convincing the policymaker is altogether a different challenge.

Bowen (2020) notes, that compared to Strategic Intelligence, which focused on questions of enduring interests, anticipatory intelligence focuses upon "on- and over-the-horizon problems whose nature, implications, or intersection with other security challenges is unclear." Anticipatory intelligence is comparatively a new term in the field of intelligence. It gained prominence in 2010s

owing to the rising diversity, complexity, and interconnectedness of threats and challenges to U.S. national security (Bowen, 2020). The DNI abandoned the "old-style warning", which focused on military threats, in order to adopt the concept of anticipatory intelligence which embraced the evolving nature of security challenges (George, 2020, p. 167 and Bowen, 2020). While many scholars think of it as merely a new jargon, it additionally highlights the need for advance analytical skills and mechanisms to maximise decision advantage. In order to produce effective anticipatory intelligence, NIS directs the IC to: (a) develop quantitative methods and data analysis techniques to anticipate new trends; (b) promote the understanding and use of anticipatory intelligence in routine IC efforts and work towards eliminating any barriers in this regard; (c) develop integrated alert capability for providing timely warning; and (d) work on areas of limited customer focus (ODNI, 2019a).

Good strategic and anticipatory intelligence are vital to avoid "strategic surprise", which is one of the four purposes of intelligence (Lowenthal, 2012 as cited in Moran, 2015). A strategic surprise, as articulated by Roberta Wohlstetter, is "an event that has significant negative impact on national interests, in which timely information was lacking or not transmitted or not correctly understood so that alternative courses of action were not taken to avert the surprise" (George, 2022, p. 154). The 1941 Pearl Harbour attack, 9/11 attacks, 1971 Yom-Kippur War, etc. are some examples. This is usually caused by ineffective communication between analysts and policymakers. It should be noted that strategic surprise is different from intelligence failure, as blame in the latter is squarely placed on the IC (George, 2022). Intelligence is vital to the formulation and execution of national security policy, but policymakers consider it as only one of the many options (George, 2020). It falls on the analyst to convince the policymaker to act on his intelligence analysis.

(3) Current Operations Intelligence: NIS defines **Current Operations Intelligence** as "the collection, analysis, operations, and planning support that IC elements conduct to enable successful planned and ongoing operations." It is "characterised by the immediacy of the support provided" (ODNI, 2014). It includes the IC function of addressing time-sensitive needs of the military, homeland security, diplomats, and policymakers in order to maximise operational decision advantage (ODNI, 2019a). This kind of function usually includes intelligence support to

ongoing international negotiations, target analysis, and crisis management. George (2020) refers to them as "Specialised types of policy support" (p. 185).

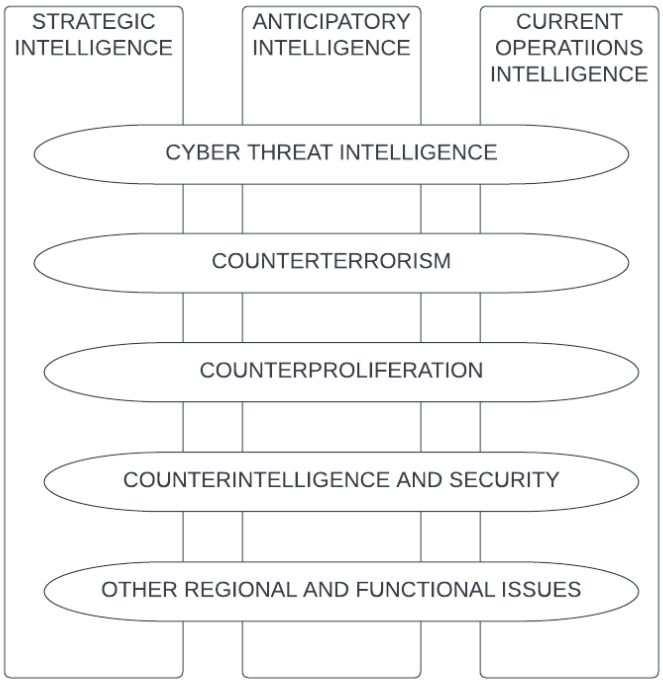
(a) Support to Diplomatic Negotiations: A former intelligence advisor to Madeleine Albright has argued that "Intelligence is the silent partner in these diplomatic endeavours, rarely acknowledged or recognised. Intelligence is a support function to diplomacy, not a peer relationship." Intelligence and diplomatic communities have a history of cooperation. U.S. diplomats have often relied upon their IC counterparts for helping build effective negotiating strategies, by assuming the role of the opposing party. Intelligence analysts also provide important assessments in ongoing negotiations and are often a part of negotiating teams. For example: CIA analysts were part of arms control negotiations throughout the cold war. Also, WMD analysts are part of the U.S. delegation in Vienna (George, 2020. P. 186).

(b) Target Analysis: is "conducted in direct support of military, counterterrorism and Counterproliferation operations" that target particular individuals or groups (George, 2020, p. 311). Target analysis can also be aimed at narco-trafficking, cyber threats, counterintelligence, etc. CIA and other defence intelligence agencies recruit analysts for these roles. While they also write threat assessments like other analysts; their main work is providing analytical support to military, intelligence operators, and law enforcement (George, 2020).

(c) Crisis Management Support: "Daily tactical intelligence", provided to policymakers, during major crisis is one of the most important intelligence functions. Agencies like CIA form "special task force of analysts" during such times, which provide round-the-clock in-depth analysis to policymakers. These analysts often produce 'situation reports' or more popularly 'known as sit-reps'. The 1962 Cuban missile crisis is an apt example of this kind of intelligence support. HUMINT, SIGINT, and IMINT collection was conducted round the clock and analysts provided frequent updates of the missile sites. The U-2 photos used during the famous Adlai Stevenson address to the security-council were a product of this support function (George, 2020).

One can also add "**Covert Action**" to this list. Although, it should be noted that only the CIA is authorised to conduct covert operations on the direction of POTUS (ODNI, 2020). Covert action is one policy tool which is "better categorised as a policymaking role rather than intelligence-support" as the CIA is directly involved in planning and executing covert operation (George, 2020, p. 45).

These foundational mission objectives address a wide range of functional (counterterrorism, Cyber Threats, transnational crime, etc) and regional (Africa, East Asia, Europe, etc) topics. The IC is apprised of their order of prioritisation through the **National Intelligence Priorities Framework (NIPF)** (ODNI, 2019a). NIPF prioritises these topics by the method of numerical ranking. For example: 1-5.



Source: NIS 2019

Topical Mission Objectives

The other four are regarded as **Topical Mission Objectives**. These functional issues are the top priority topical missions, IC is tasked with. They are: *Cyber Threat Intelligence*, *Counterterrorism*, *Counterproliferation*, and *Counterintelligence and Security*.

(4) Cyber Threat Intelligence: is focused upon "detecting and understanding cyber threats from state and non-state actors" to inform national security decision-making, enhance cybersecurity and enable responses (ODNI, 2019a). Cyber threats pose a risk to public health, critical infrastructure and information networks. The NIS directs the IC to: (a) increase understanding of cyber operations; (b) expand the production and dissemination of actionable intelligence to protect information networks and critical infrastructure; (c) expand its ability to enable operations (diplomatic, military, information, law enforcement, financial, economic and intelligence) for countering cyber threats.

(5) Counterterrorism: IC provides integral support to the government effort against terrorism. The National Counterterrorism Centre serves as the NIM for counterterrorism. The NIS directs the IC to: (a) address the evolving threat of WMD terrorism; (b) support disruption of terrorist attacks; (c) warn about threats and trends; (d) deepen understanding through strategic intelligence analysis of global terrorism landscape.

(6) Counterproliferation: IC provides integral support to the whole-of-government effort for Counterproliferation. The National Counterproliferation Centre serves as the NIM for Counterproliferation. The NIS directs the IC to: (a) develop strategic intelligence capabilities to deepen the understanding of foreign WMD programs; (b) assist in strengthening U.S. efforts to counter WMD threats and secure stockpiles; (c) anticipate and manage any related crisis.

(7) Counterintelligence and Security (CI&S): focuses upon countering 'insider threats' and threats from 'Foreign Intelligence Entities (FIE)' to "protect U.S. national and economic

security." These threats put cyber tools, supply chains and critical infrastructure at risk. The National Counterintelligence and Security Centre serves as the NIM for CI&S. The NIS directs the IC to: (a) advance understanding of FIE threats and security vulnerabilities and strengthen the exchange of their information to coordinate mitigation approaches; (b) develop capabilities to "detect, deter, and disrupt" FIE and insider threats; (c) advance efforts to protect from these threats.

ENTERPRISE OBJECTIVES

The *Enterprise Objectives* outlined in NIS 2019 support the seven mission objectives and address the effective management of mission capabilities and business functions of the IC. The first objective, "Integrated Mission Management" focuses upon coordinating and de-conflicting IC mission capabilities, minimising redundancies and efficient use of resources. The second, "Integrated Business Management" aims to optimize IC business functions and practices. The third, "People" embraces diversity and inclusion and aims to retain an expert workforce committed to these principles. The fourth, "Innovation" seeks to nurture an atmosphere of innovation, encourage ground-breaking research to improve capabilities, and advance tradecraft. Projects like the Intelligence, Science and Technology Partnership (In-STeP) are important steps in achieving this objective. The fifth, "Information Sharing and Safeguarding" aims to safeguard information and improve collaboration. The sixth, "Partnerships" focuses on "enhancing intelligence through partnerships." The seventh and the last objective, "Privacy, Civil Liberties, and Transparency" seeks to safeguard privacy and civil liberties and build public trust. It also features the *Principles of Intelligence Transparency* that provides general guidelines for the IC to make information public to build trust and enhance public understanding of IC activities.

STRATEGIC ENVIRONMENT

NIS 2019 features the IC's assessment of 2019 strategic environment. This assessment remains largely relevant today. To begin with, NIS recognises that we live in an increasingly uncertain world and face a highly volatile strategic environment. It categorises the threats faced by United

States as: **conventional/traditional** and **new/evolving**; acknowledging the new challenges posed by technological advancement. It further adds that both these threats are complex, interconnected and transnational in nature.

Conventional/Traditional Threats

The NIS mentions that the US faces many ***conventional threats*** from its traditional adversaries like Russia, China, North Korea and Iran; pervading all spheres of state activity (economic, political, military, traditional, non-traditional, etc). These include, Russian attempts to increase its influence; China's military modernisation and quest for hegemony in the pacific; North Korean aggression and pursuit of ballistic missile technology; Iran's quest for advancing military capability and support to terrorist groups; and WMD related threats.

New/Evolving Threats

Technological advancement, NIS mentions, has enabled ***new/evolving threats***, especially in the realm of space, cyberspace, computing and emerging technologies. **Democratisation of Space** has led to increase in adversarial presence. China and Russia are aiming at parity or even exceeding United States in many areas. **Increasing commercialisation of Space** is another concern as now anybody with resources can exert influence in space. **Cyber Threats** shake public confidence and increase economic costs. Adversaries with advance cyber capabilities pose threat to US security and critical infrastructure. **Emerging Technologies** like Artificial Intelligence (AI), automation and high-performance computing have numerous benefits, but they also mean advancement in military and intelligence capabilities of adversaries. Other emerging technologies like bio- and nanotechnologies lack "common ethical standards."

Democratisation of communications technology and **abundance of data** has created opportunities for IC but has also challenged its ability to "collect, process, evaluate, and analyse such enormous volumes of data quickly enough to provide relevant and useful insights to its customers." **Increase in influence of individuals and groups** in all areas of state activity poses a grave threat to governmental institutions. Their influence has empowered ethnic and religious

sources of identity, frequently exploited by violent extremist groups. **Increasing migration and urbanisation of populations** strains government capacities and causes resource scarcity, resulting in fractured societies. These are often root causes of political instability and radicalization. Other threats include climate change, outbreaks of infectious diseases and transnational criminal organizations.

CONCLUSION

NIS 2019 technically presents DNI's strategic direction to the IC. It is supposed to act as the guiding strategy for the community. It undoubtedly, falls short of that. The foundational mission objectives, which are no doubt vital for intelligence support, are incomplete without other critical support functions that IC provides to the policy community, such as policy action and policy evaluation support. In addition to this, insufficient attention is given to covert operations which have a long history of being the preferred instrument of US foreign policy execution. Another criticism of the NIS is that the *Principles of Professional Ethics* although noble, are "strikingly general and more of a declaration of intent rather than an actual guide for action" (Vrist Ronn, 2017). Frisk and Johansson (2021) also argue similarly that these principles are not ethical principles as they offer no action-guidance at all. They cannot help the officer or the decision-maker in conducting intelligence activities. They further mention that NIS "implies that intelligence ethics is an oxymoron" (p. 85). They also cite an example, noting that the code includes a principle like 'diversity' which has no relevance to collection or decision-making, but fails to include any guidelines for covert operations and interrogation techniques. Many believe that these principles were released post-Snowden revelations in order to save-face. Although, this has been denied by DNI Clapper in his memoir, it remains a cogent argument. To conclude, ODNI must work towards an effective intelligence strategy which does not ignore key support functions and is not based on generalisations. If this persists, the NIS, like many other unclassified US strategies, will continue to be regarded as rhetoric rather than genuine substance.

References

1. George, R.Z. (2022). Intelligence and Strategy. In J. Baylis, J.J. Wirtz & J.L. Johnson (Eds.), *Strategy in the Contemporary World* (pp. 145-164). Oxford University Press.

2. George, R.Z. (2020). *Intelligence in the National Security Enterprise: An Introduction*. Georgetown University Press.

3. Lowenthal, M.M. (2020). *Intelligence: From Secrets to Policy*. SAGE Publications.

4. Moran, A. (2015). Intelligence and Security. In P. Hough, S. Malik, A. Moran & B. Pilbeam (Eds.), *International Security Studies: Theory and Practice* (pp. 178-190). Routledge.

5. Ronn, K.V. (2017). The Professional Ethics of Intelligence. In N.R. Fyfe, H.O.I. Gundhus & K.V. Ronn (Eds.), *Moral Issues in Intelligence-led Policing* (pp. 121-139). Routledge.

6. Frisk, R. & Johansson, L. (2021). From Samurais to Borgs: Reflections on the Importance of Intelligence Ethics, *International Journal of Intelligence and CounterIntelligence*, 34:1, 70-96, DOI: 10.1080/08850607.2020.1734768

7. Office of the Director of National Intelligence. (2020). *Intelligence Community Legal Reference Book.* https://www.dni.gov/files/documents/OGC/IC%20Legal%20Reference%20Book%202020.pdf

8. Office of the Director of National Intelligence. (2019a). *National Intelligence Strategy of the United States of America*. https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf

9. Office of the Director of National Intelligence. (2019b, January 22). *DNI Coats unveils the 2019 National Intelligence Strategy* [Press release]. https://www.dni.gov/index.php/newsroom/press-releases/item/1941-strategy-promotes-integration-innovation-partnerships-and-transparency-for-the-17-intelligence-elements

10. Office of the Director of National Intelligence. (2014). *National Intelligence Strategy of the United States of America*. https://www.dni.gov/files/documents/2014_NIS_Publication.pdf

11. Bowen, B.D. (2020). *Lessons from Anticipatory Intelligence: Resilient Pedagogy In The Face Of Future Disruptions. https://oen.pressbooks.pub/resilientpedagogy/chapter/lessons-from-anticipatory-intelligence-resilient-pedagogy-in-the-face-of-future-disruptions/*