

Understanding The GENERATION WARFARE INTELLIGENCE (GWARINT) of Social Media and Generative AI for Digital Communication PSYOPS

Noor Nirwandy Mat Noordin

*Centre for Media & PSYOPS Studies, Faculty of Communication & Media Studies
Universiti Teknologi MARA*

Corresponding email: nirwandy3493@uitm.edu.my

ABSTRACT

GWARINT (Generation Warfare Intelligence) in current digital context involves the connecting element of intelligence family to uphold Digital Asymmetrical Environment strategies which includes the related component of intelligence traits. This new dimension brings new innovation and approach in PSYOPS including as GWARINT applications is fundamental particularly in PSYOPS application. It consists of the existing intelligence approaches as in digital asymmetrical environment it requires more flexible and modularized GWARINT strategic applications in PSYOPS application. Hence, understanding these components will benefit the intelligence practitioners and policy makers as the rapid changes in PSYOPS application strategy is influenced by this additional dimension. This article provides essential GWARINT Operational Mapping Component for PSYOPS application practices in digital asymmetrical environment of social media including generative AI user. The article also presents the essential component a GWARINT Operational Mapping Guidance Framework. It analyses and conceptualizes potential strategy for improving the implementations of PSYOPS using GWARINT as intelligence component. The input is significant as this intelligence understanding will provide insights for understanding best practices for PSYOPS application practitioners in the Digital Asymmetrical Environment complexity. The framework of GWARINT Operational Mapping Guidance Framework is suitable for Intelligence Community and PSYOPS policy makers to design suitable engagement in the GWARINT practices for PSYOPS application practitioners.

Keywords: Digital Asymmetrical Environment, GWARINT, Generative AI, Intelligence, PSYOPS

INTRODUCTION

Technology has brought social implications to society. It has expedited information sharing in digital and social media, changing the tempo and structure of communication process and devices. It has brought some changes to people belief and values occurring with current emerging threat of people centric domination that has shown some unnecessary situational conducts throughout the world as in current reality the people power is greater than people in power (Nepstad,2023). The rebellious conducts in some continents together with aggressive political turmoil in certain PSYOPS recipient are among the consequences of communication technology advancement to society. The turmoil has proved the adaptation of current demographic changes that include the global acceptance concept on equality – promoting through human security and human rights, expedite by rapid communication processes, which lead to potential changes of society behaviour when it collides with authoritative governance. Although these emerging threats are fresh concern to many PSYOPS strategist, however definite identification framework to absorb the potential impacts is still vague in determining what are the exact cause of societal changes towards holding government policies and particular governance structure.

In prevailing against current changes of people perception over governance structure and political stability issues, particular mobilizations are needed as understanding and controlling the populace are no longer depends primarily on superiority of intelligence (Lowenthal, 2021). Intelligence apparatus or intelligence family consist of HUMINT, OSINT, IMINT, MASINT, SOCMINT has to be further extended. The vague, inconsistency without define identification policy framework will expose any country to potential political turmoil and people centric rebellious. Thus, any governance holder must look on how technological advancement has changed the society preferences to understand the emerging threats to any national stability, understanding of digital asymmetrical environment forming naturally from the information complex environment. This is consistent as underlined by NATO on information complexity (NATO, 2023). Injecting GVARINT will determines the success of international influence activity but it has to be implemented through core representation of intelligence components. In addition to that, as to accelerate the PSYOPS success, the supporting or moderating variables for GVARINT is studied. Thus, understanding these relationship triggers better application of influence activity through GVARINT conducts. In PSYOPS strategy is part of the measurable and important framework for shaping public opinion and manage perceptions (Muhic, 2025). Therefore, it is crucial for any policy makers to have the ability to identify these mentioned variables for the shown relationship, as these understandings project better understand for strategic planning and GVARINT effects – evaluation and impact analysis. Social adjustment will expedite the PSYOPS outreach (Whyte et al., 2021). In term of the applications, PSYOPS explains that selective mission of military, economic and societal underlines decides the formidable application to audience.

PSYOPS fundamental aspects that utilize GVARINT structures are benefiting PSYOPS practitioners of tailoring the best representation in digital asymmetrical environment. It helps underlines PSYOPS allegiance in generation warfare with strategic assimilation. Adversary will continuously spur anti-social convention asymmetrically to indulge certain

hegemony which deposited adversary benefit. Civilization clashes varies in groups and nation states with PSYOPS as common fault lines including cultural clashes that will trigger clash within various civilizations from this faulty lines. Emphasizing correct PSYOPS is detrimental emotional schematic tool in digital asymmetrical environment to shape cognitive unification for PSYOPS recipient. Although PSYOPS ground is a challenging approach, implementing GVARINT as in the findings have will enable more comprehensive intelligence component to guide the PSYOPS best practices.

COMPONENT OF GVARINT IN DIGITAL ASYMETRICAL ENVIRONMENT

Digital Asymmetrical Environment is a situation when an adversary strength is not known in the information influx reality, which has created impossible identification of friendly parties or hostile adversary hence identifying common enemy existence are more complex. Digital Asymmetrical Warfare (DAW) is fought in DAE. Among the vital construct of technology in communication is the explodes of social media, and the emergence of dimension to communication processes in complex communication of social media. Moreover, with billion adopting generative AI that is directly associating with global digital transformation through personal device as highlighted by The World Economic Forum (2024). Technological advancement brought new direction warfare of peoples' digital asymmetrical environment compositions. Ciphering information through personal devices is non-extraordinary cultures in current environment as most of any citizens in the current global context are ciphering to this generational personal digital device particularly to the social media including generative AI user but in GVARINT it requires more that. Although social media including generative AI user were not the only populace component in society that utilize the gadget but social media including generative AI user are the important construct in society to reflect its ideologies and behaviour pertinently. Social media including generative AI user is subject to numerous situational discussions on how their philosophical understanding on current realities motivates them into looking for the truth according to their id driven beliefs and values. In seeking for the realities, social media including generative AI user seeks and exploits information according to their holding beliefs and values. Thus, some identifications process is required to identify social media including generative AI user and other component of society interactions to predict and analyse their desirable actions. It must integrate from human everyday technologies (Floridi,2023). Through acknowledging their exposed interactions, modifications and aligning people information seeking process will be more focus and eccentrics to their natural consonant. In GVARINT, understanding the people preferences in complex information system in social media including generative AI user is complicated, as extraction of raw data is needed from various cluster backgrounds from social media including generative AI user monitoring system to find emotional pattern sub conscious algorithm preferences that deepen their ideological substance. The intelligence data in GVARINT set helps to formulate an applicable approach to provide essential data to compute public preferences in information seeking process and taking side in their political participations from their possible means in the complex data compound. The expected output is an applicable conceptualized design application of the underlined efforts in digital and social media including generative AI user

including the identification process of digital traits signatories to compute the essential variables to explore the society segment more extensive variable. Their participation expedites the complexity of information exchanges leading to massive flow of information of various contexts through algorithmic pattern given or driven by them across diverse context (van Djick et al., 2023). This regulate to fabricating a digital traits signatories' procedures- to identify the cluster digital communications traits. In current technological stream information seeking and sharing is transpired in more niche cluster that leads to formation of complex information system due to the complex data existence.

Current technological stream brings changes in communication patterns although it means a smaller groups or capable individuals to use their supremacy capability to cause disaster on instability. Information is no longer privileged as it travels deliberately in open source environment central to intelligence and decision making (Zulkiflee, 2024). GVARINT enable the exploring the niche cluster need reliable software and conceptualizations process as this challenges are yet to be overcome solidly through any formidable approach such as the domestic supported semantic applications of data sentiment analysis, which is the ability to identify the populace sentiment based on their local dialects and jargons that trigger emotions ideological value and beliefs of GVARINT component of intelligence thresholds.

GVARINT Component Operational Mapping	Operational Descriptions
Algorithmic Pattern	Identifies how algorithms (social media, search engines, recommender systems) amplify, suppress, or repeat content based on user behaviour digital traits and preferences as likes, shares, watch time, and comments. Algorithmic detection visibility control and narrative escalation.
Emotional Insight	Maps emotional attachment (fear, anger, sympathy, pride, resentment, hope) influencing audience reaction. Insight data of emotional vulnerability and predict response to messaging or events.
Ideological Substance	Analyses core belief systems shaping opinions (nationalism, religion, liberalism, conservatism, anti-establishment views). Detect ideological preferences alignment or resistance to narratives.
Subconscious Preferences	Detects obvious or retaliation implicit biases, identity attachments, cultural instincts, and habitual content preferences that influence behaviour without conscious awareness. Critical for subtle persuasion and constructive narrative framing.
Extremism Potential	Assesses potential likelihood of radicalization by examining grievance intensity, civil disobedience, moral absolutism, "us vs

	them” framing, echo-chamber exposure, and emotional escalation patterns. Used for early warning and prevention as indicator and warning.
--	--

Figure 1: GVARINT Component Operational Mapping

PSYOPS categorization

PSYOPS categories have three levels, namely SPO/ CRPO/ CPO. Strategic Psychological Operation (SPO) is a psychological operations plan aimed at winning support and cooperation from groups that have already provided support and from neutral groups (NATO,2020). Its objective is to reduce and minimize hostile sentiments from enemies who have the potential to engage in aggressive actions and behaviours that could become sources of threats in crisis management or diplomatic actions. It is a plan to elevate the level of support for the government and national responsibilities. SPO objectives are long-term plans with political elements. SPO is a non-military activity to escalate influence operation for populace. Crisis Response PSYOPS (CRPO) is a PSYOPS plan conducted as part of the crisis response subjugating crisis responses situation in ample response time. Its objective is to gain support and willingness to cooperate among conflicting parties and society. While, Combat Psychological Operation (CPO) refers to enemy forces and the public that sides with them attacking their core ideal and values consistently. The objective of CPO is to reduce opposing power by reducing the enemy's willingness to remain aggressive and shifting them to support the government. Extended towards that, PSYOPS Support Levels are deploying various strategy, operation and tactics of PSYOPS. PSYOPS can be conducted at the strategic, operational, and tactical levels. It can be launched using Strategic PSYOPS supports the success of national objectives. Moreover, using Operational PSYOPS supports mission success and deploying Tactical PSYOPS supports tactical mission success in targeted compound. PSYOPS conduct required proper staffing of PSYOPS Staff that are PSYOPS officers need to identify behaviours, attitudes, and perceptions that need to be promoted within specific groups under their responsibility so that the planned mission is achieved. PSYOPS activities are designed to inform, reinforce, and persuade specific groups to follow the government's mission. These activities involve disseminating information to specific groups through the use of audio, visual, and audio-visual mean as states by FM 3-13 (2022). Their responsibilities in the military and non – military context, PSYOPS activities are products of PSYOPS agencies or units that support the government's mission. In missions, approval of PSYOPS plans, programs, and products remains with the government are develop into several categories. It is clustered PSYOPS activities that can be categorized according to source and objective. Categories according to source of Black Propaganda refers to information obtained from sources other than those that have been identified, Grey Propaganda refers to information whose source of information is unknown or White Propaganda refers to information received from sources that overtly in open source and publicly known.

METHODOLOGY

Exploring digital asymmetrical environment traits signatories is a situation when an adversary strength is not known in the information influx reality, which has created impossible identification of friendly parties or hostile adversary hence identifying common enemy existence are more complex. Digital Asymmetrical Warfare is fought in digital asymmetrical environment. Among the vital construct of technology in communication is the explodes of social media, and the emergence of social media including generative AI user is directly associated with global technological advancement through personal device. Technological advancement brought new dimension to communication processes in complex generation warfare of current technological stream stimulates of peoples' digital asymmetrical environment compositions. This include the capability if government algorithmic structure to accommodate asymmetrical flow of populace information (Gilliespie, 2023). Ciphering information through personal devices is non-extraordinary cultures in current environment as most of any citizens in the current global context are ciphering to this generational personal digital device particularly to the social media including generative AI user. Although social media including generative AI user were not the only populace component in society that utilize the gadget but social media including generative AI user are the important construct in society to reflect its ideologies and behaviour pertinently. Social media including generative AI user is subject to numerous situational discussions on how their philosophical understanding on current realities motivates them into looking for the truth according to their id driven beliefs and values. In seeking for the realities, social media including generative AI user seeks and exploits information according to their holding beliefs and values. Their participation expedites the complexity of information exchanges leading to massive flow of information of various contexts. Thus, some identifications process is required to identify social media including generative AI user and other component of society interactions to predict and analyse their desirable actions. Omand et al., (2012) has coined the terminology of SOCMINT and this extension of more than data extraction, analysing the big data and traits of behavioural pattern have move to more complexity of intelligence insight. This is extended terminology of GWARINT meaning, component and operational mapping. Through acknowledging their exposed interactions, modifications and aligning people information seeking process will be more focus and eccentrics to their natural consonant.

GWARINT and Digital Asymmetrical Environment Ethnography

Understanding the people preferences in complex information system in social media including generative AI user is complicated, as extraction of raw data is needed from various cluster backgrounds from social media including generative AI user monitoring system. Getting in depth of GWARINT component operational mapping consist of algorithmic pattern, emotional insight, ideological substance, subconscious preferences, extremism potential is part of digital ethnography matrix evaluation methodology in GWARINT component apparatus mapping. The data from digital ethnography helps to formulate an applicable approach to provide essential data to compute public preferences in information seeking process and taking side in their political and social participations from their possible means ideological, idea belief and

values in the complex data compound. The expected output is an applicable conceptualized design application of the underlined efforts in digital and social media including generative AI user including the identification process of digital traits signatories to compute the essential variables to explore the society segment. This regulate to fabricating a digital traits signatories' procedures- to identify the cluster digital communications traits. Their digital footprint pattern accommodates the understanding contextual of digital traits (Km et al., 2022). In current technological stream information seeking and sharing is transpired in more niche cluster that leads to formation of complex information system due to the complex data existence. Current technological stream brings changes in communication patterns although militarily it means a smaller groups or capable individuals to use their supremacy kills to cause disaster on instability. Information is no longer privileged as it travels deliberately in open source environment. Exploring the niche online cluster need reliable methodological such as digital ethnography process (Conway et al., 2024). Thus, engaging digital asymmetrical environment ethnography is important as this challenges of uncertainty is yet to be overcome solidly through any formidable approach such as the domestic supported semantic applications of data sentiment analysis, which is the ability to identify the populace sentiment based on their local dialects and jargons which includes the social media including generative AI user emotional and linguistic cues (Callaci et al., 2024)

FINDINGS AND DISCUSSIONS OF GWARINT OPERATIONAL MAPPING GUIDANCE IN PSYOPS APPLICATION

Restoring community stability is part of national stability to ensure national security upholds. National security is not limited to military threats as any form of threats fall under the covering aspect of national security. National security policy is vital security requirement for any country. National security is explored through robust domain threats of national interest. This includes the combining function in restoring community stability making information gathering and disseminating more vital than before. Furthermore, depleting in current situation when the foundation of human security and human rights - people centric representations is refining new form of global stability and transforming the national policy, national security policy must consider all permissible threat from current reality, emerging global concepts and extensive communication dissemination level in today's situation. Confidentiality and privacy is history. Information gathering and accessing activities are becoming a normal process for general citizens as explained in the context of digital asymmetrical environment ethnography. Imposing restrictions is no more a recognizable pattern without adequate information to curve the community acceptance pattern. Exploring the niche cluster in current technological stream is equally important to pivot community patterns towards any national policy – important indicator towards state stability. It is merely as social media including generative AI user are so competence with current information and vast exposure of current foundation of governing principal. As state centric is diluting or has diluted on its authoritative measurement to people centric charges, therefore engaging GWARINT Operational Mapping Guidance namely algorithmic pattern, emotional insight, ideological substance, subconscious preferences, and extremism potential is leading information to assure stabilities. These factors are important as

national security policy must include these concerns in its formulation. National security policy must consider the situational people centric thoughts and their behaviour that include communications activities, society behaviour causes and other related component as another securing data on intelligence. The essential elements and components for the intelligence formulation must address the cluster based communication process to reflect the validated intelligence output of people thoughts. The acquisition of information or intelligence gathering on national security policy formation is the new spectrum of anticipating threats and civil disobedience. Intelligence gathering for this process must be engaged through conceptualizing the necessary framework to curb these phenomena through new form of intelligence in current generation warfare.

This requires effort to underline the important variables comprising the influential component launch operative PSYOPS to construct and control community information trending patterns national for collective national security objectives. In these emerging current technological stream of social media including generative AI user, to identify the important construct to reflect the intelligence findings using GWRINT is operatively reliable. State holders are now facing the information complex systems of complex data with unlimited singular player on their personalized gadget hence identifying the variables to produce intelligence output is a mounting task. GWRINT highlights this complexity of intelligence in current generation warfare. It explains how PSYOPS non-linear communication in complex information system has disabled the identification process in digital and social media including generative AI user with the duplication of asymmetrical battle in digital zone—in digital asymmetrical environment. Conducting the intelligence through this platform must address these relatively factual findings, engaging the information through unlimited cluster that is formed in today's current technological stream arena. Overlapping of information runs naturally in social media including generative AI user making overlapping of information from multiple sources, inducing people to tap on the information accordingly in their clusters of principle, belief and values. They share selective traits making multiple group or cluster that represents selective traits and are associated with multiple personalities in reflecting the cultural and the representations of social media including generative AI user digital clusters. The emerging technological advancements and personal device communications has brought public into participating in policymaking changes. Public shares opinion, relay critics and follow domain manoeuvres conscious or subconsciously. The information within information has triggered civilian in conducting their own defining intelligence practices. Privacy and confidentiality are dead. Intelligence is no longer a privileged. Civilian share the common intelligence skills hence forcing the facet of intelligence to another decree. GWRINT identify this event, the overlapping of intelligence between the intelligence community and public dissident. It explains the race between information provider and information seekers, with both entities tries to become dominant. Moulding public perception using PSYOPS operative categorization is no longer viable unless some identification of trends and community trending pattern is known. Multiple variables are needed to explore the intelligence gathering process. GWRINT task is to conceptualize the detailing on the important variables in multi digital cluster of populations to assure national stability and security. Intelligence in GWRINT

component operational mapping addressing multiple clusters in complex data pond requires information computing tools and software computations. Technology has not only affected the society but also the intelligence dimension to accommodate the changes for assuring reliable intelligence output for national benefits.

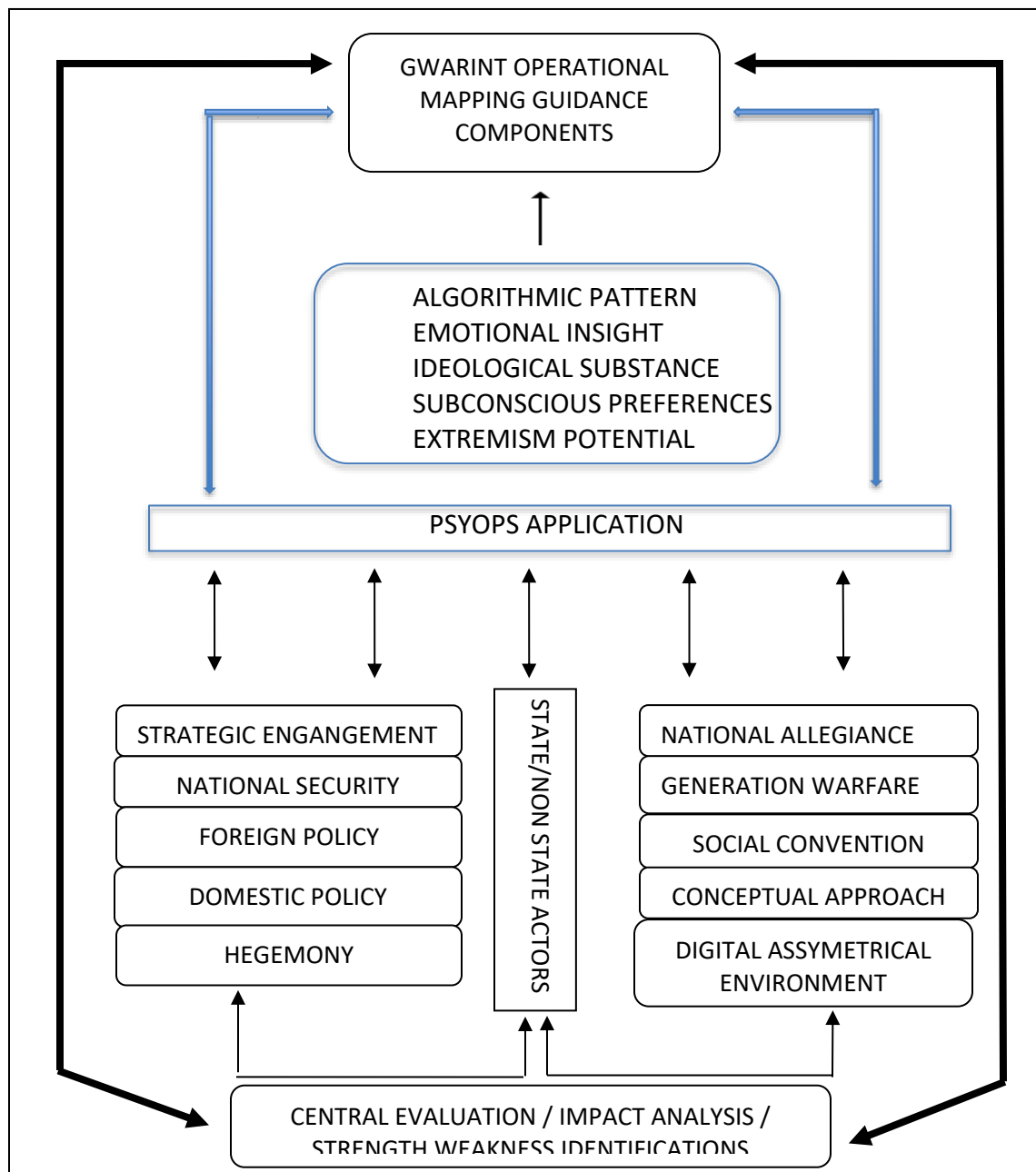


Figure 2: Gwarint Operational Mapping Guidance Framework

The GVARINT Operational Mapping Guidance Framework addressed the challenge of understanding social media including generative AI user which are commonly among some of the obstacles for PSYOPS practitioners in digital asymmetrical environment. In reality of today complex information system PSYOPS advancement have to be based inclusive data of intelligence as provided by GVARINT Operational Mapping Guidance for understanding social media including generative AI user, to seek and follow the information from intelligence effectively. These aspects are among the core details suggested to be shown in the article to fill in the gap and assuring the establishment of proper GVARINT Operational Mapping Guidance for PSYOPS participant especially on the context of current warfare applications. As illustrated in the figure above, GVARINT Operational Mapping Guidance provides conceptual framework to digest and launch GVARINT more structurally and for more effective PSYOPS application by absorbing the input of GVARINT Operational Mapping Guidance namely algorithmic pattern, emotional insight, ideological substance, subconscious preferences and extremism potential centric.

Engaging PSYOPS after deliberately being feed by GVARINT insights, PSYOPS is strategically engaged through strategic engagement to protect national policy, foreign policy and domestic policy and retaining or developing national interest hegemony. National security is set of important consideration before deploying PSYOPS and GVARINT ensure deployment of PSYOPS aligned with the intelligence checking in the complex information system reality. GVARINT Operational Mapping Guidance Framework provides detrimental knowledge of target PSYOPS recipient populace, assist formulating of PSYOPS strategies prior to adequate comprehension of target audience that will not dampened PSYOPS broader objective. Developing conceptual approach hook the masses PSYOPS doctrine of idea using social convention, generation warfare reality in the digital asymmetrical environment underlined in GVARINT Operational Mapping Guidance components listed as algorithmic pattern, emotional insight, ideological substance, subconscious preferences and extremism potential centric.

National Allegiance

In current reality global changes has escalated technologies to advance applications that has affected human routines. Technologies leading the transition flow and provide data belonging to their personal devices such as smart phones, gadget for their enjoyment and personal expression in the era information superiority mania (Vanden Abeele et al., 2023) Besides that, the shift creates dynamic communications in multi digital cluster in complex information system. It also transfers privilege information and participation to general populace, making public keener to participate in national policy discussion. Hence altering national allegiance based on individualisations cognitive behaviourism is part of modern society traits. No information is deemed privileges and privates as public keen to involve in governance functions. Comments, opinion, rejection, condemnations are no longer shared within authoritative or involved parties as it is becoming a social convention in digital society. From modern gadget and personalized software these changes are reaming to induce people to

participate in national policy and governance. Furthermore, all the discussion is centralized towards their digital cluster snowballing to negative or positive acceptance of national structures, policy and governance. National allegiance does not constitute support as the dynamic communications has refined national allegiance. It creates information competition as states by NATO (2024). Patriotism does not more reliably being enhanced through the national anthem as it need to fulfil the cluster requirement to maintain national unity, signifying patriotism through more creative methods and medium. Social convention is changing parallel to global concept hegemony rather than national centric hegemony for the social media including generative AI user users in a nation states. The changing scenario hurled the communication barrier of state centric to more dynamic global emerging hegemonic concept such as the human centric - human security and human rights. Human security coined by is centralized to emerging global concepts, people centric as compared to the state centric approaches. Several mechanisms have been outlined, looking from the context of prevention and punishment. The two contentions are interrelated as both aspects are equally important to assure better security social order in communities. Within human security which as extension of human rights definition (UNDP,2025) people are the dominant form of state growth. It means the security of people is vital concern for any country to ensure its citizen is not neglected but it also switches the peoples thought, framing their allegiance through new emerging perspective.

Hence, GVARINT identifications need to be accurate, conceptualized and statistical proven as information is an asset to remain superior over adversary or friendly enemy in any governance or civilizations from the algorithmic floating data with deep the consideration of GVARINT Operational Mapping Guidance. The intelligence input of GVARINT component of algorithmic pattern, emotional insight, ideological substance, subconscious preferences and extremism potential is set to surpassed the privileges of the influx of information complex data, in digital asymmetrical environment that will benefit any particular premises or individuals which are dominating the information. Surpassing this allow to retain national allegiance moulding them accordingly through changing of PSYOPS customized and dedicated social convention. The current technological stream has moved to upheaval surroundings where it transacted from the cluster based allegiance – transforming the control forms to approaching latitude. Government is no more isolated and has exclusive entity in the governing of populace. Global governance is shifting to benefit the people needs and demands, hedging security of people as national top priority. Traditional security looks on direct threats, relying on military and intelligence of the state against any aggression but GVARINT leads the national allegiance PSYOPS in intelligence driven enhance dictations. And ironically, in present formation, national security no more focus on the military parades and accessories as security has transformed to broader contexts definitions—security of the people. Formulating a stabilize country must address the national allegiance in current situations, conceptualized PSYOPS using more populace phenomenal GVARINT dimensions.

GWARINT Intelligence Community

In current reality, social media including generative AI user is a generation with subcultures of information superiority effect that exposed to myriad of changes. Social media including generative AI user is a complex group to understand. In current context, social media including generative AI user s are the generation that are reflecting this subculture, with lots of activity, with lots of potentiality or perhaps lots of potential harms towards the nation buildings if their aspirations differ from the state holders visioning perspectives. In maintaining their directions to be aligned as the fundamental of future national growth, these social media including generative AI user must be treated as selective principal with lots of potentials particularly for the social upbringings of a country. Social media including generative AI user are among the most exposed component of society in technology advancement particularly in communication through social media including generative AI, making social media including generative AI user engagement in current technological stream realities is important. The future lies in social media including generative AI user. Stability in a state is determined with total support of social media including generative AI user , and positive social convention will assure prosperity and growth in this technology advancement era is secured without modification of behaviours through insurgency alike social convention in important as technology has affected many PSYOPS recipient' societies changing behavioural, making the affiliation of social media including generative AI user in participating with society safety such as on national interest is important. Social media including generative AI user must be included in making the society prosper and ensuring national stability is upheld from within populace strongholds. Social media including generative AI user are potential to tap into national policy structures for cushioning the negative impact of technology to society. Intelligence Community in GWARINT has to adopts traits of intelligence analyst such as having a diligent mind, stay beyond conventional cognitive have the capability to curb intelligence failure, identifying signal and indicator in alert mode and to predict denial and deception of many forms.

GWARINT INTELLIGENCE COMMUNITY HEAT MAP INDICATOR				
Dimension	Exposure Level	Influence Impact	Volatility	Security Risk
Algorithmic Pattern	Critical	Critical	High	Critical
Emotional Insight	High	Critical	Critical	High
Ideological Substance	Medium	High	Medium	High
Subconscious Preferences	Critical	Critical	High	High
Extremism Potential	Medium	Critical	Critical	Critical

Figure 3: GWARINT Intelligence Community Heat Map Indicator
(Simulation Data Example)

New thrust of PSYOPS approaches must be developed through adequate intelligence from GVARINT identifications and applications. Social media including generative AI mapping user shall be addressed from the Intelligence Community to project pattern of GVARINT Operational Mapping Guidance Potentials in specific indicator. The algorithmic pattern, emotional insight, ideological substance, subconscious preferences and extremism potential is developed by Intelligence Community for better PSYOPS intervention or modification. Intelligence heat map is part intelligence new era integration (Kim et al.,2022). Projecting necessary intelligence heat map to sense any high, medium or critical indicator for immediate alteration or to maintain a positive social convention is part of GVARINT operative modes. It involves collecting data and understanding in categorization of populace complex cluster. Stepping to their clustering unit seems as an ordinary process but it requires lots of digestion and feasible method, working on common traits or features for them to involve voluntarily in your directions with are not possible without GVARINT understandings to expedite the changes and forecasting the coming effects. Recognize heterogeneity of social media including generative AI user by their hidden capability such as AI augmented human (Ferrara,2024) are among the method to navigate the lesser negative outcome by inclusive dimension GVARINT projection. Tackling social media including generative AI user is a collective based representation to analyse and conceptualized the whole realities as complex of many domains. Social media including generative AI user perception in digital cluster of is not a single application nor can be controlled through authoritative functions. These interrelations help to form more constructive approach in approaching social media including generative AI user complex subcultures. Integrating sub section intelligence non-traditional online data dominants form is pre requisite to address social media including generative AI user potentials and building more reliable GVARINT Intelligence Community.

CONCLUSION AND RECOMMENDATIONS

National security reflects all the traditional and non-traditional threats prevailing in community. Today is the era of people security, consisting from protections from all dimensions. People security consists of socio-political security issues, which are important for people comprehensive security. Thus is detrimental to assure technological impact to society is looking from adequate intelligence approaches. GVARINT address reflecting current security concerns, where national security must be burdened to domestic populace to cushion the modern form of threats internally and externally. Conclusively, engaging social media including generative AI user threats in assuring society stability is important and it can be achieved by crafting PSYOPS strategic efforts based on their dominant features, particularly on technology exposures in digital and social media including generative AI user for preventing and assuring national security. GVARINT Operational Mapping Guidance will able to formulate and conceptualize appropriate national security policy intelligence components and insights. Later, the data and complexity of information will be utilised to form a strategic PSYOPS as illustrated in GVARINT Operational Mapping Guidance Framework in this article. It will compensate the emerging threat from the current global reality and situational conducts ad to current intelligence family apparatus.

Stability is built in this generation due to the ability to overcome challenges from information war and citizen glory – advancement of information, software and devices, making people capability to navigate information warfare (Bennett & Livingston, 2023) as exact component in building civilizations, overcoming the negativity from digital clusters in digital and social media including generative AI user through structured process of condensing positive social convention in modern manners. Some mechanism is outdated to be emphasized national allegiance particularly to the social media including generative AI user generation. A suitable PSYOPS approach must be formulated. It starts with GVARINT identifications of information, extract, and analyses the degree of input on algorithmic pattern, emotional insight, ideological substance, subconscious preferences and extremism potential which will help to provide the assurance for national stability launched in PSYOPS campaign.

REFERENCES

- Bennett, W. L., & Livingston, S. (2023). The disinformation age: Politics, technology, and disruptive communication. *Cambridge University Press*.
- Calacci, D., Butler, B. S., & Sugimoto, C. R. (2024). Emotions in big data: Understanding affect in social media. *Journal of Computational Social Science*, 7, 345–364. <https://doi.org/10.1007/s42001-024-00212-x>
- Conway, M., Scrivens, R., & Macnair, L. (2024). Right-wing extremism and the internet: Researching niche online communities. In *The Routledge handbook of terrorism and counterterrorism*. Routledge.
- Ferrara, E. (2024). The rise of social bots and human–AI hybrids. *Communications of the ACM*, 67(1), 58–65. <https://doi.org/10.1145/3610405>
- Floridi, L. (2023). AI as agency without intelligence: On ChatGPT, large language models, and other generative systems. *Philosophy & Technology*, 36, 1–7. <https://doi.org/10.1007/s13347-023-00613-z>
- Gillespie, T. (2023). *Platforms and the algorithmic public*. Yale University Press.
- Keim, D. A., Andrienko, G., Fekete, J.-D., Görg, C., Kohlhammer, J., & Melançon, G. (2022). Visual analytics: Definition, process, and challenges. *Information Visualization*, 21(1), 5–27. <https://doi.org/10.1177/14738716211067352>
- Kim, J., Persson, J., & Jonsson, L. (2022). Digital footprint analysis: Comparing social media signatures across platforms. *Journal of Data and Information Quality*, 14(4), Article 20. <https://doi.org/10.1145/3503160>
- Lowenthal, M. M. (2021). *Intelligence: From secrets to policy* (8th ed.). CQ Press.
- Muhić, E. (2025). *Psychological operations on social networks: Examples, techniques, tactics, and procedures*. *Zaštita i sigurnost*, 5(1). <https://doi.org/10.70329/2744-2403.2025.5.9.7>
- NATO. (2023). *Allied joint doctrine for information operations (AJP-3.10)*. NATO Standardization Office.
- NATO. (2020). *Allied joint doctrine for psychological operations (AJP-3.10.1)*. NATO Standardization Office.
- NATO. (2024). *Cognitive warfare*. NATO Innovation Hub.
- Nepstad, S. E. (2023). *Nonviolent revolutions: Civil resistance in the late 20th century*. Oxford University Press.

- Omand, D., Bartlett, J., & Miller, C. (2012). Introducing social media intelligence (SOCMINT). *Intelligence and National Security*, 27(6), 801–823. <https://doi.org/10.1080/02684527.2012.716965>
- United Nations Development Programme. (2025). *Human security in the digital context*. UNDP. <https://www.undp.org/digital/blog/human-security-digital-context>
- U.S. Department of the Army. (2022). *FM 3-13: Information operations*. U.S. Government Publishing Office.
- Vanden Abeele, M. M. P., Halfmann, A., & Ooms, K. (2023). The lived experience of smartphone use: A qualitative study of enjoyment, attachment, and meaning. *Mobile Media & Communication*, 11(1), 3–21. <https://doi.org/10.1177/20501579221125292>
- van Dijck, J., Poell, T., & de Waal, M. (2023). *The platform society: Public values in a connective world* (2nd ed.). Oxford University Press.
- World Economic Forum. (2024). *The future of jobs report 2024*. World Economic Forum. <https://www.weforum.org/reports/the-future-of-jobs-report-2024>
- Whyte, A., Thrall, T. & Mazanec, B. M (2021) *PSYOPS in the Age of Cyber Conflict*. New York : Routledge
- Zulkiflee, E. F. (2024). *Digital era OSINT: Formulating special intelligence frameworks*. *Journal of Media and Information Warfare*, 17(2).