OPEN PUBLICATIONS

Cognitive Domain: The Role of Emerging Disruptive Technologies in the Transition from Situational Awareness to Situational Understanding

Volume 10, Number 4, 2025
ISSN 2957-7160 (Online)
ISSN 2957-7799 (Print)

DISCLAIMER:

Let us know your thoughts on "Cognitive Domain: The Role of Emerging Disruptive Technologies in the Transition from Situational Awareness to Situational Understanding" by emailing us at:
editor@openpublications.org

www.openpublications.org

CREDITS

CONTRIBUTING AUTHORS

Dr Georgios Nounesis, Director of Research,
National Centre for Scientific Research “Demokritos”, Hellas

OPEN CAPABILITY LEADER

Col Stefan Lindelauf

OPEN LEAD EDITOR

Mr Jeffrey Reynolds

OPEN OPERATIONS MANAGER

LTC Alexios Antonopoulos

ACTION OFFICER

LTC Alexios Antonopoulos

OPEN EDITORIAL REVIEW BOARD

LTC Tor-Erik Hanssen
CDR Silvio Amizic
CDR Alan Cummings
LTC Claus Slembeck
LTC Anders Wedin
LTC Mithat Almaz
Ms Klodiana Thartori
Mr Helmar Storm
Mr Theodore Rubsamen
Mr Christopher Hall

TECHNICAL EDITOR

Dr. Maureen Archer

ART DESIGNER

PO1 Emilia Hilliard

CONTENTS

EXECUTIVE SUMMARY 06

INTRODUCTION 07

ANALYSIS 10

1. THE SIGNIFICANCE OF EDTS IN THE TRANSITION FROM SA TO SU 10

2. THE ROLE OF EDTS IN THE PROCESS OF ANALYSIS AND JUDGEMENT IN COGNITIVE DOMAIN FOR AN EFFECTIVE MILITARY THINKING AND UNDERSTANDING. 15

A. EDTS AS A TOOL FOR DEALING WITH THE THREATS TO UNDERSTANDING 16

B. EDTS AND ENHANCING OF THE SITUATIONAL UNDERSTANDING FUNCTIONS 20

RECOMMENDATIONS FOR NATO 21

KEY RESULTS/ CONCLUSION 23

REFERENCES 24

COGNITIVE DOMAIN: THE ROLE OF EMERGING DISRUPTIVE TECHNOLOGIES IN THE TRANSITION FROM SITUATIONAL AWARENESS TO SITUATIONAL UNDERSTANDING

DR GEORGIOS NOUNESIS
DIRECTOR OF RESEARCH, NATIONAL CENTRE FOR SCIENTIFIC RESEARCH "DEMOKRITOS", HELLAS

ABSTRACT

Integrating Emerging and Disruptive Technologies (EDTs) into military operations revolutionizes Situational Understanding (SU and is critical to informed decision-making and mission success. These advancements in information management and communication technologies significantly influence command capabilities. This paper explores the pivotal role of EDTs in enhancing data collection, processing, and analysis, thereby enabling military organizations to counter effectively misinformation, disinformation, and malinformation, as well as cognitive biases and information overload. By leveraging AI-powered algorithms, big data analytics, and real-time verification methods, EDTs ensure intelligence assessments' accuracy and reliability, fostering better judgment in complex operational environments.

Central to the effective use of EDTs is the human factor— individuals' creativity, competence, and strategic thinking. NATO's strength lies in its human capital, where technological superiority results from the collaborative efforts of operators (i.e. end users), researchers, scientists, and leaders making strategic choices. The paper emphasizes the importance of integrating EDTs into military training and education programs to develop digital literacy, analytical skills, and resilience against cognitive biases. Military personnel can adapt to evolving threats through interdisciplinary approaches and immersive training simulations. This ensures that the human element remains at the forefront of technological advancements in defence.

EXECUTIVE SUMMARY

This paper delves into the profound impact of EDTs on SU within military operations, emphasizing their critical role in effective decision-making and mission success.

Additionally, this paper underscores the importance of human creativity, competence, and strategic decision-making in achieving technological superiority, emphasizing NATO's strength in its human capital. Military organizations can navigate complex operational environments more clearly and precisely using information management and communication technologies. Nevertheless, it is critical to recognize that EDTs' effectiveness depends not only on the technology but also on the people and processes involved in implementing and using the technology. Ensuring that the technology is seamlessly integrated with personnel and procedural frameworks is key to maximizing the effectiveness of EDTs in military operations.

EDTs such as AI-powered algorithms, big data analytics, and real-time data verification methods enhance intelligence assessments by counteracting misinformation, cognitive biases, and information overload. To further capitalize on these benefits, the paper advocates for the integration of EDTs into military training and education programs in order to enhance digital literacy, analytical skills, and resilience against cognitive biases. By fostering critical thinking and adaptive decision-making through interdisciplinary approaches and immersive simulations, military personnel can effectively respond to evolving security challenges, ensuring agile, resilient, and effective military operations.

EDTs emerge as essential tools for countering contemporary hybrid threats. They enable the military to detect and neutralize misinformation, ensure data integrity, and facilitate rapid, reliable information dissemination. By harnessing these technologies, NATO aims to bolster resilience against modern warfare complexities, safeguard critical infrastructure, and uphold state stability, providing a strong foundation for economic growth and development and societal cohesion.

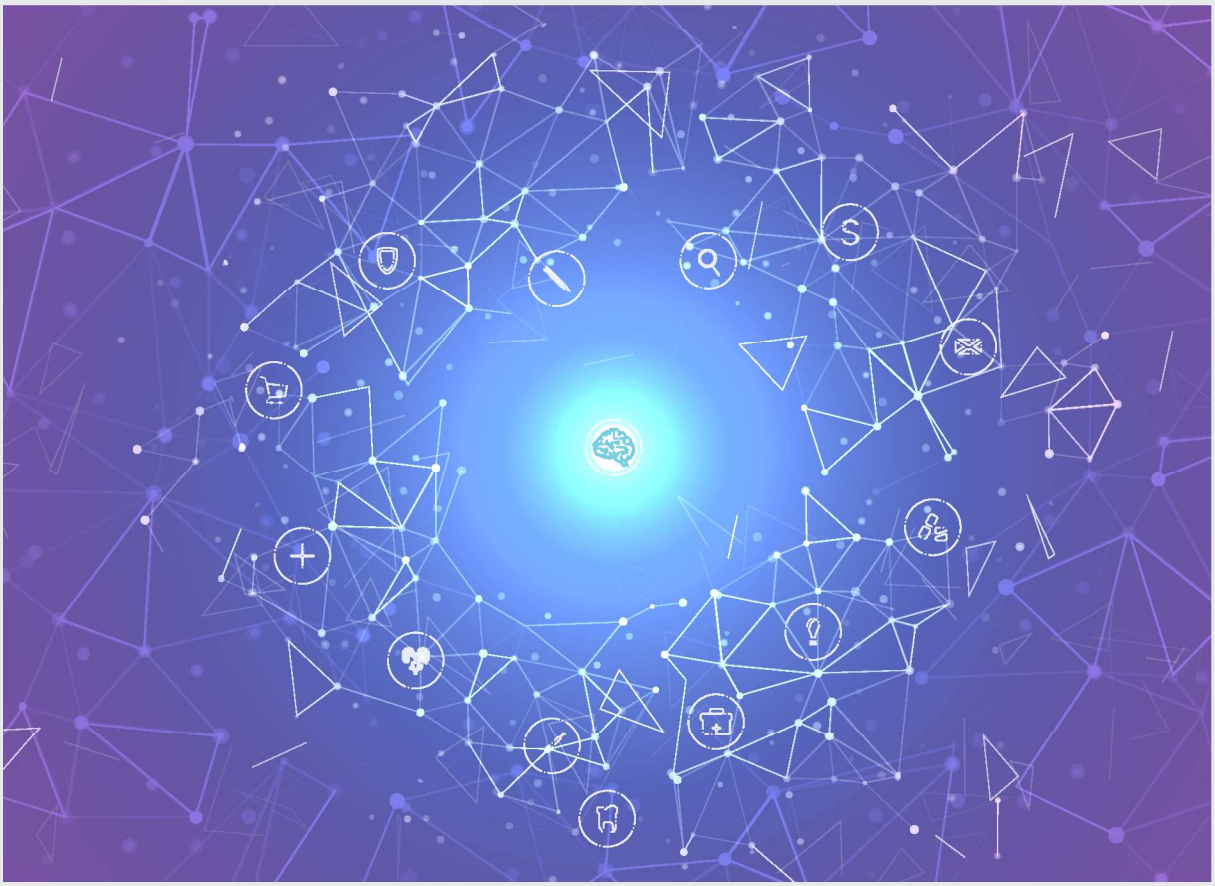
Keywords: *Emerging Disruptive Technologies (EDTs), Situational Awareness (SA), Situational Understanding (SU), Resilience, Cognitive Biases, Digital Literacy, Misinformation, Hybrid Threats*

INTRODUCTION

The term 'emerging and disruptive technologies' refers to new and innovative technologies that are affecting the military and other sectors in a significant way. Artificial Intelligence (AI), including Machine Learning (ML) and Large Language Models (LLMs), along with autonomous systems, big data analytics, and advanced communication networks, are among these technologies, which are used to improve decision-making, logistics, and operational efficiency.

Situational awareness (SA) is the perception of environmental elements and events, the comprehension of their meaning, and the projection of their future status. In military contexts, it involves understanding battlefield dynamics, including the positions and movements of friendly and enemy forces, terrain, and potential threats. Enhanced SA enables commanders to make informed decisions based on real-time data, improving operational effectiveness.

Situational understanding (SU) extends beyond mere awareness by integrating information and insights to form a comprehensive picture of the operational environment. It involves analysing the significance of the data collected and interpreting it in the context of strategic objectives and potential



outcomes. This deeper level of understanding is crucial for the effective planning and execution of military operations, allowing leaders to anticipate challenges and adapt their strategies accordingly. SU and SA are enhanced by EDTs. The tools EDTs provide allow military personnel to make effective strategic decisions in complex environments. In the dynamic landscape of contemporary conflicts, achieving comprehensive SA and SU is critical for maintaining NATO's readiness, coordination, and operational effectiveness in collective defence and security operations. The transition from SA to SU comprises a complex multiparameter, multidomain cognitive process of analysis and judgment that enhances awareness by adding sense and context. It requires the utmost ability to collect, process and analyse information. From forecasting to military planning to successful decision making, it will enable the Alliance to Out-Think, Out-Place, Out-partner and Out-Last adversaries.

SA and SU, grounded in intelligence and foresight, are essential for the success of NATO's Joint Headquarters, where different military branches coordinate, and for the military commanders who lead and make strategic decisions. Commanders at all levels are now expected to take ownership of intelligence, highlighting the need for timely, accurate, and detailed information. This includes gender-disaggregated data to better understand population dynamics and perspectives.[1] Achieving this understanding requires more than utilizing various sources and agencies; it involves formulating smart, relevant information requirements that probe the environment and adversaries effectively.

Historically, doctrines like AJP-02 (Allied Joint Publication - Intelligence), planning processes such as the Comprehensive Preparation of the Operational Environment (CPOE), and concepts like Knowledge Development (KD) have been fundamental to military understanding. Warfare's quickly evolving nature requires a broader SA through the collection, processing and dissemination of accurate information, and good analysis and judgement skills to develop robust SU. This need has led to significant reflection, incorporating insights from initiatives like the Defence Innovation Accelerator for the North Atlantic (DIANA) to enhance military intelligence and analysis by considering diverse cultural, societal, and political factors.

Operational experiences in war zones such as Ukraine, as well as conflict zones such as Afghanistan and the Middle East, have influenced the discussion on SA and SU. Counterinsurgency campaigns have underscored the importance of understanding the various dynamics and differing perspectives at play. This has shifted the focus from identifying threats to comprehending the broader operational environment. This shift has transformed military intelligence and analysis practices within NATO and beyond.

EDTs are becoming increasingly significant within this context. Michael T. Flynn emphasizes the importance for analysts to absorb, organize, and disseminate information effectively and efficiently. The lifeblood of analytical work, he argues, is open-source, population-centric information.[2] EDTs offer not only the technical capabilities to process and analyse vast amounts of data but also the means to derive actionable insights that inform decision-making.

Inadequate understanding of the potential of EDTs and their exploitable vulnerabilities pose significant threats to national security and defence. Risks include the acquisition of sensitive data about state organizations and security systems, as well as the compromise of infrastructure necessary for national security.

In the framework of Cognitive Domain, transitioning from SA to SU is a multifaceted cognitive process involving the analysis and interpretation of vast amounts of information in a dynamic and often ambiguous environment. While SA captures and processes relevant data points, SU looks beyond awareness to comprehend a situation's context, implications, and potential future developments. However, this transition is fraught with challenges, including information biases, personal/group biases, cognitive limitations, and the sheer volume of data that can overwhelm decision-makers.

---

[1]NATO, Bi-Strategic Command Directive 040-001 (Public Version) (2017), https://www.forsvarsmakten.se/siteassets/english/swedint/engelska/swedint/courses/genad/05-bi-scd-040-001-integrating-unscr-1325-and-gender-perspective-into-the-ncs.pdf.

[2]Matthew Pottinger, Michael Flynn, and Paul D. Batchelor, Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan (Washington, DC: Center for a New American Security, 2010).

Current HQ SACT work on the NATO Layered Resilience Concept, especially with the SU Thematic Working Group currently led by Greece, has indicated that addressing these challenges is crucial for effective decision-making. In this paper I would like to explore how EDTs like AI, Machine Learning (ML), and Big Data Analytics can facilitate this transition, while also mitigating threats to understanding.

Accordingly, this paper addresses the following questions:

- How can EDTs, such as AI, ML, and Big Data Analytics, be effectively leveraged to facilitate the transition from SA to SU within the context of NATO's Layered Resilience Concept?

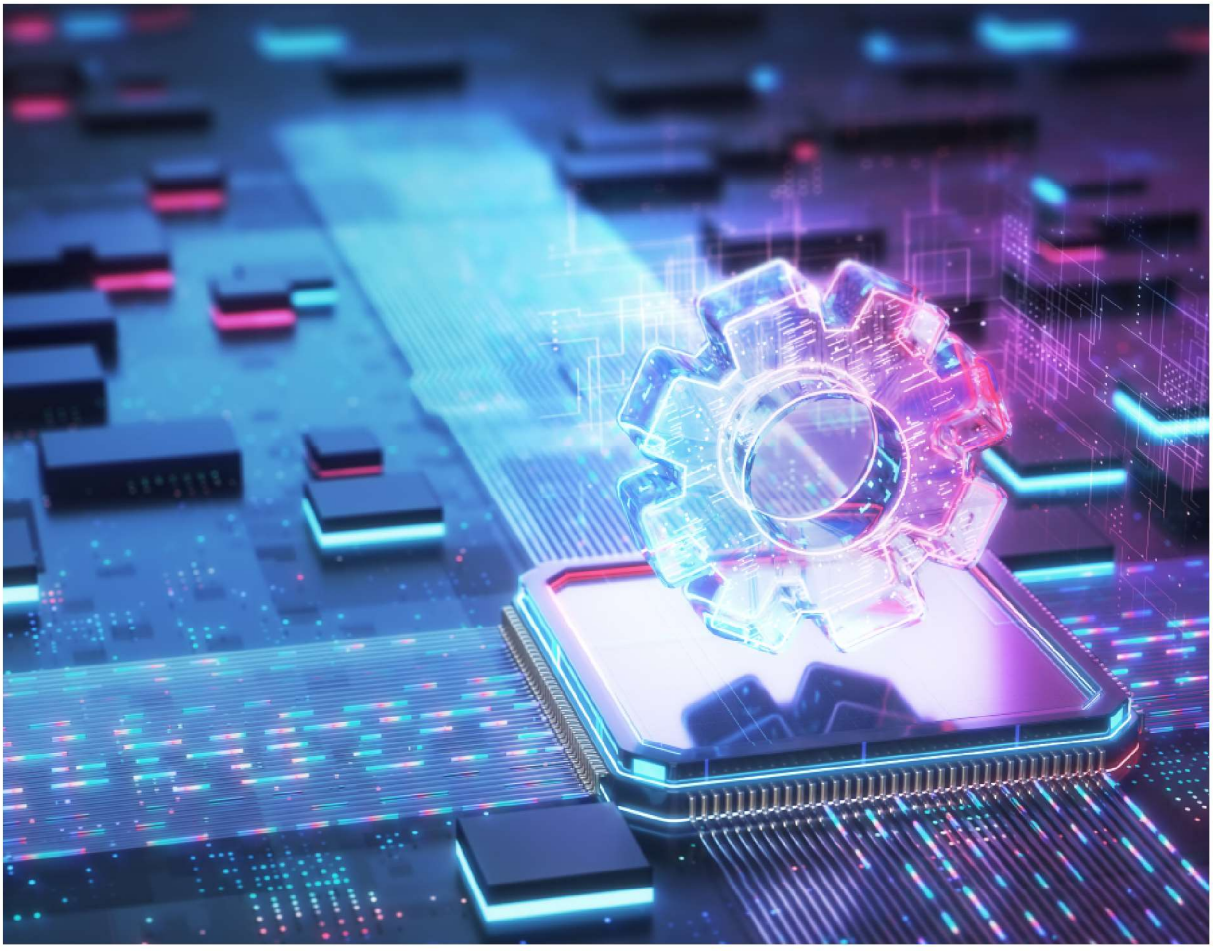
- Furthermore, how can EDTs mitigate threats to understanding, such as misinformation, disinformation, and cognitive biases, while enhancing the accuracy and efficacy of decision-making processes?

This paper discusses these questions and provides a comprehensive analysis of how EDTs enhance SU within NATO. The objective is to inform strategic decision-making, improve operational effectiveness, and advance knowledge in military science and technology.

ANALYSIS

1. The significance of EDTs in the Transition from SA to SU

SA provides individuals or organizations with a real-time understanding of the current state of affairs, enabling them to anticipate potential changes and project the environmental status into the near future. It serves as the foundation for informed decision-making and effective responses to dynamic situations, offering an awareness of what is happening without necessarily delving into the underlying causes.[3]



[3] *T. Lovering, "From Situational Awareness to Understanding," The Three Swords Magazine (2014), https://www.jwc.nato.int/images/stories/threeswords/NOV_SITAW.pdf.*

On the other hand, SU represents a deeper comprehension of the situation, extending beyond mere awareness to grasp the broader context, implications, and potential future developments. SU involves synthesizing diverse sources of information, analysing patterns and trends, and discerning the underlying dynamics shaping the situation. It provides a holistic understanding of the environment, encompassing socio-political, economic, cultural, and technological dimensions, and the relationships and interactions between various elements. This enables decision-makers to anticipate challenges, identify opportunities, and formulate strategic plans with greater foresight and precision. As human cognition is limited, and much of the information gathered during crises and conflicts is contradictory or false, more information does not necessarily lead to better understanding. A situational understanding between the enemy, partners, and civilians requires intelligence and operations integration.[4]

In a military context, understanding is the ability to accurately perceive and evaluate a situation. This is to provide the context, insight, and foresight necessary for effective decision-making. As Yufic and Malhotra explain, understanding is the feature of human intelligence that enables one to perform adequately in novel situations when prior knowledge is not available or when one needs to counteract existing inertia.[5]

[4] *United States Army Training and Doctrine Command (TRADOC), The United States Army Functional Concept for Intelligence, 2020–2040 (Pamphlet 525-2) (2017), iii.*

[5] *Yuri Yufik and Ramesh Malhotra, "Situational Understanding in the Human and the Machine," Frontiers in Systems Neuroscience 15 (2021), https://www.frontiersin.org/articles/10.3389/fnsys.2021.786252/full.*

By analysing information, one gains insight into the problem, and judgements based on this insight produce insight (foresight). The difference between SA and SU lies in the depth of analysis and comprehension that facilitates effective judgement. To make informed decisions and plan strategically, it is not sufficient to know about adversaries and their capabilities alone. It is imperative to understand their institutions, cultures, fears, perceptions, motivations, and history.

• Challenges in transitioning from SA to SU

Transitioning from SA to SU can be daunting for NATO decision-makers and analysts. One of the biggest challenges is that processing and analysing vast quantities of data can lead to paralysis by analysis.[6] The explosion of information from sensors, satellites, social media, and open-source intelligence platforms, combined with the speed at which it is generated, overwhelms traditional analytical methods in today's information-rich environment.

Discerning relevant information from noise is another major challenge.[7] Amidst the data deluge, distinguishing critical insights from irrelevant or misleading information is increasingly difficult. This is compounded by the prevalence of misinformation, disinformation, and deceptive tactics used by adversaries to obfuscate truth and manipulate perceptions. Furthermore, the landscape is complicated by the presence of lone wolf operatives and trolls, who exploit online platforms to spread false narratives and sow discord, adding another layer of complexity to the information environment. Analysts must use sophisticated techniques and tools to accurately filter, validate, and prioritize information.

Interpreting the significance of patterns and trends in the data introduces another layer of complexity. While SA offers a snapshot of the current state, achieving SU necessitates a deeper comprehension of the underlying dynamics, relationships, and causal factors driving observed phenomena. Identifying meaningful patterns, discerning causal relationships, and forecasting future trends require advanced analytical capabilities and domain expertise.

In complex operational environments of modern conflicts and crises, traditional analytical methods may not be sufficient for achieving SU. Cognitive biases, limited attention spans, and mental overload plague human analysts when dealing with large data volumes. Traditional approaches may struggle to meet the demands of modern conflicts, which are characterized by rapid changes, uncertainties, and asymmetrical threats.

[6] *Brett Forester, Toward the Data-Driven Army of 2040: Avoiding Analysis Paralysis and Harnessing the Power of Analytics (Modern War Institute, 2023), https://mwi.westpoint.edu/toward-the-data-driven-army-of-2040-avoiding-analysis-paralysis-and-harnessing-the-power-of-analytics/.*

[7] *"Discerning relevant information from noise" refers to the difficulty in distinguishing important, meaningful data from irrelevant or distracting information.*

Transitioning to SU can also be hindered by manual processes and outdated frameworks. In the past, data collection, processing, and interpretation involved manual labour, which can lead to errors. Military organizations need timely, accurate, and actionable intelligence to inform decision-making and operations planning.

• Role of EDTs in SU transition

EDTs revolutionize how we interact with and influence complex operational environments, to include the observation and collection of vast amounts of information. This overwhelming selection of information will complicate the transition from SA to SU, forcing this function to increasingly rely heavily on advances in AI, ML, and big data analytics.

As AI/ML data collection and processing from the battlefield are critical for the transition from SA to SU, more effective methods of data safeguarding should be leveraged. Post-quantum encryption (PQC) techniques[8] will allow for quantum-safe and secure data exchange between monitored personnel and mission-critical equipment, avoiding cyber threats and espionage while safeguarding important data assets. PQC will fortify data exchange on the battlefield against emerging quantum-based threats.

In the realm of SA, EDTs excel at rapidly collecting and processing diverse sources of information. AI algorithms analyse vast datasets, detecting patterns and anomalies that may indicate emerging threats or opportunities. Autonomous systems, such as unmanned aerial vehicles (UAVs), provide real-time updates, enhancing SA even in hazardous environments.

Future communication networks, such as 5G and beyond, offer high-speed, low-latency connectivity that enables real-time data sharing and collaboration among distributed teams and platforms. By adopting these advanced communication technologies, organizations can enhance coordination, interoperability, and situational awareness (SA) across diverse operational environments.

5G networks will play a central role in enabling the convergence of AI and machine learning (ML) capabilities at the edge—where data is processed on or near the source, such as sensors and battlefield systems. With support for billions of connected devices, 5G provides the low-latency, high-bandwidth communication needed to access high-quality data in real time. This infrastructure enables direct deployment of AI models on edge devices, supporting rapid, decentralized data analysis and near-real-time situational understanding (SU), even in environments with limited connectivity to central systems.

[8] *"Post-quantum encryption (PQC) techniques" refers to cryptographic methods designed to resist attacks from quantum computers, which have the potential to break many conventional encryption algorithms.*

Nonetheless, emerging and disruptive technologies (EDTs) are powerful enablers of situational understanding (SU). AI and ML algorithms take this a step further by analyzing data in depth to uncover complex interdependencies and emerging patterns in the operating environment. They generate insights, predictions, and what-if scenarios that help decision-makers anticipate challenges and develop effective strategies

• Benefits of EDTs in Achieving SU

EDTs offer numerous advantages in transitioning from SA to SU, providing organizations with increased agility, resilience, and adaptability in addressing evolving threats and challenges.

One key benefit is their capacity to enhance agility by enabling rapid adaptation to changing circumstances and emerging threats. Through advanced algorithms and real-time data analysis, EDTs empower decision-makers to identify trends, anticipate risks, and adjust strategies promptly. This agility enables organizations to respond effectively to dynamic operational environments, minimizing disruption and maximizing operational effectiveness.

Furthermore, EDTs support resilience efforts by enhancing an organization's ability to anticipate, adapt, prepare, withstand, respond to and recover from significant shocks and/or protracted adversity. For example, EDTs can help continuously monitor and analyse the operational environment, anticipating potential threats and risks. This can provide decision-makers with timely and actionable intelligence during crises or contingencies, but also facilitate decisions on force adaptation and preparation to deter potential adversaries.

Additionally, EDTs facilitate strategic foresight by analysing historical data, simulating alternative scenarios, and forecasting future outcomes. This foresight enables decision-makers to anticipate emerging threats, identify opportunities, mitigate risks before they escalate into crises, and formulate proactive strategies, thus positioning organizations ahead of the curve.

• Challenges and Considerations

The integration of EDTs into SA and SU processes poses various challenges demanding attention to optimize effectiveness and mitigate risks.
Data privacy concerns are paramount, as EDTs rely on vast data sources, often containing sensitive information. Adherence to stringent data protection regulations is necessary to safeguard privacy rights and avoid breaches, which could erode trust and incur legal consequences, undermining the legitimacy of SA and SU efforts.

Algorithmic biases present another significant challenge, particularly in AI and ML-driven EDTs. These biases can distort data analysis, perpetuate inequalities, and create ethical dilemmas. Biases often stem from imbalanced or non-representative training data, which can result in systems that misinterpret cultural behaviors, misclassify targets, or disproportionately flag certain groups as threats. For instance, an AI system trained primarily on

data from Western urban environments may underperform when deployed in diverse operational theaters, such as rural areas in the Middle East or Africa, leading to inaccurate threat assessments. In NATO operations, such distortions could impair coalition coordination, erode local trust, and compromise mission success. Addressing these challenges requires transparent methodologies, inclusive datasets, and continuous validation processes across varied geopolitical contexts.

The involvement of humans in decision-making is also an important challenge. While EDTs enhance analytical capabilities and provide valuable insights, human analysts are indispensable for interpreting and contextualizing EDT-generated information. Effective collaboration between humans and machines, management of cognitive biases, and addressing resistance to change are essential considerations for leveraging EDTs effectively in SA and SU processes.

2. The Role of EDTs in the Process of Analysis and Judgement[9] in the Cognitive Domain for Effective Military Thinking and Understanding

As military operations grow increasingly complex and data-driven, the demands on commanders and analysts to swiftly and accurately process, interpret, and apply information are intensifying. Advanced technologies like AI and ML are becoming indispensable in this context. These technologies can quickly analyse vast amounts of data, detect patterns, and generate actionable insights, enabling faster and more precise decision-making. ML systems can be employed to infer behaviors or traits—such as possible affiliations with terrorist groups or a person's rank within those groups—by analyzing their connections with others in the network.[10] At the same time, by automating routine tasks, AI-driven solutions free up military personnel to concentrate on more critical aspects of operations, reducing the risk of human error and enhancing overall strategic judgment. The integration of EDTs not only augments human cognitive capabilities but also provides real-time insights, leading to more informed and effective military decisions.

EDTs can therefore enable analysts to focus on higher-level tasks such as sense-making, interpretation, and strategic reasoning. AI-driven data visualization tools transform complex datasets into intuitive visual representations, allowing analysts to identify trends, patterns, and outliers. Similarly, natural language processing (NLP) algorithms parse unstructured text data, extract relevant information, and summarize key insights, enabling analysts to distil large volumes of information into actionable intelligence quickly.

This human-machine collaboration is essential for achieving SU. While EDTs process and analyse data, human analysts provide critical domain expertise and intuition. Together, they harness collective intelligence to achieve deeper insights and more informed decisions. SA serves as a critical foundation for decision-making, but it is the combination of comprehension and judgment—what we call understanding—that enables informed choices and forward-looking insights. Understanding involves using the clearest possible picture of a situation to support more effective decisions. Its goal is to provide decision-makers at every level with the insight and foresight necessary to act decisively while anticipating and managing potential risks and cascading consequences.

---

[9] *B. R. Parish and B. K. Madahar, Understanding Cyberspace Through Cyber Situational Awareness, Defence Science and Technology Laboratory, Cyber and Information Systems Division (DSTL Publication: DSTL/CP097651, 2016).*

[10] *Anna Nadibaidze, Ingvild Bode, and Qiaochu Zhang, AI in Military Decision Support Systems: A Review of Developments and Debates (Odense: Center for War Studies, 2024).*

A. EDTs as a Tool for Dealing with Threats to Understanding

Achieving SU is crucial for informed decision-making and mission success in military operations. However, misinformation, cognitive biases, information overload, and ambiguous data interpretation often hinder this understanding. Additional challenges include cultural and linguistic barriers, technological constraints, psychological factors, and interpersonal dynamics.

To overcome these challenges, cyber-resilient networks and integrated communication systems are essential for interagency coordination and combatting misinformation campaigns in multi-domain operations. Integrating EDTs is crucial to ensuring communication security, streamlining big data management, enhancing cyber defence, and securing defence supply chains. These technologies collectively reinforce the resilience of military communications and operations against emerging threats.[11]

Disinformation can significantly impact both military and civilian contexts, with severe consequences. For example, lynchings triggered by disinformation spread over social media[12] demonstrate its dangers across all social scales and borders. Shrewd disinformation campaigns, such as those executed by the Internet Research Agency in St. Petersburg, Russia,[13] have impacted a minority of the European population, illustrating the pervasive impact of misinformation. Cyber-attacks, like the NotPetya incident[14], have demonstrated how uncontained cyber payloads can cause extensive damage, estimated at $10 billion, by disrupting hospitals, ports, and industrial infrastructures globally. The Russia-Ukraine war further highlights the rising significance of hybrid threats in the 2020s. The advent and maturation of 5G technology will likely increase these vulnerabilities by expanding the Internet of Things, creating more opportunities for societal manipulation.[15]

These threats can impede decision-making, reduce operational effectiveness, and undermine mission objectives. Addressing them requires a multifaceted approach that promotes critical thinking, ensures access to reliable information, fosters cultural competence, utilizes technology, and employs interdisciplinary strategies.

In military operations, threats can manifest in various forms, including false reports, incomplete intelligence, and deceptive tactics employed by adversaries. False reports can mislead military decision-makers by providing inaccurate or fabricated information, leading to misguided actions or strategies. Incomplete intelligence presents only partial or fragmented information, hindering the military's ability to fully assess a situation and make informed decisions. Additionally, adversaries may use deceptive tactics to manipulate military forces, such as spreading misinformation or disinformation to create confusion or undermine trust in military operations. Adversaries might also exploit legal mechanisms, a strategy known as lawfare, to complicate military operations and decision-making processes by using legal systems to their advantage.

• Role of EDTs in Addressing Threats

EDTs revolutionize how military organizations address and counter evolving threats. These technologies bring advanced capabilities in data processing, analysis, and interpretation, allowing forces to tackle modern warfare complexity with enhanced clarity and precision.

AI-powered algorithms can scan and analyse vast amounts of data at speeds unimaginable for human operators. The algorithms can identify patterns and anomalies that could indicate potential threats, such as misinformation campaigns or cyberattacks. By filtering through large datasets, AI helps military personnel quickly distinguish credible intelligence from misleading information, ensuring decision-makers act on accurate, reliable data.

---

[11] *European Defence Agency, Enhancing EU Military Capabilities Beyond 2040 (2023), https://eda.europa.eu/docs/default-source/eda-publications/enhancing-eu-military-capabilities-beyond-2040.pdf.*

[12] *Chinmayi Arun, "On WhatsApp, Rumours, and Lynchings," Economic & Political Weekly 54, no. 6 (2019), https://www.epw.in/journal/2019/6/insight/whatsapp-rumours-and-lynchings.html.*

[13] *The Internet Research Agency (IRA) was a private enterprise that carried out influence operations on behalf of the Russian Government between 2013 and 2018. The University of Melbourne, Understanding Mass Influence: A Case Study of The Internet Research Agency as a Contemporary Mass Influence Operation (Melbourne: The University of Melbourne, 2021).*

[14] *Alex Hern, "'NotPetya' Malware Attacks Could Warrant Retaliation, Says NATO-Affiliated Researcher," The Guardian, July 3, 2017, https://www.theguardian.com/technology/2017/jul/03/notpetya-malware-attacks-ukraine-warrant-retaliation-nato-researcher-tomas-minarik.*

[15] *Tim Sweijs, Between War and Peace: 'Hybrid Threats' and NATO's Strategic Concept (The Hague: The Hague Centre for Strategic Studies, 2022), https://hcss.nl/report/war-peace-hybrid-threats-natos-strategic-concept/.*

Big Data analytics further enhances this process by correlating information from multiple sources, providing a more comprehensive picture of the operational environment. This allows for early detection of disinformation efforts and adversarial tactics. AI algorithms can help uncover and disrupt terrorist networks by analysing communication patterns and financial transactions.

Real-time data verification tools play a crucial role in ensuring military decision-making integrity. These tools can substantiate and cross-check data against known facts and reliable sources, reducing deception and enhancing intelligence assessment accuracy.

A critical component of supporting critical thinking and evidence-based reasoning is the use of EDTs, such as Cognitive Modelling and Decision Support Systems. Commanders can evaluate potential scenarios and outcomes with these technologies before committing to a specific course of action. This not only improves SU but also enhances decision-making on the battlefield, allowing for more adaptive and informed responses to threats.

In essence, EDTs are not just tools but essential allies in modern military operations. They provide the clarity, speed, and foresight needed to navigate an increasingly complex threat landscape, enabling military organizations to stay ahead of adversaries and protect their strategic interests effectively.

- **Advancing Counter-Disinformation Strategies through EDTs**

EDTs are revolutionizing the battle against disinformation, offering sophisticated tools to detect, analyse, and counter false narratives with unprecedented precision. This comprehensive approach integrates real-time monitoring, advanced analytics, and robust security measures to uphold the integrity of information in the digital age.

Real-time monitoring and detection form the backbone of this strategy. EDTs leverage AI algorithms and natural language processing (NLP) to continuously scrutinize digital platforms and social media networks. This vigilant oversight enables the early identification of suspicious patterns and misleading narratives, allowing for immediate action to curb the spread of disinformation.[16]

Advanced data analytics play a crucial role in this process. EDTs analyse vast volumes of information

---

[16]*Bence Kollanyi, Philip N. Howard, and Samuel C. Woolley, "Bots and Automation over Twitter during the U.S. Election," Data Memo, Computational Propaganda Research Project (Oxford, UK: Oxford Internet Institute, 2016).*

from diverse sources, uncovering patterns, trends, and anomalies that signal potential falsehoods. This analytical prowess helps assess the credibility of sources and validate intelligence reports, ensuring that only reliable information influences decision-making.

Content analysis and verification are further enhanced by digital forensics, which meticulously examines the origin and authenticity of digital information. By collecting, preserving, and analysing digital evidence, EDTs can trace the source of information, verify its chain of custody, and detect any tampering or manipulation. This rigorous approach ensures that intelligence assessments are based on trustworthy data, reinforcing the accuracy of the information.[17]

Sentiment analysis and network mapping provide deeper insights into the dynamics of disinformation. Sentiment analysis algorithms track shifts in public opinion and monitor the spread of false information across social networks. Network mapping techniques reveal the actors and entities behind disinformation campaigns, enabling targeted strategies to disrupt these operations effectively.[18]

In addition to these analytical tools, EDTs facilitate the development of counter-narratives. By analysing adversarial messages and themes, EDTs guide the creation of strategic responses designed to debunk false information and promote accurate narratives. This proactive approach helps counter misinformation by presenting clear and compelling alternatives.[19]

Automated response systems further strengthen these defences. AI-driven chatbots and automated moderation tools engage with users in real time, addressing misinformation and providing factual corrections. These systems are essential for managing misinformation as it emerges, ensuring that accurate information is readily accessible and widely disseminated.[20]

Cryptographic techniques also play a vital role in the EDT arsenal. By employing sophisticated algorithms and protocols, EDTs secure and authenticate digital communications, protecting them from unauthorized access, tampering, or forgery. Encryption and digital signatures verify the identity of information sources and safeguard the integrity of transmitted data, ensuring that critical intelligence remains secure.

Moreover, EDTs enhance collaborative efforts through improved information sharing. By fostering partnerships among military organizations, government agencies, and civil society, these technologies create a unified front against disinformation. Cross-sector collaboration and information-sharing networks enable a coordinated

[17] *Anik Chakraborty, Natalia Kowalczyk, and Andrzej Kolcz, "Towards Combating Fake News in Social Media Platforms: A Data Management Perspective," in Proceedings of the 2017 IEEE 33rd International Conference on Data Engineering (ICDE) (2017): 1429–1432.*

[18] *Philip N. Howard and Bence Kollanyi, "Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum," SSRN Electronic Journal (2016).*

[19] *Stefan Stieglitz, Mohammad Mirbabaie, and Benedikt Ross, "Social Media Analytics – Challenges in Topic Discovery, Data Collection, and Data Preparation," International Journal of Information Management 49 (2020): 252–260.*

[20] *Bence Kollanyi, Philip N. Howard, and Samuel C. Woolley, "Bots and Automation over Twitter during the U.S. Election," Data Memo, Computational Propaganda Research Project (Oxford, UK: Oxford Internet Institute, 2016).*

response, amplifying the effectiveness of counter-disinformation strategies.[21]

As military operations become increasingly data-driven, integrating EDTs is essential for maintaining confidence in the information that drives strategic decisions. Through vigilant monitoring, advanced analytics, forensic verification, automated responses, cryptographic security, and collaborative efforts, EDTs are pivotal in navigating the complexities of the digital landscape and safeguarding the accuracy of critical intelligence.

- **Cognitive Bias Mitigation**

EDTs are instrumental in addressing cognitive biases among military decision-makers, playing a vital role in enhancing the accuracy and effectiveness of SU. By incorporating real-time feedback, cognitive modelling, and decision support systems, these technologies foster cognitive diversity, encourage critical thinking, and reinforce evidence-based reasoning. This holistic approach ensures more effective decision-making processes and mitigates the risks posed by misinformation or manipulation, which can exacerbate cognitive biases.

The integration of cyber-resilient networks further strengthens the reliability and security of information sources. These networks provide a continuous command and control (C2) framework during multi-domain operations, ensuring that interagency coordination remains robust. By supporting automated and decentralized Command, Control, Communications, Computers, and Intelligence (C4I) systems, EDTs facilitate both strategic and operational planning, creating a secure environment for data exchange and reducing the likelihood of biases influencing military judgments.

Big Data and advanced analytics complement these efforts by enabling comprehensive analysis of extensive datasets. These technologies reveal patterns and insights that may not be immediately apparent, thereby reducing the influence of subjective biases on strategic and tactical assessments. Quantum technologies further enhance this process by improving data collection and processing, offering an even clearer understanding of the operational environment.

The role of EDTs extends beyond real-time applications; their integration into military training and education is essential for developing the digital literacy and analytical skills necessary to counter cognitive biases. Immersive training simulations and scenario-based exercises provide military personnel with realistic operational environments, honing their decision-making skills. Moreover, collaboration among data scientists, intelligence analysts, and military strategists fosters a culture of continuous learning and innovation, further strengthening the ability to make informed and unbiased decisions.[22]

In summary, EDTs are not just tools but strategic enablers that enhance decision-making and

[21] *Emanuele Mariconti, Graham Ross, and Richard Welby, "Using Social Network Analysis and Machine Learning to Detect Cyber-Physical Attacks on Smart Grids," Applied Network Science 6, no. 1 (2021): 48.*
[22] *European Defence Agency, Enhancing EU Military Capabilities Beyond 2040.*

operational effectiveness in the military. By leveraging these technologies, military organizations can improve mission success through more informed, unbiased, and resilient decision-making processes.

B. EDTs and Enhancing of the Situational Understanding Functions

In a NATO context, resilience involves the ability of individual nations and the collective Alliance to anticipate, withstand, respond to, and quickly recover from strategic disruptions and shocks across various threats. It encompasses the capacity of Allies, at both national and collective levels, and NATO itself to endure disruptions while maintaining operations.[23]

Allied Joined Publication (AJP-2) stresses that "the complexity of modern operations produces a greater need for all-encompassing intelligence [...] to enable comprehensive understanding about the environment" in an approach that "should be sufficiently inclusive, flexible and adaptive to accommodate a wide range of experts, both within and external to the formal NATO structure". Accordingly, it emphasizes that "Such experts may hold the key to understanding within the contemporary operational environment".[24]

It's crucial to acknowledge that EDTs are tools designed to augment, not replace, human expertise. They enhance decision-making by providing comprehensive data analysis, predictive modelling, and real-time feedback, which support more informed and effective strategies. This augmentation allows military personnel to focus on higher-order thinking and complex problem-solving tasks.

The integration of EDTs into command and control systems enhances resilience, agility, and effectiveness in facing evolving security challenges. By focusing on EDTs, militaries can navigate complex operational environments with improved SA and decisive action.

One of the most significant challenges in achieving SU is overcoming cognitive and informational biases that can distort decision-making. EDTs address this by offering sophisticated tools for data collection, processing, and analysis, which go beyond human capabilities. By employing AI-powered algorithms, military organizations can sift through vast datasets, identifying patterns and anomalies that might otherwise go unnoticed. This capability is critical in countering misinformation and disinformation campaigns, which are increasingly sophisticated and pervasive.

Algorithmic bias presents a unique challenge, as the very tools designed to assist in decision-making can inadvertently perpetuate societal biases embedded in their training data. Recognizing and addressing these biases is essential to ensure that EDTs enhance, rather than undermine, the fairness and inclusivity of military operations.

NATO's emphasis on integrating EDTs into command and control systems is key to enhancing resilience and agility in the face of evolving security challenges. Using AI, big data analytics, and predictive modelling, military leaders can anticipate adversarial behaviour, optimize resource allocation, and develop robust strategies. With these technologies, military organizations can turn raw data into actionable insights, thereby maintaining a crucial advantage in dynamic and complex operational environments.

Knowledge Development (KD) within NATO is another critical area where EDTs have a transformative impact. Providing continuous learning and adaptation through EDTs ensures that military personnel are not only skilled in the newest technologies but also capable of applying them successfully. Digital literacy programs and immersive training simulations help build a culture of data-driven decision-making, where the lessons of past operations inform future strategies.

As NATO navigates the complexities of modern warfare, the integration of EDTs into its strategic framework is essential. These technologies enhance situational awareness, mitigate biases, and strengthen the Alliance's overall resilience, ensuring that NATO remains agile and effective in protecting its member states and responding to global threats.

---

[23] *Allied Command Transformation – NATO's Strategic Warfare Development Command, "Resilience and Civil Preparedness in NATO" (2023), https://www.act.nato.int/article/resilience-and-civil-preparedness-in-nato.*

[24] *NATO, AJP-2: Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security (Edition A, Version 2) (February 2016), section 2.5, https://jadl.act.nato.int/ILIAS/data/testclient/lm_data/lm_152845/Linear/JISR04222102/sharedFiles/AJP2.pdf.*

RECOMMENDATIONS FOR NATO

Addressing the challenges and limitations in integrating EDTs into SA and SU processes requires strategies that not only improve technical integration and ethical governance but also explicitly facilitate the transition from awareness to deeper understanding.

1. Establishing robust data governance frameworks to ensure compliance with regulations, clarify data ownership, and safeguard privacy rights.

2. Conducting regular audits of EDT algorithms to identify and mitigate biases, promote transparency, and ensure fairness in outcomes.

3.Providing human analysts with training to enhance digital literacy, critical thinking, and collaboration skills, fostering a culture of continuous learning and adaptation.

4.Facilitating interdisciplinary collaboration between data scientists, domain experts, and decision-makers to leverage the strengths of humans and machines.

5.Engaging stakeholders in discussions about ethical, social, and legal implications of EDTs, promoting transparency and building trust in EDT-enabled solutions.

These recommendations aim to strengthen the analytical foundation provided by SA while enhancing the interpretive and judgment-based elements required for SU, ultimately enabling NATO to make more informed, foresight-driven decisions.

Prioritizing Human Capital Education in NATO Strategies

NATO's strength lies in its human capital, with its technological edge stemming from strategic decisions and collaboration. Prioritizing human involvement alongside technological advancements is crucial due to both economic constraints and the unique capabilities humans provide. Advanced technology is costly to develop,

deploy, and maintain, necessitating balanced investment in other critical areas such as training and education. Human capital education refers to the systematic development of individuals' skills, knowledge, and competencies to enhance organizational performance and adaptability. In the military context, this involves equipping personnel with the critical thinking, technological proficiency, and ethical awareness needed to navigate complex operational environments. To integrate human capital education into NATO's strategies, the following steps can be taken:

1. Develop training programs: Establish training programs focusing on digital literacy, analytical skills, and technological proficiency, including hands-on workshops and seminars on EDTs and data analysis techniques.

2. Foster cross-disciplinary collaboration: Promote knowledge sharing between different departments and member states to encourage innovation and continuous learning.

3. Invest in talent development: Identify and nurture individuals with specialized skills in EDTs by offering scholarships, internships, and career development opportunities.

4. Promote ethical and responsible use: Integrate ethics and compliance training into educational programs to raise awareness of potential risks and ensure adherence to ethical standards.

5. Support lifelong learning: Provide access to online resources and professional development opportunities to facilitate continuous skill development and knowledge exchange.

Investing in human capital education will enable NATO to leverage EDTs effectively, enhancing SA and SU capabilities and ensuring agility and resilience.

KEY RESULTS/ CONCLUSIONS

This analysis underscores a crucial shift in military operations from mere SA to a more profound level of SU. This transition marks a move from simply knowing what is happening in real-time to comprehending the broader socio-political, economic, cultural, and technological contexts that shape events. EDTs are at the heart of this evolution, serving as essential tools in bridging the gap between SA and SU.

The integration of EDTs is transforming the transition from SA to SU within complex operational environments. EDTs, encompassing advancements such as AI, ML, 5G networks, and sophisticated data analytics, provide significant enhancements in processing and interpreting vast amounts of information. These technologies are crucial in helping decision-makers swiftly navigate the overwhelming influx of data generated by modern sensors, satellites, social media, and open-source intelligence platforms.

One of the key results of integrating EDTs is the improved ability to anticipate and prepare for emerging threats. By leveraging AI algorithms to analyse large datasets and utilizing real-time data processing capabilities, EDTs offer a heightened sense of agility, resilience, and adaptability. This advancement enables military and organizational decision-makers to not only discern patterns and trends but also to effectively counter misinformation and deceptive tactics. For instance, AI-driven data visualization and natural language processing tools can distil complex information into actionable insights, revealing critical trends and anomalies that might otherwise remain obscured.

However, the adoption of EDTs comes with its own set of challenges. Issues such as data privacy, algorithmic bias, and the integration of human judgment with machine capabilities must be addressed to ensure that these technologies enhance rather than compromise decision-making processes. Moreover, the potential for misinformation and cyber-attacks underscores the necessity for robust cyber-resilient networks and cryptographic measures to safeguard critical data and maintain the integrity of intelligence operations.

Ultimately, EDTs represent a pivotal shift in modern military and organizational strategies, augmenting traditional methods with advanced analytical capabilities and real-time data processing. NATO's focus on integrating these technologies underscores the importance of building a data-driven culture and continuously adapting to an evolving threat landscape. The future of strategic decision-making will increasingly rely on the synergy between human expertise and technological advancements, highlighting the indispensable role of both in navigating the complexities of contemporary operations.

REFERENCES

1. Allied Command Transformation – NATO's Strategic Warfare Development Command. "Resilience and Civil Preparedness in NATO." 2023. https://www.act.nato.int/article/resilience-and-civil-preparedness-in-nato.

2. Arun, Chinmayi. "On WhatsApp, Rumours, and Lynchings." Economic & Political Weekly 54, no. 6 (2019). https://www.epw.in/journal/2019/6/insight/whatsapp-rumours-and-lynchings.html.

3. Chakraborty, Anik, Natalia Kowalczyk, and Andrzej Kolcz. "Towards Combating Fake News in Social Media Platforms: A Data Management Perspective." In Proceedings of the 2017 IEEE 33rd International Conference on Data Engineering (ICDE), 1429–1432. 2017.

4. European Defence Agency. Enhancing EU Military Capabilities Beyond 2040. 2023. https://eda.europa.eu/docs/default-source/eda-publications/enhancing-eu-military-capabilities-beyond-2040.pdf.

5. Forester, Brett. Toward the Data-Driven Army of 2040: Avoiding Analysis Paralysis and Harnessing the Power of Analytics. West Point, NY: Modern War Institute, 2023. https://mwi.westpoint.edu/toward-the-data-driven-army-of-2040-avoiding-analysis-paralysis-and-harnessing-the-power-of-analytics/.

6. Hern, Alex. "'NotPetya' Malware Attacks Could Warrant Retaliation, Says NATO-Affiliated Researcher." The Guardian, July 3, 2017. https://www.theguardian.com/technology/2017/jul/03/notpetya-malware-attacks-ukraine-warrant-retaliation-nato-researcher-tomas-minarik.

7. Howard, Philip N., and Bence Kollanyi. "Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum." SSRN Electronic Journal (2016).

8. Kollanyi, Bence, Philip N. Howard, and Samuel C. Woolley. "Bots and Automation over Twitter during the U.S. Election." Data Memo, Computational Propaganda Research Project. Oxford, UK: Oxford Internet Institute, 2016.

9. Lovering, T. "From Situational Awareness to Understanding." The Three Swords Magazine (2014). https://www.jwc.nato.int/images/stories/threeswords/NOV_SITAW.pdf.

10. Mariconti, Emanuele, Graham Ross, and Richard Welby. "Using Social Network Analysis and Machine Learning to Detect Cyber-Physical Attacks on Smart Grids." Applied Network Science 6, no. 1 (2021): 48.

11. Nadibaidze, Anna, Ingvild Bode, and Qiaochu Zhang. AI in Military Decision Support Systems: A Review of Developments and Debates. Odense: Center for War Studies, 2024.

12. NATO. AJP-2: Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security. Edition A, Version 2. February 2016. Section 2.5. https://jadl.act.nato.int/ILIAS/data/testclient/lm_data/lm_152845/Linear/JISR04222102/sharedFiles/AJP2.pdf.

13. NATO. Bi-Strategic Command Directive 040-001 (Public Version). 2017. https://www.forsvarsmakten.se/siteassets/english/swedint/engelska/swedint/courses/genad/05-bi-scd-040-001-integrating-unscr-1325-and-gender-perspective-into-the-ncs.pdf.

14. Parish, B. R., and B. K. Madahar. Understanding Cyberspace Through Cyber Situational Awareness. Defence Science and Technology Laboratory, Cyber and Information Systems Division. DSTL Publication: DSTL/CP097651, 2016.

15. Pottinger, Matthew, Michael Flynn, and Paul D. Batchelor. Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan. Washington, DC: Center for a New American Security, 2010.

16. Stieglitz, Stefan, Mohammad Mirbabaie, and Benedikt Ross. "Social Media Analytics – Challenges in Topic Discovery, Data Collection, and Data Preparation." International Journal of Information Management 49 (2020): 252–260.

17. Sweijs, Tim. Between War and Peace: 'Hybrid Threats' and NATO's Strategic Concept. The Hague: The Hague Centre for Strategic Studies, 2022. https://hcss.nl/report/war-peace-hybrid-threats-natos-strategic-concept/.

18. The University of Melbourne. Understanding Mass Influence: A Case Study of The Internet Research Agency as a Contemporary Mass Influence Operation. Melbourne: The University of Melbourne, 2021.

19. United States Army Training and Doctrine Command (TRADOC). The United States Army Functional Concept for Intelligence, 2020–2040 (Pamphlet 525-2). 2017.

20. Yufik, Yuri, and Ramesh Malhotra. "Situational Understanding in the Human and the Machine." Frontiers in Systems Neuroscience 15 (2021). https://www.frontiersin.org/articles/10.3389/fnsys.2021.786252/full.

Cognitive Domain: The Role of Emerging Disruptive Technologies in the Transition from Situational Awareness to Situational Understanding

www.openpublications.org