14th International Defense and Homeland Security Simulation Workshop, 005
21st International Multidisciplinary Modeling & Simulation Multiconference

2724-0363 © 2024 The Authors.
doi: 10.46354/i3m.2024.dhss.005

Strategic Engineering to support Decision Makers in Complex Systems: Innovative Models for Cognitive Warfare Simulation

Agostino Bruzzone[1,2,3,*], Antonio Giovannetti[2] , Marco Gotelli[2,3], Jan Hodicky[4], Marina Massei[1,2], Alberto De Paoli[2], Roberto Ferrari[2] , Filippo Ghisi[2]

[1]Sim4Future, Via Trento 43, Genova, 16145, Italy
[2]Simulation Team, Via Magliotto 2, Savona, 17100, Italy
[3]DIME Genoa University, Via Opera Pia 15a, Genova, 16145, Italy
[4]HQ SACT NATO, Blandy Rd, Norfolk, VA 23505, United States

[*]Corresponding author. Email address: agostino@.itim.unige.it

Abstract

In the modern scenario of cognitive warfare, understanding, predicting and manage human behavior in response to various strategies is a crucial goal. Cognitive warfare, a critical component of modern hybrid warfare, presents a complex challenge. Hybrid warfare blends traditional military actions with cyber operations, information manipulation, and psychological tactics, creating an intricate battlefield where the cognitive domain is increasingly targeted. This paper presents an advanced simulator, named CW-SINON (Cognitive Warfare- Simulation, artificial Intelligence & Neural networks for modeling human behaviors in Operations, population and social Networks), incorporating multiple Human Behavior Models (HBM) to replicate the impacts of cognitive attacks, Behavioral Psychological Social Models (BPSM), kinetic actions, and hybrid warfare initiatives. Our simulator uniquely evaluates these impacts across multiple players, institutions, and populations, taking into account their intricate structures and interactions. The core of our methodology is the Strategic Engineering Paradigm, which integrates Modeling & Simulation, Artificial Intelligence, and Data Analytics to provide robust support for decision-makers. A Design of Experiment (DoE) and ANOVA (Analysis of Variance) were performed in order to validate and verify dynamically the models, optimal duration and replication to obtain estimates on target functions.

Keywords: Modeling & Simulation; Cognitive Warfare; Strategic Engineering; Hybrid Warfare; Human Behavior Modeling

1. Introduction

Hybrid warfare, characterized by the combination of conventional and unconventional tactics, has been a persistent feature of military strategy since antiquity (Hoffman, 2014). Historically, armies have consistently integrated symmetric and asymmetric approaches, blending brute force with psychological operations. However, the term "hybrid warfare" gained prominence in public discourse only in the Third Millennium, reflecting a growing recognition of the

complexities and nuances of modern conflict (McCulloh & Johnson, 2013). This delay in recognition by the general populace underscores a broader historical trend: the masses have often been slow to grasp the full scope and nature of warfare, which has evolved significantly beyond traditional battlefields to permeate everyday life.

In contemporary conflicts, cognitive warfare has emerged as a pivotal element of hybrid warfare (Backes & Swab, 2019). Cognitive warfare targets the minds of individuals and populations, exploiting information and psychological tactics to influence perceptions, behaviors, and decision-making processes. The rapid proliferation of social media platforms has exponentially increased the speed and reach of information dissemination, amplifying the effects of cognitive operations. This new dimension of warfare presents a highly complex system, necessitating innovative and sophisticated solutions to effectively counter these threats.

Our understanding of cognitive warfare and its integration within the broader context of hybrid warfare requires advanced analytical tools and methodologies. This paper introduces a sophisticated simulator designed to model and predict human behavior in response to various cognitive strategies. The simulator incorporates multiple Human Behavior Models (HBM) capable of replicating the effects of cognitive attacks, Behavioral Psychological Social Models (BPSM), kinetic actions, and hybrid warfare initiatives. The interface of CW-SINON is proposed in figure 1. By evaluating these impacts across diverse players, institutions, and populations, the simulator provides comprehensive insights into the dynamic interplay of factors within this complex system. Central to our approach is the Strategic Engineering Paradigm, which combines Modeling & Simulation, Artificial Intelligence, and Data Analytics to support decision-makers in navigating the challenges of modern warfare. This paradigm allows for the systematic analysis of different strategies, enabling the identification of optimal approaches for influencing human behavior and institutional responses. CW-SINON represent an innovative simulator developed within the framework of the M2SG (Modeling, interoperable Simulation & Serious Games) paradigm by the Simulation Team. The M2SG paradigm synergistically integrates scientific modeling, interoperability, and the engagement of serious games to tackle complex systems. CW-SINON is specifically designed to model human behaviors and cognitive warfare, while also maintaining the capability to federate with other models, thereby enabling a comprehensive analysis of human behavior dynamics and their impacts on various fields such as economy and politics. This simulator addresses the inherent complexity of these contexts by employing high-fidelity models that replicate the intricate interactions among numerous objects and variables.

To ensure that the simulation is both effective and reliable, the M2SG paradigm facilitates intuitive understanding for validation and verification processes. Additionally, by incorporating extended reality technologies, CW-SINON offers an immersive and graphically rich environment that enhances the representation of different domains, including cyber space, population behavior, human behavior modifiers, and cognitive elements. This approach not only aids in validation and verification but also engages decision-makers by making complex scenarios more accessible and comprehensible. Consequently, CW-SINON stands as a robust tool for simulating and analyzing cognitive warfare and human behavior in an interconnected world.

The results from our simulator underscore its potential to adapt dynamically to various scenarios, offering valuable predictions and strategic recommendations. This paper emphasizes the critical importance of integrating advanced simulations and AI-driven analytics in enhancing decision-making processes in cognitive warfare. This research contributes to the growing body of literature on cognitive and hybrid warfare, highlighting the need for continued innovation and adaptation in military strategies. As the nature of conflict continues to evolve, so too must our approaches to understanding and addressing these complex challenges.

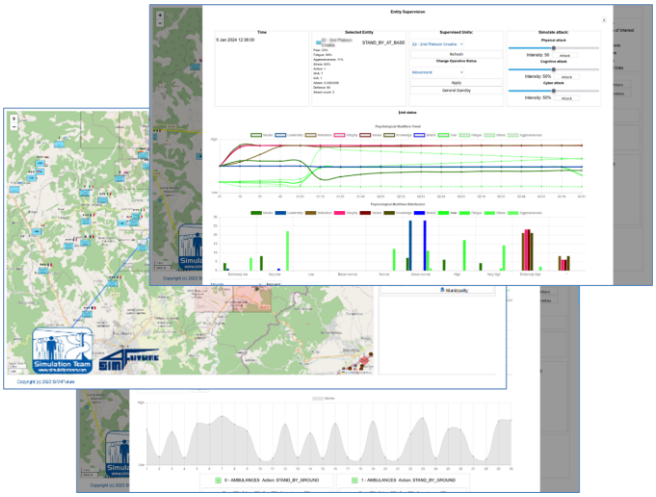

Fig.1 CW-SINON and its Human Behavior Modifiers

2. State of the Art

Hybrid warfare is an evolving form of conflict that combines traditional military force with unconventional methods such as cyber-attacks, information warfare, and psychological operations. This approach aims to exploit the vulnerabilities of adversaries across multiple domains, making it difficult to attribute actions to a single actor and

complicating the response strategies. The concept of hybrid warfare has been extensively discussed in recent literature, highlighting its complex nature and the challenges it poses to conventional defense mechanisms (Hoffman, 2007; Renz, 2016).

Hybrid warfare blurs the lines between war and peace, involving state and non-state actors, and exploiting a mix of kinetic and non-kinetic tactics. For example, Russia's actions in Ukraine and the annexation of Crimea in 2014 are often cited as quintessential examples of hybrid warfare, where military force was used in conjunction with cyber-attacks, propaganda, and the support of local militias (Marten, 2015). This type of warfare requires a comprehensive approach to security and defense, integrating military, political, economic, and informational measures. Psychological operations, or PsyOps, are a key component of both hybrid and cognitive warfare. PsyOps involve the planned use of psychological tactics to influence the perceptions, emotions, attitudes, and behavior of target audiences. These operations are executed through various means, including propaganda, misinformation, and psychological manipulation, aiming to weaken the morale of adversaries or sway public opinion in favor of the initiator's objectives (Narula, 2004).

PsyOps have been employed throughout history, but their significance has grown in the context of modern hybrid warfare. The effectiveness of PsyOps relies on a deep understanding of the target audience's psychology, culture, and social dynamics. Modern advancements in technology and communication have enhanced the reach and impact of PsyOps, allowing for more precise targeting and real-time adjustments (Paul, 2010). The increasing use of social media platforms as tools for PsyOps has transformed the battlefield, making it easier to disseminate information rapidly and widely, often blurring the lines between information and disinformation (Ramsay, 2021).

Cognitive warfare represents the next evolution in the strategy of modern conflicts, focusing on the human mind as the battlefield (Claverie & du Cluzel, 2022). This form of warfare aims to influence or disrupt the cognitive processes of individuals and groups, affecting their decision-making capabilities and perception of reality. Cognitive warfare integrates elements of PsyOps, information warfare, and social engineering, and is highly reliant on understanding and exploiting cognitive biases and psychological vulnerabilities.

The primary goal of cognitive warfare is to alter the target's perception and behavior without their awareness. Cognitive techniques include the use of tailored misinformation, deepfake technology, and sophisticated psychological manipulation to create confusion, fear, and distrust. The effectiveness of cognitive warfare is amplified by the pervasive reach of digital communication and social media, which provide platforms for rapid and widespread dissemination of manipulative content (Libicki, 2020).

The advent of social media has significantly impacted the landscape of cognitive warfare. Social media platforms serve as powerful tools for the dissemination of information and misinformation, enabling actors to reach vast audiences quickly and with relative ease. The algorithms that drive these platforms often amplify content that evokes strong emotional responses, which could be exploited to manipulate public opinion and behavior (Pennycook et al., 2018).

Cognitive biases, such as confirmation bias, availability heuristic, and social proof, play a critical role in the effectiveness of social media manipulation. These biases influence how individuals process information and make decisions, often leading them to accept and share information that aligns with their preexisting beliefs or that appears to be endorsed by their social networks (Kahneman, 2011). Understanding and leveraging these biases is a key aspect of cognitive warfare strategies.

For instance, confirmation bias leads individuals to seek out and give more weight to information that confirms their existing beliefs, while ignoring or discounting information that contradicts them. This bias could be exploited by propagandists who flood social media with targeted misinformation designed to reinforce specific narratives (Lewandowsky et al., 2012). Similarly, the availability heuristic, where people judge the likelihood of events based on how easily examples come to mind, could be manipulated by repeatedly exposing individuals to certain information or images, making them seem more prevalent or significant than they are (Tversky & Kahneman, 1973).

The integration of social media into cognitive warfare strategies highlights the importance of understanding human psychology and cognitive biases. By exploiting these elements, actors are able to effectively shape perceptions and behaviors on a large scale, making cognitive warfare a potent component of modern hybrid conflicts.

Our advanced simulator, CW-SINON, represents the culmination of integrating these cutting-edge concepts and technologies through sophisticated modeling and simulation techniques, combined with the power of generative AI. By incorporating the principles of traditional warfare, hybrid warfare, PsyOps, cognitive warfare, and the influence of social media and cognitive biases, CW-SINON provides a comprehensive platform for analyzing and understanding the nature of modern conflicts. This simulator allows us to replicate and study the implications of various types of attacks—kinetic, cyber, and cognitive—on multiple players, dimensions, institutions, and populations. Through dynamic validation and verification processes, including Design of Experiment (DoE) and Analysis of Variance (ANOVA), CW-SINON offers robust support for decision-makers, enhancing their ability to strategize and respond effectively in the complex and rapidly evolving landscape of contemporary warfare.

3. General Architecture

The simulation architecture of CW-SINON is built on a robust framework of stochastic simulation driven by Intelligent Agents (IA), a technology developed by SIM4Future for various applications, including the CAPIAS (CAbles, Pipelines, marine Infrastructures, Austonomous systems: protection and Simulation) demonstrated in the WIN Wargame Initiative for NATO. These Intelligent Agents, defined as REB-IA (Reactive and Emergent Behaviors by Intelligent Agents), form the core of our innovative approach, enabling the replication of cognitive warfare scenarios through a multi-layer simulation system that integrates REB-IA and Human Behavior Models.

The REB-IA modules are an advanced evolution of the original IA-CGF (Intelligent Agent Computer Generated Forces) created by the experts of Simulation Team. The REB-IA modules are designed to simulate complex scenarios by encompassing various components:

- REB-IA People

- REB-IA Interest Groups

- REB-IA Elements, Entities & Units

- REB-IA Human Behaviors

- REB-IA Non-Conventional Frameworks

These modules enable the simulation of local populations, supporting strategic planning for countries, regions, or towns and analyzing population reactions to crises such as flooding, earthquakes, pandemics, toxic contamination, and CBRN (Chemical, Biological, Radiological, and Nuclear) events.

1. REB-IA People: Characterized by various human behavior modifiers including fear, aggressiveness, fatigue, and stress, as well as individual parameters such as gender, age, health status, education level, social status, political preferences, religion, and ethnic group. These individuals are interconnected within people networks through friendship and parental relationships. Each individual also maintains positive and negative links with several REB-IA interest groups (e.g., political parties, media editors, political leaders, crime organizations, police departments, industrial associations, and religious communities).

2. REB-IA Interest Groups: These groups are interconnected by dynamic positive and negative links that evolve during the simulation due to events, actions, and activities, influencing each other and the various objects within the simulation.

3. REB-IA Operational Units, Actions, and Entities: Examples include squads, brigades, and helicopters, which interact with people and interest groups based on tactical actions and specific events (e.g., a police car entering a town area causing tension or an accident that affects the local population's attitude and potentially ignites a riot).

The human behaviors within the simulation are defined by conceptual models that dictate their evolution based on current status and previous experiences of the people, units, or other entities. Key parameters related to metrics proposed by ACT (Allied Command Transformation) include:

- M1: Impacts on Combat Readiness of CW Attacks: Evaluates the decrease in combat readiness due to cognitive attacks, measured by the time to complete task assignments.

$$M1_{j,v} = \max\left(\min\left(Re\Delta t_k\left(Toc_{j,v} - Toa_{j,v}\right), 200\%\right), 0\right)$$

$$M1_{\mu_k(t)} = \frac{1}{ntk}\sum_{i=1}^{ntk(t)} M1_{j,i}$$

$M1_{j,k}$ M1 for the j-th uit respect the v-th mission fo k-th type mission at small team

$Re\Delta t_k$ Reference duration for the k-th type mission

$Toc_{j,v}$ Time of task completion for the j-th uit on v-th mission of the k-th type

ntk Number of task assigned for k-th type mission at t time

$M1_{\mu_k(t)}$ Average readiness fot eh k-th type mission at t time

- M2: Operational Effectiveness: Assesses the reduction in operational effectiveness caused by cognitive attacks, measured by the quality of mission achievements.

$$M2F_{j,dmg}(t) = \max\left(\min\left(DMG_j(t)/(t), 200\%\right), 0\right)$$

$$M2F_{\mu_{dmg}}(t) = \frac{1}{nu}\sum_{i=1}^{nu} M2Fj_{dmg}(t)$$

$M2F_{j,dmg}(t)$ M2 Fighting computed for the j-th unit respect the damages produced until t time at small team level at t time

Dmg(t) Damages produced by the j-th unit until time j

ReDmg Reference Damages to be created over time unit

Nu Numebr of units

$M2F_{\mu_{dmg}}(t)$ Average effectiveness in fighting at t time

- M3: Vulnerability to Physical Attacks: Analyzes

increased vulnerability to physical attacks when cognitive attacks divert military personnel's attention, measured by unit damages under fire.

$$M3C(t) = \sum_{j=1}^{nu} Casualties\ j(t)$$

M3C(t) M3 Casualties computed for each j-th units up to t time

Nu Number of units

- M4: Information Security: Examines compromised information security due to cognitive or cyber attacks, measured by the number of information breaches and their operational impacts.

$$M4g(t) = \frac{1}{nug}\sum_{i=1}^{nuag} ConfLevel\ i(t)$$

$$M4\mu(t) = \frac{\sum_{i=1}^{ng} M4i(t)\ Force_i(t)}{\sum_{i=1}^{ng} Force_i(t)}$$

$M4g(t)$ Average Confidentiality Level within g-th group at t time

$ConfLevel_i(t)$ Current level of Confidentiality of the i-th unit at t time

$nuag$ number of units aggregated to group g

ng Number of group

$M4\mu(t)$ Weighted Average of Confidentiality at t time balanced based on each Group Force

$Forceg(t)$ Force of the Group g based on the sum of the forces of each of its units

- M5: Decision-Making Process: Investigates impaired decision-making resulting from cognitive attacks, measured by delays and effectiveness in decision-making.

M5T(t) = $\sum_{i=1}^{ndCOM} TimeToDecidedCOM_i$

M5C(t) = $\sum_{i=1}^{nuCOM} Casualties_i(t)$

ndCOM Number of Decision of Commander COM at t tie

nuCOM Number of Unities under Commander COM

TimeToDecide Time taken to finalize decision by Commander COM for i-th decision

$$M5U(t) = k_{M5T}M5T(t) + k_{M5C}M5C(t)$$

$M5U(t)$ Unified M5 combining axchievement level and timely decisions

k_{M5T} Coefficients for a weighed sum of M5U

- M6: Society Resilience to CW Actions: Studies the impact of cognitive attacks on societal perceptions and trust in military structures, measured by changes in trust and support for NATO and its member nations.

$M6k\ (t) = \sum_{i=1}^{npop} \boldsymbol{Trustinessi\ k(t)}$

M6k (t) Trustiness of the k-th population element respect the k-th interest group (i.e. alliance, military command, Nation A, B,C) at t time

An Overall Resilience is evaluated as weighted sum of the M6k of the crucial interest group identified as crucial for Society Resilience; the ktk factors are used to weight the sum.

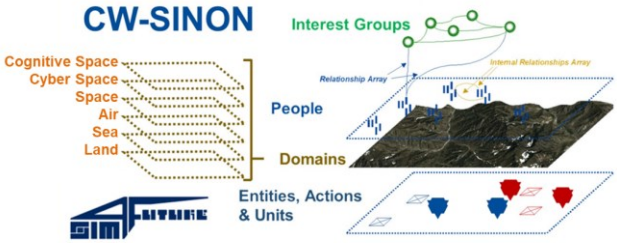

Fig.2 CW-SINON Layers

In CW-SINON, virtual humans are interconnected through social networks based on family and friendship ties, which evolve alongside population growth and area characteristics. These connections, influenced by the Health Belief Model (HBM), impact behaviors such as requiring a virtual human to undergo a stress test when their friend is injured. Emotional states like fear or stress could also transfer between connected individuals, depending on their status and leadership roles.

Additionally, virtual humans are linked to media outlets, including broadcast, print, and social media, based on their demographic traits. The likelihood and intensity of these connections vary by age, nationality, and personal characteristics. For example, a teenager may have a stronger connection to Instagram or TikTok compared to an older adult, and a Croatian virtual human may engage with more press news than a Serbian one. These media connections shift as the scenario evolves, such as losing TV or internet access, and are vulnerable to Broadcast, Print, and Social Media (BPSM) attacks, which alter perceptions of events.

Moreover, troops in the scenario develop relationships with the local population, including friendships, business ties, and other connections. These relationships influence the outcomes of kinetic, cyber, and BPSM actions, further affecting the virtual human behavior model (HBM). Links between virtual humans from different factions were also introduced, though at low initial percentages, allowing for future expansion in scenarios where cultural, religious, and historical backgrounds create deeper social mixes. CW-SINON lays the groundwork

for more complex interactions in future scenarios.

4. Experimentation

In the experimentation phase, we employed extensive ANOVA (Analysis of Variance) and Design of Experiments (DOE) to perform comprehensive sensitivity analyses within the proposed scenarios. These analyses were conducted across five distinct vignettes, each designed to test different aspects of cognitive warfare and human behavior modeling.

To ensure the robustness of our simulation results, we conducted ANOVA on replicated runs by varying the random seeds. This approach allowed us to determine the optimal simulation duration needed to achieve reliable results and to define the number of replications required to obtain a stable confidence band. Specifically, we analyzed the Mean Squared Prediction Error (MSpE) in relation to the simulation run duration and the number of replications. MSpE was used to evaluate the variance evolution concerning the number of replications obtained under the same boundary conditions, with only the random seeds being altered. This was applied to each j-th Y output, representing a target function.

The DOE methodology selected for our study was the Central Composite Design (CCD), which involves executing a factorial design with replicated runs at the center of the experimental range. This design allowed for a comprehensive exploration of the input space and facilitated the assessment of interactions between various factors influencing the simulation outcomes.

The simulation scenarios were designed to investigate the complexities of cognitive warfare, incorporating traditional and advanced elements such as operations with traditional assets, unmanned robotic systems, SOPs, snipers, IEDs, and cyber attacks across multiple domains. The Human Behavior Models (HBM) and cognitive warfare elements were particularly intricate, and the Intelligent Agents (IA) demonstrated the ability to fully control scenario dynamics by acting and reacting realistically within the simulation environment. This included interactions among Blue and Red forces, as well as neutral entities and local populations.

The human factors integrated into the simulation included over 26 variables, which were used as initial settings and independent variables to represent dynamic factors influencing scenario evolution under different hypotheses or courses of action (COAs). Despite the complex mutual interdependencies, the simulation consistently generated realistic behaviors, as confirmed by ANOVA and experimental analysis.

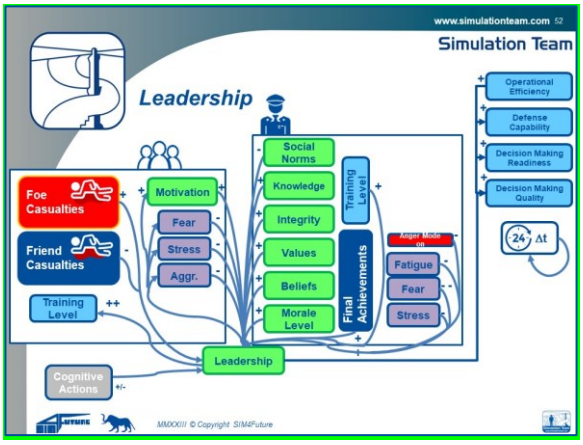

Fig.3 Example of HBM: Leadership

5. Conclusions

This project confirmed the potential of using simulation as a foundational element of a strategic engineering approach. Our simulations provided valuable insights into future developments, the influence of actions, and alternative decision-making processes. The simulations were capable of estimating consequences, target functions, costs, casualties, direct and indirect effects, second-order effects, and associated risks. These runs were based on different hypotheses and the outputs of data analytics, which characterized the situation, population, and force status, highlighting current vulnerabilities and the effectiveness of ongoing cognitive actions.

Within this framework, AI and machine learning were employed to refine the parameters of data analytics algorithms and the HBM and simulation models. Machine learning techniques were used to compare estimations against real-world situation evolutions, continuously improving the accuracy and reliability of the simulation.

Overall, the extensive experimentation and analysis demonstrated the robustness and versatility of the CW-SINON simulator in replicating and understanding the impacts of kinetic, cyber, and cognitive attacks in modern conflict scenarios. The results underscore the importance of simulation as a strategic tool for decision-makers, providing a detailed and dynamic understanding of complex warfare environments.

References

Bruzzone, A. G., Gotelli, M., Giovannetti, A., De Paoli, A., Ferrari, R., Pedemonte, M., ... & Frosolini, M. (2023). Strategic Engineering for Decision Making during Urban Crises.

Bruzzone, A. G., & Massei, M. (2017). Simulation-based military training. *Guide to Simulation-Based Disciplines: Advancing Our Computational Future*, 315-361.

Bruzzone, A., Massei, M., Longo, F., Poggi, S., Agresta, M., Bartolucci, C., & Nicoletti, L. (2014, April). Human behavior simulation for complex scenarios based on intelligent agents. In *Proceedings of the 2014 Annual Simulation Symposium* (pp. 1-10).

McCulloh, T., & Johnson, R. (2013). Hybrid warfare (p. 0155). JSOU Press.

Hoffman, F. G. (2014). Hybrid warfare and challenges. In Strategic Studies (pp. 329-337). Routledge.

Backes, O., & Swab, A. (2019). Cognitive Warfare. The Russian Threat to Election Integrity in the Baltic States, Cambridge: Belfer Center for Science and International Affairs.

Claverie, B., & Du Cluzel, F. (2022). "Cognitive warfare": The advent of the concept of "cognitics" in the field of warfare.

Hoffman, F. G. (2007). Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies.

Renz, B. (2016). Russia and 'hybrid warfare'. Contemporary Politics, 22(3), 283-300.

Marten, K. (2015). Putin's Choices: Explaining Russian Foreign Policy and the Ukraine Crisis. Washington Quarterly, 38(2), 189-204.

Paul, C. (2010). Strategic Communication: Origins, Concepts, and Current Debates. Praeger.

Ramsay, G. (2021). Weaponizing News: RT, Sputnik and Targeted Disinformation. Journal of Strategic Studies, 44(2), 286-309.

Libicki, M. C. (2020). Conquest in Cyberspace: National Security and Information Warfare. Cambridge University Press.

Pennycook, G., Cannon, T. D., & Rand, D. G. (2018). Prior exposure increases perceived accuracy of fake news. Journal of Experimental Psychology: General, 147(12), 1865-1880.

Kahneman, D. (2011). Thinking, Fast and Slow. Farrar, Straus and Giroux.

Lewandowsky, S., Ecker, U. K. H., & Cook, J. (2012). Misinformation and Its Correction: Continued Influence and Successful Debiasing. Psychological Science in the Public Interest, 13(3), 106-131.

Narula, S. (2004). Psychological operations (PSYOPs): A conceptual overview. Strategic Analysis, 28(1), 177-192.

Tversky, A., & Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability. Cognitive Psychology, 5(2), 207-232.