



From Drones to Deepfakes: Non-Kinetic Warfare Trends in West Asia and Strategic Lessons for India

Gopal Ji Rudra¹

Research Scholar, Department of Defence and Strategic Studies,
K. S. Saket P.G. College, Ayodhya, Uttar Pradesh,

Dr. Ashish Vikram Singh²

Assistant Professor, Department of Defence and Strategic Studies
K. S. Saket P.G. College, Ayodhya, Uttar Pradesh,

DOI : <https://doi.org/10.5281/zenodo.21675507>

ARTICLE DETAILS

Research Paper

Received: 26-05-2026

Accepted: 30-06-2026

Published: 15-07-2026

Keywords:

Deepfakes, Disinformation, Drone warfare, Hybrid warfare, India's strategic doctrine, Non-kinetic warfare, West Asia conflict

ABSTRACT

This study examines with the changing nature of war in West Asia from “old war” to “new war” – from kinetic to non-kinetic, and from “war of arms” to “war of minds.” The first aim of research is to examine the impact of new non-kinetic instruments on the changing regional security landscape in the West Asia, with a focus on the policies and actions of Iran, Israel and the Gulf countries. The study is of qualitative and interdisciplinary nature, using a case-study analysis, strategic-security literature, policy documents and the current developments of the conflict in the region. The paper focuses on the extent to which the boundaries between war and peace, between state and non-state actors and between military and political have been increasingly intermingled in the last ten years due to the growing use of unmanned aerial systems, cyber-attacks on critical infrastructure, and the use of AI for disinformation campaigns. The results demonstrate that non-kinetic warfare is becoming an effective and disruptive means of strategic competition, with both state and proxy warfare wielders

Disclaimer: The opinions, interpretations, conclusions, recommendations, analyses, and statements expressed in this research article are solely those of the author(s) and do not reflect the views, policies, or positions of the Publisher, Chief Editor, Editors, Editorial Board, Reviewers, or their affiliated institutions. The author(s) are solely responsible for ensuring the originality, authenticity, and integrity of the manuscript and for ensuring that it is free from plagiarism, AI-generated content, copyright infringement, data falsification, and any other form of academic misconduct.

capable of shaping the opponent without resorting to overt conventional conflict. The study also identifies the combination of cyber, drone and cognitive warfare as a contributing factor to sparking strategic instability in West Asia while also redefining the nature of deterrence mechanisms. The paper concludes that these emerging trends in conflict have important implications for the national security of the Indian state in terms of cyber resilience, indigenous technological capability, information security, and multi-domain defence readiness. Hybrid warfare is a tactic that is increasingly becoming a defining feature of future warfare, especially in the West Asian experience.

Introduction

The current twenty first century warfare has changed beyond a shadow of a doubt from the traditional military confrontation to a technologically advanced non kinetic warfare. Old ideas of warfare through territorial conquest and conventional armies and direct military combat are giving way to cyber operations, information warfare, artificial intelligence, electronic warfare, and autonomous systems. These new techniques have begun to erase the lines separating war from peace, combatants from civilians and the real and virtual worlds. Non-kinetic warfare provides states and non-state actors with a cost-effective and deniable way of accomplishing strategic goals without engaging in direct conventional warfare. This shift is more clearly seen in West Asia, where geopolitical competition, religious differences and resource politics have historically played a significant role. The region has seen an increase in the use of drones, cyber warfare, digital propaganda and disinformation as weapons of strategic competition since the start of the Arab Spring in 2011. Iran, Israel and the Gulf powers have now been making a significant investment in the use of hybrid warfare tactics using advanced technologies with the use of conventional deterrence. Meanwhile, non-state entities like Hezbollah and the Houthis have also shown how the threat posed by low-cost drones and information networks can be a match for more powerful military forces. Given India's strategic, economic and energy interests in West Asia, these developments hold great significance for India. The study thus explores how drones, cyber operations and information warfare are changing the security landscape in the region and their impact on India's national security and multi-domain defence capabilities.

Research Methodology



The study relies on qualitative research, analytical and descriptive approaches to explore the changing aspects of non-kinetic warfare in West Asia, including cyber warfare, artificial intelligence warfare, drone warfare, information warfare, and hybrid warfare. The research is largely secondary, with academic journals, books, government reports, policy papers, strategic affairs publications and reports by reputed think tanks like the Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA), RAND Corporation, Brookings Institution, Carnegie Endowment for International Peace and the Observer Research Foundation (ORF) being the primary sources consulted. Relevance and accuracy has also been ensured using credible news reports, documents from international organizations as well as scholarly databases. A comparative case study approach has been used in the study, with the countries of Iran, Israel and selected countries of the gulf region, because of their growing engagement in the field of cyber operations, drones, technological strategic competition, and so on. The time frame of the research covers developments from 2010 to 2025, including the Arab Spring, cyberattacks on critical infrastructure, and the growing use of AI-driven technologies in regional conflicts. Strategic and Geopolitical interpretation is applied to the analysis in order to understand the implications of non-kinetic warfare for the regional stability and India's national security. This study, however, has limitations due to limited information access to classified documents and the advent of new technologies.

Conceptual Framework: Understanding Non-Kinetic Warfare

The non-kinetic warfare is a term that is used to denote the application of non-physical capabilities, i.e. cyber, informational, electronic and psychological, to achieve strategic goals without a physical fighting. Non-kinetic tools are aimed at cognition, communication systems and critical infrastructure unlike kinetic operations, which are based on physical destruction (Kello 2017).

Rapid Evolution of Non-Kinetic Warfare.

Non-kinetic warfare has its origins in the information-age war and the network-centric operations. The essence of this change is represented by the concept introduced by Joseph Nye the soft power with hard effects, the possibility to influence the results by means of persuasion, control of the narrative, and domination over technology instead of brute force (Nye 2011). The convergence of cyber capabilities, artificial intelligence, and autonomous systems has resulted in a phenomenon known by military theorists as hybrid or multi-domain warfare- where digital, informational, and psychological planes of power are synchronized with conventional forms of power. The conflicts witnessed in West Asia mostly with Iran, Israel and Saudi Arabia, are a perfect example of such a synthesis.



Hybrid Warfare Theory

The term Hybrid Warfare came into use after the Cold War and has been gaining traction since the wars in Iraq, Afghanistan, Georgia, Crimea and Ukraine, among others. Frank Hoffman is the most prominent scholar of this concept. Hoffman, in his ground-breaking book *Conflict in the 21st Century: The Rise of Hybrid Wars* (2007), defines hybrid warfare as a combination of the use of conventional weapons, irregular tactics, terrorism, cyber warfare and criminal action, conducted simultaneously and adaptively by state and non-state actors. But today's enemies are not just shooting at you on the battlefield, they're using all tools of war in all the domains –soft and hard, to exploit your weaknesses,” Hoffman said. Hybrid warfare is a concept that merges the borders of war and peace, military and civilian targets, and state and non-state actors. It's not just about taking over a territory and it's not just about fracturing the social fabric and it's not just about breaking people's psyches, either. The framework has particular relevance to the Russia's use of force and manipulation in the countries of Eastern Europe and the Indo-Pacific region, as well as for the new and growing role of disinformation campaigns and cyberattacks in international politics. The analysis of this research has been enhanced by Hoffman's theory as it provides an explanation for how modern conflicts have become a combination of military force, information manipulation, cyber and psychological operations all united by a single strategy.

Cyber Deterrence Theory

Cyber deterrence is an application of classical deterrence theory in cyber space. But according to scholars, cyberspace has certain characteristics that make it difficult to apply traditional deterrence measures. Martin Libicki says that cyber deterrence is hard because:

It is often hard to identify the perpetrator of a cyberattack, and The cost of cyber operations is relatively low, Non state actors may have sophisticated capabilities,

Damage from cyberattacks can be reversible and ambiguous, Limits for retribution are not set.

Libicki states that there are three predominant ways to deter cyber-attacks:

1. Deterrence by Punishment
2. Deterrence by Denial
3. Resilience-Based deterrence



Deterrence by punishment is a threat of punishment given to attackers. Deterrence by denial is achieved by making cyberattacks less effective by augmenting the defence and cybersecurity infrastructure. The resilience-based deterrence is based on swift recovery and adaptation of the system after attacks. Thomas Rid is another significant researcher of cyber studies. In *Cyber War Will Not Take Place*, Rid argues against the notion that cyber conflict is “war” in the traditional Clausewitzian sense. He maintains that most cyber operations are akin to sabotage, espionage, or subversion; not direct warfare. Rid’s argument is significant because it brings clarity to the concept in the study of cyber. His approach is useful in clarifying the difference between cyber operations and traditional military warfare, as well as the political and psychological aspects of cyber operations.

Cognitive Warfare

Cognitive Warfare is one of the newest trends in the field of strategic studies. Cognitive warfare is defined as actions that target the cognition, emotions, perceptions and decision making of humans. People and cognitive warfare are different from traditional warfare, which is concentrated on physical infrastructures or military power. Its main goal is to influence beliefs, change perceptions, cause disintegration and erode the social fabric. NATO refers to the current usage of the term cognitive warfare in its contemporary literature as a new phase of information warfare and psychological operations in the digital age. It integrates:

1. Artificial intelligence
2. Big data analytics
3. Social media algorithms
4. Psychological operations
5. Disinformation campaigns
6. Behavioural manipulation techniques

The objectives of cognitive warfare are to sow divisions in society, to polarize public opinion, instill mistrust in institutions and to influence the decision-making process. Here civilians are legitimate targets in the information and perception war. From this perspective, Joseph Nye's definition of “soft power” and Libicki's “information warfare” framework are highly complementary to cognitive warfare theory, as both highlight the strategic value of influence, perception, and story.

Aspects of Non-Kinetic Warfare

Cyber and Electronic Operations:



These attacks are against communication systems, networks and data infrastructure. As an illustration, the Stuxnet virus (2010) which is said to be developed by the U.S and Israel has caused paralysis to the nuclear program in Iran and this is seen as a precedent of offensive cyber capabilities as tools of deterrence.

Unmanned Systems and Autonomous Systems:

The tangible aspect of non-kinetic warfare is realized by drones and systems powered by AI. They offer surveillance, strike, and deterrence capabilities with a minimal risk to the operators thus they allow asymmetric actors to fight better armies. Alone, these areas form a multi-layered, non-linear battlefield-a battlefield that re-invents deterrence and projection of power.

Case Studies: Non-Kinetic Warfare in West Asia.

The non-kinetic warfare in West Asia is indicative of the global evolution of hybrid warfare and the significant role cyber operations, drones, AI and information warfare have gained in today's strategic competition. The region has seen a shift in warfare from traditional warfare to technologically advanced warfare since the Arab Spring of 2011 which involved cyberattacks, digital propaganda and unmanned systems. The adoption of cheap technologies has allowed both state and non-state actors to engage in asymmetric action against more powerful adversaries. Israel, Iran and the Gulf nations are major players in this shift. Israel has built cutting-edge intelligence and cyber technology, and precision drone systems. The 2010 Stuxnet attack on Iran's nuclear facilities proved how cyber operations can be used to create strategic impact without use of military means. In response, Iran continued to advance its asymmetric warfare tactics via cyberattacks, proxy forces and drones. In 2019, Saudi Aramco was attacked with drones at Abqaiq and Khurais, this exposed the critical infrastructure and its impact on global oil production. Saudi Aramco was attacked with drones in 2019 in Abqaiq and Khurais, this exposed the critical infrastructure and its impact on global oil production. Drones, social media and psychological warfare are increasingly important and have been employed by non-state actors like the Houthis, Hamas and Hezbollah to affect regional conflicts.

Iran: Hack Power and Drone Diplomacy.

The Iranian strategy is an amalgamation of cyber warfare, proxy warfare and the spread of drones. After the Stuxnet attack, Tehran has expanded its cyber departments within the Islamic Revolutionary Guard Corps (IRGC) activities against Israeli, Saudi, and American targets. In a provisional manner, the Saudi Aramco strike of 2019, which was executed with the assistance of drones and cruise missiles, paralyzed half of the oil production of Saudi Arabia and demonstrated that Iran did manage to perform some



types of strategic signaling by launching deniable operations (Sanger and Perlroth 2019). The cyber-attack on Iranian energy grids, not to mention the disinformation being applied on the Gulf states are signs that it wants to balance the asymmetry in the region in a clever manner through technology rather than through equality.

Israel: Creative Edge and Cognitive Warfare.

The Israeli defence innovation system is a system that brings together the artificially intelligent cybersecurity and public diplomacy into a single online method to the country. The Israeli Defence Forces (IDF) apply AI in the Guardian of the Walls (2021) operation in terms of the prioritization of the targets, narrative management of the conflicts, and real-time threat analysis. Its partnership with the commercial technology sector has created a security-technology complex, which strengthens the deterring orientation of Israel and sells non-kinetic equipment to the rest of the world (Inbar 2022). The policy of Israel is that of cognitive dominance or to dominate the narratives in the domestic and international arenas to ensure legitimacy and deterrence.ⁱ

Online Surveillance and Strategic Communication: the UAE and Saudi Arabia.

The Gulf kingdoms have incurred a massive cost on cyber defence, AI regulation, and information control. Saudi Arabia and UAE are engaged in mass surveillance of the digital realm with the assistance of Western and Israeli surveillance technologies in spaces to anticipate and affect the outside discourse (Feldstein 2021). Their propaganda online networks introduce projects of leadership such as Vision 2030 as an indication of modernity and change as they disapprove critical reports by Iran or western media. The creation of the AI Ministry in the UAE shows its wish to unite the control of the governance, security, and technology. Non-State Actors: Hezbollah, Hamas and the Houthis. The non-state groups have democratized the non-kinetic tools, and they employ drones, encrypted messages, and internet propaganda to generate oversized effect. The Houthis have continued to launch attacks on Saudi infrastructures using Iranian-supplied drones in Yemen. Hezbollah and Hamas have digital recruiting, psychological warfare, and propaganda-spreading systems. The situation underscores the fact that information asymmetry is a force multiplier taken by non-state actors.

Key Lessons for India

Not only has the rise of non-kinetic warfare but also the integration of a blend of non-kinetic and kinetic warfare in West Asia has significant implications for India's national security policy. India's economic, energy, and strategic presence in the region has increased and threats like cyber warfare, drones,



artificial intelligence and disinformation have emerged that have to be given more weight. The key takeaway is that cyber security is an important topic, as the attacks on the critical infrastructure in West Asia have shown how vulnerable digital and energy systems are. Institutions like the Defence Cyber Agency have been strengthened and cyber security policies have been drawn up in India, however in the current times, there is a need to continuously upgrade them. One of the other major take-aways is the increasing strategic importance of drones and autonomous systems. Iran, Israel and the Houthis are all employing low cost drones, which are effective for modern warfare. India has thus been investing in its indigenous drone and anti-drone capabilities via DRDO programmes. Furthermore, the proliferation of AI-generated disinformation and digital propaganda underscores the importance of enhancing cognitive security and information resilience in India's national security landscape.

Adopting Technological Adaptation and Indigenous Innovation.

The conventional deterrence of land, air and sea dominance has always been the focus of India defence preparedness. Nonetheless, the case of West Asia shows that the modern concept of deterrence can also be characterized by technological agility and ecosystems of innovation. Other states such as Israel have integrated artificial intelligence (AI), data analytics, and unmanned systems into their defence-industrial systems, allowing them to make decisions in real-time and be precise in their operations. The fact that even the low-cost drones and cyber tools are being indigenized by Iran is another sign that strategic impact is no longer about the high-end platforms but adaptive innovation. In the Indian case, it will have to accelerate efforts such as the Defence Cyber Agency (DCA), Defence Space Agency (DSA) and the Intelligent Defence AI Council (IDAC). These should not just be symbolic of the bureaucracy but integration. The process of institutionalization of the collaboration between the state and the businesses must be conducted in such a way that the Indian start-ups and research centres could cooperate with each other in terms of the creation of independent systems, counter-drone technologies, and AI-enabled early-warning systems. The formation of a National Centre of Unmanned Systems under the DRDO or IN-SPACE would provide one platform in the development and management of the drone forces and anti-drone forces.ⁱⁱ

Cognitive and Narrative Resilience Development.

Perceptions are receiving more targets of non-kinetic warfare instead of positions. Gaza, Yemen, and Syria conflicts show that such manipulation of information and online propaganda can affect the masses, destroy the legitimacy of the opponent, and impact the outcomes of the diplomacy. India is a well penetrated democracy that is highly social-media prone and is yet vulnerable to such mode of thinking. The first action towards being resilient involves accepting that information space is one of the strategic domains. To monitor



the patterns of disinformation, stockpile the efforts of various ministries, and disseminate truthful narratives in the event of crisis, India needs an institutional mechanism, say a National Cognitive Security Directorate (NCSD). The Press Information Bureau fact-checking agency should also be turned into a cross-agency communication station capable of doing real-time digital diplomacy. Moreover, the society is also involved in cognitive defence. Media literacy campaigns especially in local languages should be incorporated in the education curriculums to immunize the citizens against fake news and deepfakes. Index Digital Hygiene Digital awareness and information resilience between states could be added to the governmental Digital India mission, which is a regular assessment of information and cyber-awareness.

Multi-domain Operation by means of Institutional Integration.

Non-kinetic war injects the border between the military and the civilian. It is possible to have an economic, an environmental, and political effect simultaneously when an oil infrastructure target is struck by a drone. Therefore, the national security framework of India must be switched to multi-domain coordination as opposed to departmental silo coordination. The institution of a Chief of Defence Staff (CDS) and the modern changes in the theatres command are crucial, yet they must incorporate the premises of cyber, space and information warfare explicit. Joint Non-Kinetic Warfare Command (JNKWC), would be in a position to integrate military, intelligence, and diplomatic instruments of statecraft. Such a form of an institution would not only react to the threats presented by the outside world but would also assist India to disseminate power as far as strategic communication, digital diplomacy and technological partnerships are concerned.

Ensuring the Enhancement of Strategic Partnerships in West Asia.

Strategic degree of engagement in West Asia has increased within the frameworks of I2U2 (India-Israel-UAE-US) and bilateral military alliance with Oman, Saudi Arabia and UAE. However, the cooperation must alter not only the logistics and trade, but also to co-development of digital defence capabilities. The Israeli example of cyber start-up ecosystem and UAE example of artificial intelligence control can teach India some valuable lessons. Such collaborative exercises, as Blue Flag (including Israel) and Desert Eagle (including the UAE), should have modules, which are not kinetic, the modules, which simulate experience of cyberattacks, information operations, and swarm of drones. The engagement of India in the activities of the Gulf think tanks and technology facilities can also result in the establishment of the norms in the responsible use of AI, cyber deterrence, and digital ethics.

The Non-Kinetic Defence Doctrine is to be institutionalized

Though Defence Cyber Strategy (2023) of India acknowledges the new digital threats, a detailed National Non-Kinetic Warfare Doctrine is still lacking. This kind of doctrine ought to establish the levels of deterrence, the response structures, and attribution systems of cyber or cognitive attacks. It should map out how the military, intelligence and civilian resources need to be combined to counter non-kinetic aggression. The legal and moral aspects of non-kinetic retaliation (which includes the matters of sovereignty, data privacy, and international conventions) should be also explained in this doctrine. To boost deterrence and legitimacy in the international cyber domain, India can make sure that its national legislations, including the Digital Personal Data Protection Act (2023), should not be inconsistent with the objectives of defence.

The Human Resources and Strategic Culture Empowerment.

Technology does not provide the question of resilience and must be driven by a flexible and competent work force. India can enhance graduates by putting more emphasis on training on the field of cybersecurity, AI ethics, behavioural psychology, and narrative studies in education institutions such as the National Defence college (NDC) and IITs. A Defence Technology Fellowship between the military, academia and external innovators would also yield new breed of so-called strategic technologists but again there is need to redefine the Indian strategic culture to be aware of how the next war could start not by a shot, but a viral hashtag or a deep fake video. To prepare future leaders to operate in multidomain settings, the military training centres should include classes on cognitive warfare, digital ethics and impression management.

Policy Recommendations

I. Form a National Non-Kinetic Warfare Command:

- a. Standardise the cyber, electronic, and cognitive activities within the Ministry of Defence.

II. Invest into Research and Artificial Intelligence:

- a. Enhance the degree of collaboration between the DRDO and the academia as well as the private industry in a bid to develop technologies on anti-drone, anti-cyber-attacks and also on those against the deepfakes.

III. Introduction of a cognitive security centre within the country:

- a. Influential activities, disinformation, and algorithmic propaganda against the information system in India are surveilled

IV. Enhance Strategic Alliance in West Asia:

- a. Arrange tripartite talks with Israel, the UAE, and Saudi Arabia regarding the security of cyber norms, export controls on drones, and AI control.



V. Develop a Resilience Doctrine:

- a. Introduce digital hygiene, data protection, and public awareness as a part of the national security policy of India to train the society about psychological and informational warfare.

Conclusion

The introduction of non-kinetic warfare is a major shift in today's security landscape. The study shows that West Asia has become an important laboratory of modern conflict in which the use of drones, cyber operations, artificial intelligence and information warfare are becoming an integral part of statecraft and strategic competition. The experience of Iran, Israel and the Gulf states shows how both state and non-state actors are using non-kinetic means to pursue political and military ends, other than through conventional military confrontation. The results of the study suggest that the use of UAS, cyberattacks against critical infrastructure, and the creation of disinformation campaigns using artificial intelligence has changed the concepts of deterrence, conflict escalation, and strategic stability. The non-kinetic warfare has made the line between war and peace indistinct as it has extended conflict to digital, informational, and cognitive space. The study also reveals technological asymmetry and information manipulation are increasingly playing a key role in hybrid warfare in West Asia. These shifts have significant strategic ramifications for India, in terms of its energy needs, economic stakes, and diaspora ties with West Asia. In the new strategic landscape, improving the capabilities of cyber resilience, indigenous technology, AI, and multi-domain defence capability will be crucial to solving new security challenges. The study is limited because it has been conducted with qualitative case-study analysis and because technological warfare is in a state of flux, creating new developments that are not considered in the study. The influence of autonomous weapons, cognitive warfare on democratic societies, strategic decision-making processes, as well as private technology corporations and quantum technologies will be further explored in future research.

References:

-
- Aryan, S., & Rahmani, R. (2021). Cyber operations and statecraft: Iran's asymmetric digital warfare. *Journal of Strategic Security*, 14(3), 45–67.
- Bachmann, S. D., & Gunneriusson, H. (2015). Hybrid wars: The 21st-century's new threats to global peace and security. *Scientia Militaria: South African Journal of Military Studies*, 43(1), 77–98.
- Bergen, P., & Rothenberg, D. (2021). *The future of drone warfare*. New America Foundation Press.



- Binnendijk, H., & Marlin, T. E. (2020). *Artificial intelligence and international security*. Center for Transatlantic Relations.
- Clausewitz, C. V. (1976). *On war* (M. Howard & P. Paret, Eds. and Trans.). Princeton University Press. (Original work published 1832)
- Farwell, J. P. (2014). *Persuasion and power: The art of strategic communication*. Georgetown University Press.
- Freedman, L. (2017). *The future of war: A history*. PublicAffairs.
- Giles, K. (2016). *Handbook of Russian information warfare*. NATO Defense College.
- Gray, C. S. (2016). *The strategy bridge: Theory for practice*. Oxford University Press.
- Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars. *Potomac Institute for Policy Studies*, 1–72.
- Inbar, E. (2022). *Israel's security doctrine in the age of technological innovation* (Policy Paper No. 203). Begin-Sadat Center for Strategic Studies.
- Kaura, V. (2024). *India–West Asia strategic convergence: Technology, security, and diplomacy*. Raisina Dialogue Papers, Observer Research Foundation.
- Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.
- Manohar Parrikar Institute for Defence Studies and Analyses. (2023, October). *Hybrid warfare and cyber conflicts in West Asia* (Issue Brief). MP-IDSA.
- Ministry of Defence, Government of India. (2023). *India's defence cyber strategy* (White Paper). Integrated Defence Staff.
- Nye, J. S., Jr. (2011). *The future of power*. PublicAffairs.
- Observer Research Foundation. (2024, June). *Iran and Israel: The expanding shadow war*. ORF.
- Raman, S. (2022). Cognitive warfare and strategic communication in Indian security policy. *IDSA Journal of Defence Studies*, 16(2), 54–56.



Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The weaponization of social media*. Houghton Mifflin Harcourt.

United Nations Institute for Disarmament Research. (2023). *Artificial intelligence, autonomous weapons, and international security*. UNIDIR Publications.

Valeriano, B., Jensen, B., & Maness, R. C. (2018). *Cyber strategy: The evolving character of power and coercion*. Oxford University Press.

Weimann, G. (2015). *Terrorism in cyberspace: The next generation*. Columbia University Press.

Westcott, N. (2021). *The new digital battlefield: Information warfare and global security*. Routledge.