JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

The Dual Role of Technology in International Relations: Coercion, Diplomacy, and Ethics in the Iran–US–Israel Conflict

Benson Onyango Nalo
Senior Lecturer, International Relations, Security and Strategic Studies
Pioneer International University, Nairobi Kenya

Abstract : Science and technological innovations have become central determinants of international relations, reshaping power dynamics, diplomatic strategies, and normative debates. This paper examines the triangular conflict among Iran, the United States, and Israel to analyze how technological innovation functions both as an instrument of coercion and a medium of diplomacy. Using a qualitative case study approach, the research triangulates primary sources such as the Joint Comprehensive Plan of Action (JCPOA) and International Atomic Energy Agency (IAEA) reports, alongside secondary sources and technical analyses of cyber operations and missile systems. Findings reveal that nuclear science plays a dual role in the international security arena. First, it intensifies rivalry by raising existential stakes—as illustrated by Iran's uranium enrichment programs and Israel's preemptive security doctrines. Second, it enables compromise through technical frameworks for negotiation, exemplified by the JCPOA's verification mechanisms. Cyber warfare demonstrates coercion through technological superiority, such as the Stuxnet attack on Iranian nuclear facilities, while simultaneously exposing vulnerabilities that demand governance. Missile defense systems, including Israel's Iron Dome, highlight survival imperatives and arms race dynamics. Meanwhile, surveillance technologies and artificial intelligence extend state power but provoke ethical debates about sovereignty, legality, and civilian protection. The study concludes that science and technology are not neutral tools but socially constructed instruments that redefine legitimacy and threat perceptions. The Iran–US–Israel conflict underscores the inadequacy of existing governance frameworks in cyber, missile, and AI domains, and highlights the need for integrated scholarship bridging material, institutional, and normative dimensions. Comparative lessons from US–China technological competition and Russia–Ukraine cyber and drone warfare suggest that the dual role of technology—intensifying conflict while enabling compromise—is a general feature of contemporary global politics. Future research should explore cross-domain integration, normative debates, and governance of emerging technologies such as quantum computing and biotechnology, which are poised to further transform the landscape of international security.

Index Terms - International Relations, Science and Technology, Iran–US–Israel Conflict, Nuclear Deterrence, Cyber Warfare, Missile Defense, Surveillance, Artificial Intelligence

I. INTRODUCTION

Science and technological innovations have consistently reshaped the trajectory of international relations, redefining how states perceive threats, construct alliances, and pursue both war and peace. From the invention of gunpowder to the nuclear revolution, technological innovation has altered the balance of power and transformed diplomacy. In the twenty-first century, the accelerating pace of innovation has intensified this dynamic, producing new domains of contestation such as cyberspace, outer space, artificial intelligence, and missile defense. This paper argues that science and technology are not neutral tools but determinants of power, identity, and diplomacy, shaping both rivalry and negotiation in international politics.

The triangular conflict among Iran, the United States, and Israel provides a vivid case study of these dynamics. At the heart of this rivalry lies Iran's pursuit of nuclear capabilities, which Washington and Tel Aviv have consistently framed as existential threats. The Joint Comprehensive Plan of Action (JCPOA) of 2015 exemplifies how scientific thresholds—centrifuge capacity, enrichment levels, inspection protocols—became the language of diplomacy, translating technical details into political compromises (Katzman, Iran's Nuclear Program and the US Policy, 2019). At the same time, the collapse of the JCPOA revealed the fragility of science-based agreements, as Iran resumed higher enrichment levels, destabilizing regional security (Fitzpatrick, 2016).

Beyond nuclear science, cyber warfare has transformed the conflict. The Stuxnet attack of 2010, attributed to US–Israeli collaboration, sabotaged Iranian centrifuges and demonstrated that software could achieve strategic effects once reserved for conventional weapons (Zetter, 2014). Iran's subsequent investment in offensive cyber capabilities, targeting banks and infrastructure abroad, illustrates the paradox of innovation suggesting that new instruments of power simultaneously create new vulnerabilities (Tabatabai, 2019). Missile defense systems reinforce this asymmetry. For instance, Israel's Iron Dome and Arrow programs, developed with US support, provide strategic confidence by intercepting rockets and ballistic missiles, while Iran's pursuit of more advanced missiles exemplifies the realist logic of survival through technological superiority (Cordesman, 2014).

Surveillance and artificial intelligence further compress decision-making time and extend the geographical reach of state power. Drone strikes against Iranian commanders illustrate how precision technologies enable deterrence for some actors while symbolizing aggression for others (Byman, 2013). These practices raise ethical and legal dilemmas, underscoring the constructivist insight that technology acquires meaning through norms and identities (Finnermore & Hollis, 2016).

By situating the Iran–US–Israel conflict within the theoretical traditions of the three mainstream international relations theories-realism, liberalism, and constructivism, this paper demonstrates how technological innovation is inseparable from geopolitical rivalry. Nuclear enrichment, cyber sabotage, missile defense, and AI surveillance are not merely technical domains; they are deeply political, shaping perceptions of threat, legitimacy, and cooperation. The case is emblematic of broader global trends, from US–China competition in artificial intelligence to Russia–Ukraine cyber operations, highlighting the urgent need for governance frameworks that can keep pace with scientific advancement. Ultimately, science and technology function simultaneously as instruments of coercion and mediums of diplomacy, making them central to the future of international relations.

By integrating realism, liberalism, and constructivism, this study contributes to scholarship on how science and technology shape international relations in the twenty-first century. Realism emphasizes material power and survival, Liberalism highlights cooperative potential, and Constructivism underscores normative meaning. Applied to the Iran–U.S.–Israel conflict, these perspectives reveal how technological innovation redefines power, diplomacy, and legitimacy. This integrated framework provides a holistic foundation for both theoretical inquiry and policy engagement, advancing the study of deterrence and technological rivalry beyond fragmented approaches.

II. LITERATURE REVIEW: SCIENCE, TECHNOLOGY AND DETERRENCE

The intersection of science, technology, and international relations has long attracted scholarly inquiry, though often in fragmented domains such as nuclear proliferation, cyber security, missile defense, or surveillance. To understand the Iran–US–Israel conflict, it is necessary to situate these technological dimensions within broader theoretical traditions—realism, liberalism, and constructivism—while engaging with empirical studies that highlight the interplay between innovation and power. This review synthesizes key contributions across these domains, identifies gaps, and establishes the foundation for a holistic analysis.

Realist scholarship has traditionally emphasized material capabilities as the foundation of state power. Kenneth Waltz's stability thesis argued that nuclear weapons promote caution and reduce the likelihood of major war, pointing to the Cold War balance between the United States and the Soviet Union as evidence that mutual arsenals prevented direct confrontation (Waltz, 2012). Extending this logic, Waltz suggested that a nuclear armed Iran might stabilize the Middle East by deterring Israel and Saudi Arabia. In contrast, Sagan (1996) highlighted organizational risk, warning that technological complexity and bureaucratic weakness increase the danger of accidental escalation. The 1983 Soviet false alarm incident, when malfunctioning satellites signaled a U.S. strike, illustrates how organizational flaws can bring the world perilously close to nuclear war. From a realist perspective, Iran's nuclear program is therefore interpreted either as a stabilizing deterrent or as a dangerous source of instability.

Liberal theorists underscore the role of institutions and regimes in mitigating conflict and fostering cooperation. Keohane & Nye's (1977) concept of complex interdependence suggests that technological domains can encourage collaboration when states recognize mutual vulnerabilities. Arms control treaties, verification mechanisms, and organizations such as the International Atomic Energy Agency (IAEA) exemplify this logic. The Joint Comprehensive Plan of Action (JCPOA) provides a vivid case: uranium enrichment levels and centrifuge limits were codified into diplomatic compromise, balancing Iran's sovereignty with international security concerns (Katzman, 2015). In this view, technology becomes a diplomatic arena of negotiation, where verification and monitoring reduce mistrust and enable compromise.

Constructivist scholarship adds a normative dimension, emphasizing that technology acquires meaning through social interaction and identity. Wendt's (1999) insight that "anarchy is what states make of it" applies equally to technological innovation. Nuclear enrichment, cyber operations, or drone strikes are not inherently threatening; their meaning depends on identities and norms. For Israel and the United States, Iran's nuclear program symbolizes existential threat, rooted in historical enmity and narratives of survival. For Iran, enrichment represents sovereignty, resistance, and national pride. The contrasting global reactions to India's nuclear tests in 1998—framed as responsible assertion—versus North Korea's tests—framed as rogue defiance—illustrate how identical technologies acquire radically different meanings depending on context. Constructivists therefore interpret Iran's nuclear program less as a technical issue than as a symbolic struggle over legitimacy and identity.

Beyond nuclear science, cyber warfare introduces a new frontier of strategic innovation. The Stuxnet attack of 2010 demonstrated both the disruptive potential of cyber weapons and the vulnerabilities they expose. Realists interpret cyber capabilities as asymmetric tools of coercion, liberals stress governance gaps and the absence of robust regimes, while constructivists highlight the symbolic meaning of cyber operations, particularly Iran's framing of Stuxnet as humiliation and violation (Lindsay, 2013; Kello, 2017). Similarly, missile defense systems illustrate material rivalry: Israel's layered defense architecture, supported by the United States, reinforces deterrence, while Iran's missile development reflects realist survival logic. Liberals caution that missile shields may destabilize deterrence by incentivizing offensive proliferation, and constructivists emphasize their symbolic role in projecting sovereignty and resilience (Cordesman, 2014; Maloney, 2015). Finally, surveillance and artificial intelligence transform conflict by compressing decision making timelines and extending state power. Drone strikes exemplify precision but raise ethical dilemmas concerning sovereignty and civilian protection. Realists see these technologies as deterrence tools, liberals highlight regulatory gaps, and constructivists stress their symbolic meaning—deterrence for some, aggression for others (Byman, 2013; Singer, 2009).

Despite these insights, several gaps remain. First, deterrence studies are often siloed, treating nuclear, cyber, missile defense, and AI separately, with limited integration of how these domains interact in triangular rivalries such as US–Israel–Iran. Second, empirical depth in Middle Eastern cases is limited compared to Cold War and South Asian studies, with analyses often descriptive rather than systematically theorized. Third, normative and ethical dimensions—particularly how norms, identities, and legitimacy shape deterrence—are less developed compared to rationalist models. Finally, emerging technologies such as quantum computing, biotechnology, and hypersonic weapons are poised to reshape deterrence, yet scholarly engagement with these domains remains nascent.

This study fills these gaps by offering an integrated framework that combines realist insights into material survival and deterrence, liberal emphasis on institutions and cooperative regimes, and constructivist attention to norms and identity. It situates nuclear science,

cyber warfare, missile defense, and AI surveillance within a single analytical lens, demonstrating how technological innovation simultaneously intensifies rivalry and enables diplomacy. By grounding the analysis in the US–Israel–Iran conflict and linking it to broader global trends such as US–China competition and Russia–Ukraine cyber operations, the study advances deterrence scholarship beyond Cold War rationalist models. It contributes both theoretically—by bridging fragmented approaches—and empirically—by providing systematic depth in a critical Middle Eastern case.

Realism, Liberalism, and Constructivism in the US–Israel–Iran War

The study of science and technology in international relations requires a robust theoretical foundation. Realism, Liberalism, and Constructivism offer distinct yet complementary perspectives on how technological innovation shapes power, diplomacy, and governance. Each framework provides insights into the Iran–U.S.–Israel conflict, illuminating the ways in which nuclear science, cyber warfare, missile defense, and surveillance technologies redefine strategic calculations and normative debates.

Realism emphasizes the centrality of power and survival in an anarchic international system. States pursue technological superiority to secure their existence and deter adversaries. Waltz (2012) argued that nuclear weapons stabilize relations by deterring aggression, since the costs of conflict become prohibitively high. In the Iran–U.S.–Israel conflict, this logic is evident in nuclear deterrence and missile defense. Israel's development of the Iron Dome and Arrow systems, supported by U.S. funding, reflects realist priorities: survival depends on technological innovation that neutralizes adversary capabilities (Cordesman, 2014). Iran's pursuit of nuclear enrichment and ballistic missile development similarly reflects realist imperatives. By acquiring latent nuclear capability and advancing missile technology, Iran seeks to counterbalance Israel's technological edge and deter U.S. intervention (Eisenstadt, 2016). The cycle of innovation and counter innovation exemplifies the realist logic of arms races, where technological superiority is equated with security. Cyber warfare further illustrates realist dynamics: the Stuxnet attack of 2010, attributed to U.S.–Israeli collaboration, was designed to weaken Iran's nuclear program and preserve strategic advantage (Lindsay, 2013). In realist terms, technology is a weapon of coercion, deployed to alter the balance of power.

Liberalism offers a contrasting perspective, emphasizing cooperation through institutions, regimes, and interdependence. Keohane and Nye (1977) argued that complex interdependence creates incentives for collaboration, even in competitive environments. In the technological domain, liberalism highlights the role of arms control treaties, verification mechanisms, and international organizations. The Joint Comprehensive Plan of Action (JCPOA) exemplifies this logic, translating technical thresholds into diplomatic compromise. Centrifuge capacity, enrichment levels, and inspection protocols became the language of negotiation, reflecting liberal institutionalist principles (Katzman, 2015). By agreeing to limit enrichment and allow inspections, Iran sought sanctions relief, while the U.S. and Israel pursued assurances of non weaponization. The JCPOA demonstrates liberal optimism: technological disputes can be managed through cooperative frameworks. However, its collapse in 2018 underscores the fragility of such arrangements, revealing the limits of liberalism in the face of mistrust and domestic political pressures. Cyber governance further illustrates liberal challenges: international law struggles to regulate cyber operations, leaving gaps in accountability and enforcement (Deibert, 2013). Liberal approaches nonetheless emphasize the potential for multilateral frameworks to address these challenges, highlighting cooperation even in emerging domains.

Constructivism adds a normative dimension, emphasizing that technology acquires meaning through social interaction. Wendt (1999) argued that anarchy is socially constructed, shaped by identities and norms. Similarly, technological innovation is interpreted differently depending on narratives and perceptions. For Israel and the United States, Iran's nuclear program symbolizes existential threat; for Iran, it represents sovereignty and resistance. Technology thus becomes a socially constructed instrument, shaping legitimacy and threat perceptions (Tannenwald, 2007). Missile tests serve not only as demonstrations of capability but also as assertions of sovereignty and defiance. Drone strikes and targeted killings illustrate similar dynamics: for the U.S. and Israel, they symbolize precision and deterrence; for Iran, they represent aggression and violation of sovereignty (Boyle, 2013). Cyber operations such as Stuxnet also carry symbolic weight, embedding vulnerability into Iran's strategic imagination and reinforcing narratives of Western hostility. Constructivism further emphasizes ethical and legal debates surrounding emerging technologies. Autonomous weapons challenge principles of distinction and proportionality, raising questions about legitimacy and accountability (Crootof, 2015). Surveillance and AI driven analytics similarly provoke normative debates about privacy, sovereignty, and civilian protection. These issues illustrate how technology is embedded in social and normative frameworks that shape its meaning and acceptance.

Each theoretical framework offers valuable insights, but none alone fully captures the complexity of the Iran–U.S.–Israel conflict. Realism explains the pursuit of technological superiority and deterrence; Liberalism highlights cooperative potential through regimes such as the JCPOA; Constructivism underscores the social construction of legitimacy and the normative debates surrounding technology. Together, these perspectives provide a multidimensional lens for analysis. Nuclear science illustrates realist deterrence, liberal cooperation, and constructivist legitimacy. Cyber warfare demonstrates realist coercion, liberal governance challenges, and constructivist symbolism. Missile defense reflects realist survival imperatives, liberal arms control concerns, and constructivist narratives of sovereignty. Surveillance and AI highlight realist power projection, liberal legal frameworks, and constructivist ethical debates. The Iran–U.S.–Israel conflict thus exemplifies the need for integrated scholarship that bridges theoretical traditions.

By integrating realism, liberalism, and constructivism, this study contributes to scholarship on how science and technology shape international relations in the twenty first century. Realism emphasizes material power and survival, Liberalism highlights cooperative potential, and Constructivism underscores normative meaning. Applied to the Iran–U.S.–Israel conflict, these perspectives reveal how technological innovation redefines power, diplomacy, and legitimacy. This integrated framework provides a holistic foundation for both theoretical inquiry and policy engagement, advancing the study of deterrence and technological rivalry beyond fragmented approaches.

Conceptual Framework

This study develops a conceptual framework that integrates Realism, Liberalism, and Constructivism to explain how science and technology shape deterrence and diplomacy in the Iran–U.S.–Israel rivalry. Each tradition illuminates a distinct dimension of technological innovation, and together they provide a multidimensional lens for analysis.

Realist Dimension (Material Power and Survival)

Technology is treated as a strategic asset in an anarchic system. Nuclear enrichment, missile defense, and cyber operations are instruments of coercion and survival. For example, Israel's Iron Dome and Arrow systems embody realist imperatives of neutralizing adversary capabilities, while Iran's pursuit of latent nuclear capability and ballistic missiles reflects the logic of balancing against

superior rivals. Cyber operations such as Stuxnet further illustrate realist dynamics, where technology is deployed to weaken adversaries and preserve strategic advantage.

Liberal Dimension (Institutions and Cooperation)

Technology becomes a bargaining chip within cooperative regimes. The JCPOA exemplifies how scientific thresholds—centrifuge capacity, enrichment levels, and inspection protocols—were translated into diplomatic compromise. Liberalism highlights the potential of institutions like the IAEA to embed technical disputes within verification frameworks, reducing mistrust and enabling compromise. Yet the collapse of the JCPOA underscores the fragility of institutional solutions when trust and enforcement mechanisms fail, pointing to the limits of liberal optimism.

Constructivist Dimension (Norms and Legitimacy)

Technology acquires meaning through identity and narrative. For Israel and the United States, Iran's nuclear program symbolizes existential threat; for Iran, it represents sovereignty and resistance. Missile tests, drone strikes, and cyber operations are not merely technical acts but symbolic performances of legitimacy, defiance, or deterrence. Constructivism also foregrounds ethical debates: autonomous weapons challenge principles of distinction and proportionality, while AI surveillance raises questions of sovereignty, privacy, and civilian protection. These normative dimensions shape how technological practices are perceived and contested.



Applied to the Iran–U.S.–Israel conflict, this framework demonstrates that nuclear science, cyber warfare, missile defense, and AI surveillance cannot be understood in isolation. They simultaneously intensify rivalry, enable cooperation, and embody contested narratives. By bridging theoretical traditions, the framework provides a holistic foundation for analyzing how science and technology redefine deterrence and diplomacy in contemporary world politics.

III. RESEARCH METHODOLOGY

This study adopts a qualitative case study approach to examine the role of science and technological innovation in shaping international relations, with particular reference to the triangular conflict among Iran, the United States, and Israel. The case study method is well suited to this inquiry because it enables an in-depth exploration of complex phenomena within their real-world context (Yin, 2018). By focusing on a single but multifaceted conflict, the research integrates diverse technological domains—nuclear science, cyber warfare, missile defense, and surveillance—into a coherent analytical framework. This approach allows the study to capture both the material and normative dimensions of technological rivalry and diplomacy.

The research design is interpretive and explanatory. It seeks not only to describe technological developments but also to explain their impact on power relations, diplomatic negotiations, and normative debates. The inquiry is guided by three central research questions: how science and technology alter power relations in international conflicts; what lessons can be drawn from the Iran–US–Israel case for global governance; and how different theoretical perspectives—Realism, Liberalism, and Constructivism—illuminate the role of technology in international relations. Structuring the study around these questions ensures that empirical evidence is systematically linked to theoretical analysis (Creswell & Poth, 2018).

To enhance validity and reliability, the study relies on triangulation of primary, secondary, and technical sources (Denzin, 2012). Primary sources include official government statements, treaties, and international agreements, such as the Joint Comprehensive Plan of Action (JCPOA), United Nations Security Council resolutions, and International Atomic Energy Agency (IAEA) inspection reports (IAEA, 2016). Secondary sources consist of peer-reviewed journal articles, scholarly books, and policy reports from reputable think tanks such as the Brookings Institution, RAND Corporation, and Carnegie Endowment for International Peace. These provide analytical perspectives on nuclear proliferation, cyber warfare, missile defense, and surveillance technologies (Lindsay, 2013; Kello,

2017; Cordesman, 2014). Technical sources include cybersecurity analyses of the Stuxnet attack, missile defense evaluations, and literature on artificial intelligence ethics, which offer detailed insights into the scientific and technological dimensions of the conflict (Singer, 2009; Crootof, 2015). This triangulated approach ensures a comprehensive and balanced analysis.

The analytical strategy unfolds in three stages. First, each technological domain—nuclear science, cyber warfare, missile defense, and surveillance—is examined individually, drawing on relevant data and scholarship. Second, the findings are interpreted through the lenses of Realism, Liberalism, and Constructivism, highlighting how each theory explains different aspects of the conflict (Waltz, 1979; Keohane, 1984; Wendt, 1999). Third, the domains are integrated into a holistic framework, demonstrating their interdependence and cumulative impact on international relations. This strategy moves beyond descriptive accounts to provide explanatory insights.

The Iran–US–Israel conflict was selected as the case study because it represents one of the most technologically complex rivalries in contemporary international relations. It encompasses nuclear science, cyber operations, missile defense, and surveillance, while also carrying global significance for diplomacy and governance. Moreover, it provides rich empirical material, including treaties, technical reports, and scholarly analyses, making it suitable for generating lessons that are both context-specific and broadly applicable (George & Bennett, 2005).

Several limitations must be acknowledged. First, the secrecy surrounding intelligence operations and military technologies constrains access to data. Cyber operations, in particular, suffer from attribution challenges, making it difficult to establish responsibility with certainty (Rid & Buchanan, 2015). Second, the study relies on secondary sources for much of its analysis, which may reflect the biases of authors or institutions. Third, the case study approach limits generalizability; while the findings provide valuable insights, they may not apply uniformly to other conflicts. Nevertheless, the depth of analysis compensates for these limitations, offering a nuanced understanding of the role of technology in international relations.

The study adheres to ethical standards in academic research. Sources are cited accurately, interpretations are presented transparently, and normative debates are acknowledged. Particular care is taken in discussing targeted killings, surveillance, and autonomous weapons, recognizing the ethical dilemmas they pose for civilian protection and international law (Boyle, 2013; Crootof, 2015). By integrating ethical reflection into the methodology, the study ensures that technological analysis does not neglect human consequences.

In conclusion, the methodology combines qualitative case study analysis with triangulated data sources to examine the role of science and technology in international relations. By integrating primary documents, secondary scholarship, and technical reports, the study provides a comprehensive account of how technological innovation shapes power, diplomacy, and legitimacy. The Iran–US–Israel conflict offers a rich case for analysis, while the theoretical frameworks of Realism, Liberalism, and Constructivism situate findings within broader scholarly debates. Despite limitations, the methodology provides a rigorous foundation for exploring the lessons of technological rivalry and cooperation in global politics.

IV. CASE STUDY ANALYSIS

The triangular conflict among Iran, the United States, and Israel provides a vivid case study of how science and technology shape international relations. Across four domains—nuclear science, cyber warfare, missile defense, and surveillance/artificial intelligence—technological innovation has redefined power dynamics, diplomatic negotiations, and normative debates. Each domain illustrates the interplay of realist imperatives, liberal institutionalism, and constructivist meaning, offering lessons for both theory and practice.

Nuclear Science and Deterrence in the Iran–US–Israel Triangle

Iran's nuclear program has long been a focal point of international concern, straddling the line between civilian energy development and suspected weaponization. From a realist perspective, Iran's pursuit of nuclear capability reflects a survival strategy in a hostile regional environment. Excluded from Western security guarantees and surrounded by adversaries, Tehran views nuclear technology as a deterrent against external intervention (Eisenstadt, 2016). This logic underscores the centrality of power and security in shaping Iran's nuclear ambitions.

Conversely, Israel and the United States interpret Iran's program as an existential threat. Israel, given its small geographic size and vulnerability, perceives a nuclear-armed Iran as intolerable. This perception has driven covert operations, sabotage, and diplomatic pressure aimed at halting Iran's progress (Byman, 2013). The United States has relied on sanctions and negotiations, culminating in the Joint Comprehensive Plan of Action (JCPOA) in 2015. The JCPOA exemplifies liberal institutionalist logic, translating technical thresholds—such as enrichment levels, centrifuge capacity, and inspection protocols—into diplomatic compromise (Katzman, 2015).

However, the collapse of the JCPOA in 2018 highlights the fragility of institutionalist solutions when realist concerns dominate. The U.S. withdrawal under President Trump reflected skepticism about Iran's compliance and dissatisfaction with the deal's scope. Iran's subsequent resumption of enrichment illustrates the cycle of mistrust and escalation (Maloney, 2015). From a constructivist perspective, the breakdown was not merely technical but deeply embedded in narratives of betrayal and resistance. For Iran, the JCPOA's collapse reinforced perceptions of Western hostility; for Israel and the U.S., it confirmed suspicions of Iranian duplicity (Tannenworld, 2007).

This case illustrates the dual role of nuclear science and technology in international relations. On one hand, nuclear science intensifies rivalry by raising existential stakes. On the other, it enables compromise by providing technical frameworks for negotiation. The Iran–US–Israel conflict demonstrates both dynamics, revealing the paradox of technological innovation: it can simultaneously destabilize security and facilitate diplomacy.

This study advances understanding of how nuclear science functions both as a driver of existential rivalry and as a technical basis for diplomatic compromise. By emphasizing the paradoxical role of technology, the study offers a conceptual lens for analyzing future nuclear negotiations beyond the Iran case, including North Korea and South Asia. This multidimensional approach underscores the importance of combining material, institutional, and ideational factors in explaining the persistence of nuclear dilemmas.

Cyber Warfare and Strategic Innovation

The Stuxnet attack of 2010, attributed to U.S.–Israeli collaboration, remains the paradigmatic case of cyber warfare producing physical damage. By infiltrating Iran's Natanz facility and sabotaging centrifuges, Stuxnet demonstrated that software could achieve strategic effects once reserved for conventional weapons (Lindsay, 2013). This operation blurred the line between war and peace, raising enduring questions about attribution, proportionality, and legality (Rid & Buchanan, 2015).

From a realist perspective, Stuxnet exemplifies coercion through technological superiority. The United States and Israel sought to delay Iran's nuclear progress without resorting to overt military strikes. By exploiting vulnerabilities in industrial control systems, they preserved strategic advantage while minimizing risk (Kello, 2017). Iran's subsequent investment in offensive cyber capabilities—targeting infrastructure and communications in adversary states—illustrates the realist cycle of innovation and counter-innovation, where survival depends on exploiting new technological domains.

Liberal institutionalist analysis emphasizes the governance challenges posed by cyber warfare. Unlike nuclear weapons, which are subject to treaties and verification regimes, cyber capabilities remain largely unregulated. International law struggles to address cyber operations, leaving gaps in accountability and enforcement (Deibert, 2013). The Iran–US–Israel conflict illustrates this gap vividly: Stuxnet was unprecedented, yet no international mechanism existed to adjudicate its legality or prevent recurrence. This absence underscores the inadequacy of existing institutions in managing emerging technologies.

From a constructivist perspective, cyber operations carry symbolic meaning that shapes strategic narratives. Stuxnet redefined perceptions of vulnerability, embedding cyber warfare into Iran's strategic imagination. For Iran, the attack symbolized Western hostility and technological dominance; for the U.S. and Israel, it represented innovation and deterrence. These symbolic dimensions influence legitimacy, identity, and threat perception, reinforcing the role of ideas and narratives in shaping cyber conflict (Lindsay, 2013).

The cyber domain thus demonstrates how technological innovation creates new vulnerabilities even as it provides new instruments of power. It highlights the inadequacy of current governance frameworks and the importance of normative debates about legitimacy and ethics. More broadly, cyber warfare illustrates the paradox of technological progress: it simultaneously destabilizes security and expands the repertoire of strategic tools available to states.

By integrating realist, liberal, and constructivist perspectives, this study advances understanding of how cyber operations function both as instruments of coercion and as catalysts for normative debate. The analysis of Stuxnet underscores the paradoxical role of technology: it destabilizes by creating new vulnerabilities, yet also enables strategic innovation. This framework provides a conceptual lens for analyzing future cyber conflicts, from state-sponsored attacks on critical infrastructure to the weaponization of artificial intelligence.

Missile Defense and Military Innovation

Missile defense systems illustrate the material dimension of technological rivalry in the Middle East. Israel's Iron Dome, Arrow, and David's Sling systems, developed with U.S. support, provide a layered defense architecture against Iranian missiles (Cordesman, 2014). These technologies reinforce Israel's strategic confidence, enabling deterrence while minimizing vulnerability. From a realist perspective, missile defense exemplifies survival through technological superiority, where security is achieved by neutralizing adversary capabilities.

Iran's development of advanced ballistic missiles, such as the Sejjil-2, represents a counterbalance to Israel's defensive edge. By investing in missile technology, Iran seeks to overcome Israel's systems and project power regionally (Eisenstadt, 2016). Missile tests serve both strategic and symbolic purposes: they demonstrate capability while asserting sovereignty and defiance. This interplay reflects realist logic, where arms races intensify rivalry and technological innovation becomes central to survival.

Liberal institutionalist analysis raises concerns about missile proliferation and arms control. Unlike nuclear weapons, missiles are not subject to comprehensive international treaties. The absence of regulation undermines stability, as states pursue innovation without constraints (Kerr, 2018). The Iran–US–Israel conflict illustrates this governance gap: missile development continues unabated, complicating diplomatic efforts and limiting the effectiveness of institutional mechanisms.

From a constructivist perspective, missile defense and offense carry symbolic meaning. For Israel, Iron Dome symbolizes resilience and protection, reinforcing national identity and legitimacy. For Iran, missile tests symbolize sovereignty, resistance, and defiance of Western pressure. These narratives shape perceptions of legitimacy and threat, illustrating how technology is socially constructed and embedded in political discourse (Maloney, 2015). 2015).

The missile domain thus demonstrates the interplay of material, institutional, and normative dimensions. It illustrates realist imperatives of survival, liberal concerns about governance, and constructivist narratives of legitimacy. Together, these perspectives highlight how military innovation both stabilizes and destabilizes regional security, reinforcing the paradox of technological progress in international relations.

Analysis of this case advances understanding of how technological rivalry unfolds across defensive and offensive systems, showing that missile technology is not merely material but also institutional and symbolic. By integrating realist, liberal, and constructivist perspectives, the analysis underscores the paradox of missile innovation: it enhances deterrence while simultaneously fueling arms races and normative contestation. This framework provides a lens for examining similar dynamics in other regions, such as South Asia and East Asia, where missile defense and proliferation shape strategic stability.

Technology, Rivalry, and International Relations

Across four domains—nuclear science, cyber warfare, missile defense, and surveillance/artificial intelligence—the Iran–US–Israel conflict demonstrates the profound impact of technological innovation on international relations. Each domain reveals distinct dynamics, yet together they illustrate the interplay of material power, institutional governance, and normative meaning.

Nuclear science intensifies rivalry by raising existential stakes, while also enabling compromise through technical frameworks such as the JCPOA. Cyber warfare, exemplified by Stuxnet, demonstrates how innovation creates new vulnerabilities even as it expands the repertoire of coercive tools. Missile defense systems highlight the arms race logic of survival through technological superiority, while exposing governance gaps in missile regulation. Surveillance and AI-driven operations redefine power projection, compressing decision-making time and provoking normative debates about sovereignty, legality, and ethics.

From a realist perspective, these technologies embody survival imperatives: Iran's pursuit of nuclear and missile capabilities, Israel's layered defense systems, and U.S. reliance on cyber and AI-driven operations all reflect the logic of coercion and deterrence. Liberal institutionalism underscores the governance challenges: nuclear agreements remain fragile, cyber and missile domains lack comprehensive regulation, and targeted operations strain international law. Constructivist analysis highlights the symbolic dimension: technologies are not neutral but embedded in narratives of legitimacy, resistance, and identity.

This study contributes to the literature on international security by offering a comparative, multi-domain framework for analyzing technological rivalry. Rather than treating nuclear, cyber, missile, and surveillance innovations in isolation, it demonstrates how each domain reflects the same paradox: technology simultaneously destabilizes security and enables compromise. By integrating realist, liberal, and constructivist perspectives, the analysis advances theoretical understanding of how material, institutional, and normative dimensions interact in shaping conflict. It also provides practical insights for policymakers: effective governance must adapt to rapid scientific advancement, balancing deterrence with regulation and embedding normative debates into institutional design.

.

IV. DISCUSSION

The Iran–US–Israel conflict demonstrates that science and technology are inseparable from the conduct of international relations. Across nuclear science, cyber warfare, missile defense, and surveillance/artificial intelligence, technological innovation has redefined power dynamics, diplomatic negotiations, and normative debates. This discussion synthesizes the findings of the case study, situates them within theoretical frameworks, and explores broader implications for global governance and comparative conflicts.

Technology as a Determinant of Power

The case study illustrates the realist insight that technological superiority is a determinant of survival in an anarchic international system. Iran's pursuit of nuclear enrichment and ballistic missile development reflects a quest for deterrence in the face of perceived existential threats (Eisenstadt, 2016). Israel's investment in missile defense systems and surveillance technologies similarly reflects realist imperatives, ensuring resilience against adversary attacks (Cordesman, 2014). The United States, as a global power, leverages technological innovation to maintain dominance, from cyber operations such as Stuxnet to drone strikes against Iranian commanders (Lindsay, 2013).

These dynamics underscore the centrality of science and technology in power politics. Material superiority in technological domains translates into strategic advantage, enabling states to deter adversaries, project power, and shape outcomes. The Iran–US–Israel conflict thus exemplifies the realist logic of arms races, where innovation and counter-innovation perpetuate rivalry.

Technology as a Medium of Diplomacy

At the same time, the case study illustrates liberal institutionalist insights. The JCPOA demonstrates how scientific detail can become the language of diplomacy, translating technical thresholds into political compromise (Katzman, Iran: Politics, Human Rights, and US Policy., 2015). Centrifuge capacity, enrichment levels, and inspection protocols were negotiated as cooperative frameworks, reflecting liberal optimism about managing technological disputes. Although the JCPOA collapsed, its existence illustrates the potential for institutions to regulate technological rivalry.

Cyber governance further highlights liberal challenges. Unlike nuclear weapons, cyber capabilities remain largely unregulated, leaving gaps in accountability and enforcement (Deibert, 2013). The Iran–US–Israel conflict illustrates the need for multilateral frameworks to address these challenges. Similarly, missile proliferation underscores the absence of comprehensive treaties, complicating arms control efforts (Kerr, 2018). Surveillance and AI raise questions about international law, particularly regarding targeted killings and autonomous weapons (Crootof, 2015). Liberal approaches emphasize the need for adaptive governance, highlighting the potential for cooperation even in emerging domains.

Technology as Socially Constructed

Constructivist perspectives add a normative dimension, emphasizing that technology acquires meaning through social interaction. For Israel and the United States, Iran's nuclear program symbolizes existential threat; for Iran, it represents sovereignty and resistance (Tannenworld, 2007). Missile tests serve as assertions of sovereignty, while missile defense systems symbolize resilience. Cyber operations such as Stuxnet carry symbolic weight, embedding vulnerability into Iran's strategic imagination (Lindsay, 2013). Drone strikes and surveillance technologies provoke debates about legitimacy, sovereignty, and ethics (Boyle, 2013).

These narratives illustrate how technology is not neutral but socially constructed. Its meaning depends on identities, norms, and perceptions. The Iran–US–Israel conflict demonstrates how technological practices shape legitimacy and threat perceptions, reinforcing narratives of hostility and resistance. Constructivist insights thus complement realist and liberal perspectives, highlighting the normative dimensions of technological rivalry.

Comparative Lessons

The Iran–US–Israel conflict offers lessons for other technological rivalries. In US–China competition, technological innovation in artificial intelligence, quantum computing, and cyber capabilities plays a central role. Similar dynamics of innovation and counter-innovation, governance challenges, and normative debates are evident (Kello, 2017). In Russia–Ukraine tensions, cyber operations, missile systems, and surveillance technologies have shaped the conflict, illustrating the global relevance of technological domains (Rid & Buchanan, 2015).

Comparative analysis underscores the universality of the dynamics observed in the Iran–US–Israel case. Technological innovation intensifies rivalry by raising stakes and creating asymmetries. At the same time, it enables compromise by providing technical frameworks for negotiation. The dual role of technology is thus a general feature of international relations in the twenty-first century.

Implications for Global Governance

The case study highlights the inadequacy of existing governance frameworks. Nuclear weapons are subject to treaties and verification regimes, but cyber capabilities, missile systems, and surveillance technologies remain largely unregulated. The JCPOA illustrates both the potential and fragility of cooperative frameworks. Its collapse underscores the need for stronger institutions and enforcement mechanisms.

Cyber governance requires multilateral frameworks to address attribution, accountability, and proportionality. Missile proliferation demands comprehensive treaties to regulate development and deployment. Surveillance and AI raise ethical and legal questions that require international consensus. The Iran–US–Israel conflict illustrates these challenges vividly, offering lessons for global governance in an era of rapid technological advancement.

Integrating Theoretical Perspectives

The case study demonstrates the need for integrated scholarship that bridges theoretical traditions. Realism explains the pursuit of technological superiority and the logic of deterrence. Liberalism highlights the potential for cooperation through institutions and regimes. Constructivism underscores the social construction of legitimacy and the normative debates surrounding technology. Together, these perspectives provide a multidimensional lens for analysis.

Integration is particularly important in the technological domain, where material, institutional, and normative dimensions intersect. Nuclear science illustrates realist deterrence, liberal cooperation, and constructivist legitimacy. Cyber warfare demonstrates realist coercion, liberal governance challenges, and constructivist symbolism. Missile defense reflects realist survival imperatives, liberal arms control concerns, and constructivist narratives of sovereignty. Surveillance and AI highlight realist power projection, liberal legal frameworks, and constructivist ethical debates. The Iran–US–Israel conflict thus exemplifies the need for integrated analysis.

Ethical Considerations

The case study also raises ethical considerations. Targeted killings, autonomous weapons, and surveillance technologies challenge principles of distinction, proportionality, and sovereignty. Scholars warn that lethal autonomous weapons systems (LAWS) pose profound questions for international law and ethics (Crootof, 2015). Surveillance and AI raise concerns about privacy, civilian protection, and legitimacy (Singer, 2009). The Iran–US–Israel conflict illustrates these dilemmas vividly, highlighting the need for ethical reflection in technological analysis.

The Iran–US–Israel conflict demonstrates the profound impact of science and technology on international relations. Across nuclear science, cyber warfare, missile defense, and surveillance/artificial intelligence, technological innovation has redefined power,

diplomacy, and legitimacy. The case study illustrates realist imperatives of survival, liberal potential for cooperation, and constructivist narratives of legitimacy. It highlights the inadequacy of existing governance frameworks and the need for integrated scholarship. Comparative lessons underscore the universality of these dynamics, while ethical considerations emphasize the human consequences of technological rivalry. In sum, science and technology are not neutral tools but central determinants of international relations in the twenty-first century.

Conclusion

The Iran–US–Israel conflict illustrates how science and technology have become decisive determinants of international relations in the twenty-first century. Across nuclear science, cyber warfare, missile defense, and surveillance/artificial intelligence, technological innovation has reconfigured power dynamics, reshaped diplomacy, and provoked normative debate. Technology emerges not as a neutral instrument but as a central axis of rivalry, negotiation, and governance.

Science and technology operate simultaneously as tools of coercion and mediums of diplomacy. Nuclear science raises existential stakes yet enables compromise through technical negotiation frameworks, as seen in the JCPOA. Cyber warfare exemplifies coercion through superiority but also exposes vulnerabilities that encourage dialogue on governance. Missile defense reinforces survival imperatives, while proliferation underscores the urgency of arms control. Surveillance and AI extend state power but provoke ethical debates requiring international consensus. The dual role of technology is thus a defining feature of contemporary global politics.

The findings underscore the value of integrating Realism, Liberalism, and Constructivism. Realism explains the pursuit of technological superiority and deterrence; Liberalism highlights cooperation through institutions and regimes; Constructivism illuminates normative debates, from nuclear taboos to drone ethics. Together, these perspectives capture the material, institutional, and normative dimensions of technological rivalry.

The conflict also reveals the inadequacy of current governance frameworks. Nuclear weapons are subject to treaties and verification regimes, but cyber capabilities, missile systems, and surveillance technologies remain largely unregulated. The JCPOA illustrates both the potential and fragility of cooperative frameworks. Cyber governance requires multilateral mechanisms for attribution and accountability; missile proliferation demands comprehensive treaties; surveillance and AI raise ethical and legal questions that necessitate international consensus. Strengthening institutions and enforcement mechanisms is imperative in an era of rapid technological advancement.

These dynamics are not unique to the Middle East. U.S.–China competition in AI and quantum computing, and Russia–Ukraine tensions involving cyber operations and missile systems, demonstrate the universality of technology's dual role: intensifying rivalry while enabling compromise. Comparative analysis underscores the global relevance of these lessons for security and diplomacy.

Technological innovation also raises profound ethical dilemmas. Targeted killings, autonomous weapons, and surveillance challenge principles of distinction, proportionality, and sovereignty. Lethal autonomous systems pose unprecedented questions for international law, while surveillance and AI raise concerns about privacy and legitimacy. Ethical reflection must be integrated into governance frameworks to safeguard human rights and international law.

This study contributes by offering a multi-domain framework that integrates material, institutional, and normative dimensions of technological rivalry. It demonstrates that technology simultaneously destabilizes security and enables compromise, a paradox central to contemporary global politics. Future scholarship should pursue cross-domain and comparative analysis, recognizing the interconnectedness of nuclear, cyber, missile, and surveillance technologies. Governance frameworks must adapt to emerging innovations such as AI, quantum computing, and biotechnology, while constructivist perspectives can deepen understanding of normative debates.

Science and technology are now central determinants of international relations. They heighten rivalry by raising stakes and creating asymmetries, yet they also enable compromise through technical frameworks for negotiation. By integrating theoretical perspectives, addressing governance challenges, and embedding ethical reflection, scholars and policymakers can better manage the transformative impact of technology on global politics. The lessons of the Iran–US–Israel conflict extend beyond the Middle East, offering insights into the future of security and diplomacy in an era defined by rapid scientific advancement.

Bibliography

Boyle, M. J. (2013). Drone Warfare and International Law. International Affairs, 89(1).
Byman, D. (2013). Why Drones Work: The Case of Washington's Weapon of Choice. Foreign Affairs, 92(4), 32-43.
Cordesman, A. H. (2014). Israel and Misile Defense: The Iron Dome, Arrow, and David's Sling. Center for Strategic and International Studies.
Crootof, R. (2015). The Killer Robots Are Here: Legal and Policy Implications. Colorado Law Review, 36(5), 1837-1915.
Deibert, R. (2013). Black Code: Surveillance, Privacy, and the Dark Side of the Internet. McClelland & Stewart.
Eisenstadt, M. (2016). The Strategyc Culture of the Islamic Republic of Iran: Operational and Policy Implications. Washington: Washington Institute for Near East Policy.
Finnermore, M., & Hollis, D. (2016). Constructing Norms for Global Cybersecurity. American Journal of International Law, 110(3), 425-479.
Fitzpatrick, M. (2016). The Iran Nuclear Deal: A Definitive Guide. International Institute for Strategic Studies.
Katzman, K. (2015). Iran: Politics, Human Rights, and US Policy. Congressional Research Service.
Katzman, K. (2019). Iran's Nuclear Program and the US Policy. Washington: Congresional Research Service.
Kello, L. (2017). The Virtual Weapon and International Order. Yale University Press.
Keohane, R. O., & Nye, J. S. (1977). Power and Interdependence: World Politics in Transition. Little Brown.
Keohane, R. O., & Nye, J. S. (1977). Power and Interdependence: Worls Politics in Transition. Boston: Little Brown.
Kerr, P. K. (2018). Iran's Nuclear program: Status. Washington: Congressional Research Service.
Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. Security Studies, 22(3), 365-404.
Maloney, S. (2015). Iran's Political Economy since the Revolution. Cambridge: Cambridge University Press.

Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. Journal of Strategic Studies, 38 (1-2), 4-37.
Segan, S. D. (1996). The Limits of Safety: Organizations, Accidents, and Nuclear Weapons. Princeton: Princeton University Press.
Singer, P. W. (2009). Wired for War: The Robotics Revolution and Conflict in the 21st Century. Penguin Press.
Tabatabai, A. (2019). Iran's Cyber Strategy: A Political Culture Perspective. Carnegie Endowment for Internationa Peace.
Tannenworld, N. (2007). The Nuclear Taboo: The United States and the non-use of Nuclear Weapons since 1945. Cambridge: Cambridge University Press.
Waltz, K. N. (2012). Why Iran should get the Bomb: Nuclear balancing would mean Stability. Foreign Affairs, 91 (4), 2-5.
Waltz, K. N. (2012). Why Iran should get the Bomb: Nuclear Balancing wouls mean Stability. Foreign Affairs, 2-5.
Wendt, A. (1999). Social Theory of International Politics. Cambridge: Cambridge University Press.
Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishing.

