CSIW

Crisis Studies of the Islamic World
Vol.12, No.5, winter 2026 (English issue)

Anarchy in Cyberspace: A Constructivist Analysis of Iran-Israel Cyber Rivalry

Mehdi Abbaszadeh Fathabadi[1] | Mosayyeb Rostami Khanmakani[2]

Received Date: 2025/10/05 Accept Date: 2026/05/14

Cite: Abbaszadeh Fathabadi, M and Rostami Khanmakani, M. (2026). Anarchy in Cyberspace: A Constructivist Analysis of Iran-Israel Cyber Rivalry. *Crisis Studies of the Islamic World*, *12*(5), 1-21.
DOI: 10.27834/CSIW.2510.596.4.40.1

Abstract

This study examines the Iran–Israel cyber rivalry through a constructivist lens, arguing that existing analyses underestimate the social and narrative dynamics that shape cyber conflict in Southwest Asia. While conventional approaches emphasize capabilities and deterrence, they often overlook how cyber operations acquire meaning through identity, discourse, and the dynamics of ontological security. Addressing this gap, the article argues that incidents such as the Stuxnet operation served as discursive turning points that reinforced Iran's pre-existing self-perception as an active cyber actor and intensified a long-standing rivalry, rather than transforming its identity. Drawing on a qualitative analysis of official statements, policy documents, and public narratives from 2010 to 2024, the study finds that the ambiguity of cyber norms enables both actors to interpret cyber operations as challenges to implicit red lines, thereby generating cycles of reciprocal action and narrative escalation. These patterns extend competition beyond the technical domain into the realms of symbolic signaling, perception management, and the strategic production of ontological insecurity. The article contributes to the cybersecurity literature by demonstrating how identities and socially constructed meanings shape cyber interactions, while highlighting the need for trust-building measures and norm-development mechanisms to mitigate escalating instability in the region.

Keywords: Cyber Conflict, Islamic Republic of Iran, Israel, Ontological Security

[1]. Associate Professor, Department of Political Science, Faculty of Law and Theology, Shahid Bahonar University of Kerman, Kerman, Iran. abbaszadeh@uk.ac.ir (Corresponding author).
[2] . Master in Political Science, Shahid Bahonar, University of Kerman, Kerman, Iran. m.rostami@uk.ac.ir

Introduction

In recent decades, cyberspace has emerged as a critical domain for state activity. Characterized by speed, attribution ambiguity, and operational complexity, cyberspace presents unprecedented challenges to traditional theoretical frameworks in international relations. Within this context, Southwest Asia has become a major arena of cyber rivalry, where regional actors increasingly employ cyber capabilities to pursue strategic objectives and project power. Among these rivalries, the cyber confrontation between Iran and Israel represents a particularly significant case for scholarly analysis because of its longstanding hostility, asymmetric character, and far-reaching implications for regional security and stability.

Unlike traditional approaches such as Realism and Liberalism, which primarily emphasize material capabilities and international institutions, respectively, this article argues that understanding the dynamics and consequences of cyber rivalry in Southwest Asia requires a theoretical framework that extends beyond material explanations. Drawing on Constructivist theory, the study addresses the following research question: How do socially constructed identities, norms, and discourses shape the cyber rivalry between Iran and Israel, and what are the implications for regional diplomacy and security in Southwest Asia?

To address an important gap in the existing literature, this article moves beyond predominantly technical and military analyses by examining the social and cognitive dimensions of cyber conflict. While previous studies have explored the technical capabilities, security implications, and defense strategies of the two actors, relatively little attention has been paid to the interactive processes through which identities, norms, and threat perceptions are socially constructed and reproduced. This study argues that cyber operations are not merely instruments of disruption or coercion; they also function as mechanisms for reinforcing identities, deepening mutual mistrust, and reshaping patterns of interaction between Iran and Israel.

The article is organized as follows. The first section reviews the relevant literature and outlines the Constructivist theoretical framework. The second section explains the research methodology, including the interpretive research paradigm, qualitative approach, and rationale for selecting the Iran–Israel cyber rivalry as the case study. The subsequent sections examine the processes of identity construction, the role of normative ambiguity in cyberspace, and the evolving patterns of interaction between the two actors. The article concludes by discussing the implications of these findings for regional diplomacy and cybersecurity governance, while highlighting their broader theoretical and practical significance.

Literature Review

In recent years, the expansion of cyberspace as a new domain of state activity has stimulated a growing body of scholarship on cybersecurity

within the field of international relations. Much of the existing literature, informed by traditional theoretical approaches such as Realism and Liberalism, has examined cyber conflict primarily through the lenses of material capabilities, deterrence (by punishment and denial), and international cooperation to mitigate cyber threats. For example, studies have analyzed the evolution of Israel's cyber security doctrine, demonstrating how the country's geopolitical constraints have encouraged sustained investment in cyber capabilities and unconventional deterrence strategies (Golmohammadi & Jamshidi, 2022).

Another strand of the literature focuses on cyber threats directed against Iran and their implications for national security. These studies primarily examine the offensive and defensive dimensions of cyber conflict, portraying hostile cyber operations as forms of hybrid warfare, psychological operations, and strategic coercion. Cyberattacks targeting critical infrastructure, economic systems, and public opinion have been identified as major threats to Iran's national security (Koohsarian et al., 2021). Similarly, several scholars argue that cyber-enabled psychological warfare constitutes one of the most significant instruments used by Iran's adversaries to undermine political stability, emphasizing the importance of strengthening national cyber defense capabilities (Pour Ebrahimi et al., 2017; Nasiri et al., 2024). Within this context, the Stuxnet attack has frequently been identified as a pivotal moment that elevated cybersecurity to a central component of regional security discourse (Mirzaei & Qoreishi, 2024). Beyond its immediate impact on Iran's nuclear infrastructure, the attack also accelerated the expansion of the country's cyber defense institutions and capabilities, including the establishment of organizations such as Iran's Cyber Army.

A growing body of international relations scholarship, particularly research grounded in Constructivist theory, moves beyond materialist explanations by emphasizing the social, ideational, and cognitive dimensions of cybersecurity (Bahoosh Fardeghi, 2017). From this perspective, national security is understood as a socially constructed phenomenon shaped by identities, norms, shared meanings, and patterns of interaction among states. Accordingly, power in cyberspace derives not only from technological capabilities but also from the capacity to construct narratives, shape identities, influence perceptions, and legitimize particular understandings of security and threat.

Despite these important contributions, a significant gap remains in the literature. Existing studies have largely examined the technical capabilities, military dimensions, or security implications of cyber conflict from the perspective of individual actors, while paying comparatively little attention to the relational and socially constructed processes through which cyber rivalries evolve. Addressing this gap, the present study analyzes the cyber rivalry between Iran and Israel through a Constructivist framework. Rather than treating cyber operations merely as instruments of disruption or

coercion, the article conceptualizes them as social practices that reinforce identities, deepen mutual mistrust, shape threat perceptions, and transform patterns of interaction between the two states. By integrating constructivist insights with empirical analysis of the Iran–Israel cyber rivalry, this study offers a theoretically grounded explanation of how cyber conflict reshapes regional security and diplomatic dynamics, thereby contributing a novel perspective to the existing literature.

1. Theoretical Framework: Constructivism and Cybersecurity

Understanding complex phenomena in international relations requires theoretical frameworks that extend beyond traditional materialist and individualist assumptions. Constructivism, as a structural idealist approach, challenges the materialist and individualist perspectives of Realism and Liberalism by emphasizing the role of shared ideas, identities, and norms in shaping social structures and state interests (Wendt, 1999: 2). Unlike Realists, who regard anarchy as an objective and material condition, Alexander Wendt argues that "anarchy is what states make of it" (Wendt, 1999: 6). From this perspective, the nature of anarchy is socially constructed through patterns of interaction among states, giving rise to Hobbesian (enmity), Lockean (rivalry), or Kantian (friendship) cultures of anarchy (Wendt, 1999: 246). Similarly, state identities and interests are not fixed or predetermined; rather, they emerge through social interaction within a framework of shared ideas and norms (Wendt, 1999: 193). Peter Katzenstein likewise argues that national security culture demonstrates how norms and identities shape states' security interests and influence the ways in which they exercise power (Katzenstein, 1996: 1).

Traditional international relations theories face significant limitations in explaining the dynamics of cyberspace because of their emphasis on material capabilities and state-centric assumptions. As Lucas Kello argues in The Virtual Weapon and International Order, conventional theories are unable to explain many of the distinctive characteristics of cyber conflict. One of these challenges concerns the ambiguity of the boundary between war and peace. Whereas Realism and Liberalism assume a relatively clear distinction between these two conditions, cyber operations frequently occur within a strategic "gray zone." To describe this phenomenon, Kello introduces the concept of unpeace, arguing that:

"Minds captured by old concepts do not readily adopt new ones ... but more flexible minds may find in the term [unpeace] a congenial vehicle for escaping the conceptual knots of the war-peace binary that so obscures common descriptions of the new domain of action." (Kello, 2017: 79)

The concept of unpeace captures a persistent condition of strategic competition that transcends the conventional war–peace dichotomy and therefore cannot be adequately explained by traditional theories.

Another defining characteristic of cyberspace is attribution ambiguity. Identifying the perpetrator of a cyberattack is often technically and politically difficult, undermining traditional concepts of deterrence that rely on the credible threat of retaliation. As Kello notes, "the rules of deterrence, if they exist at all, are largely indefinite; shared norms are rudimentary or unenforceable; and the identity, motives, or location of an attacker may be unknown" (Kello, 2017: 119). Under these conditions, deterrence based solely on material capabilities becomes increasingly difficult to sustain.

Cyber conflict also challenges the state-centric assumptions of conventional international relations theories by expanding the range of influential security actors. In addition to states, corporations, transnational criminal organizations, and hacktivist groups possess the capacity to disrupt critical infrastructure, influence interstate relations, and generate security crises beyond the direct control of governments (Kello, 2017: 57).

Given these limitations, Constructivism provides a more comprehensive framework for analyzing cyber conflict. Rather than focusing exclusively on material capabilities, Constructivism emphasizes the social construction of threats, identities, and security perceptions. From this perspective, cyberattacks acquire strategic significance not merely because of their physical consequences but because of the meanings that political actors attribute to them. The identities of the actors involved, together with their historical experiences and patterns of interaction, shape how cyber operations are interpreted and how governments respond. For example, the Stuxnet operation was perceived in Iran not simply as a cyberattack on nuclear facilities but as a challenge to national sovereignty, technological advancement, and strategic identity. Consequently, the political and security consequences of the attack were shaped primarily by these socially constructed interpretations rather than by its immediate material effects.

Constructivism also highlights the importance of norms in regulating state behavior in cyberspace. Because cyberspace lacks comprehensive and widely accepted international rules governing cyber operations, states operate within an environment of considerable normative ambiguity. Under such conditions, cyberattacks are frequently interpreted as violations of implicit expectations or unwritten red lines, thereby reinforcing reciprocal distrust and encouraging retaliatory behavior. Rather than representing a complete absence of norms, cyberspace is better understood as a domain characterized by competing interpretations of legitimate and illegitimate behavior, which contribute to recurring cycles of escalation.

Finally, Constructivism emphasizes that repeated interactions gradually shape identities and expectations. From this perspective, the cyber rivalry between Iran and Israel is not driven solely by rational calculations of material interests but is continuously reproduced through patterns of interaction. Recurrent cyber operations reinforce mutually antagonistic identities, deepen perceptions of existential threat, and generate what Wendt

describes as "collective knowledge" of hostility (Wendt, 1999: 157). Over time, this social process institutionalizes mutual distrust and sustains the rivalry independently of purely technical or strategic considerations.

This theoretical framework enables cyber conflict in Southwest Asia to be understood not merely as competition over technological capabilities or material power, but as a socially constructed process in which identities, norms, narratives, and patterns of interaction shape the meaning of threat and influence regional security dynamics. Consequently, Constructivism provides a more comprehensive explanation of the Iran–Israel cyber rivalry by illuminating dimensions of conflict that remain largely overlooked by materialist approaches.

2. Methodology

This study is conducted based on an interpretive paradigm and a qualitative approach. The interpretive paradigm is founded on the principle that social reality, including security phenomena, is constructed by individuals' ideas, meanings, and interpretations. Consequently, the goal of this research is not to explain an objective reality, but to understand and interpret the meaning of cyber actions within the framework of shared concepts, identities, and norms of the actors. The qualitative approach, by collecting textual and documentary data, allows for a deep and layered analysis of the phenomena under study.

The case study of the Iran-Israel cyber rivalry was selected for the following reasons: First, Long-Term Interactions: These two actors have a long and continuous history of confrontation in various fields. This history provides a rich context of mutual interactions and the construction of hostile identities for constructivist analysis. Second, Symbolic Attacks: Cyberattacks between Iran and Israel have often gone beyond a mere technical act, possessing symbolic and meaningful dimensions. The Stuxnet attack on Iran's nuclear facilities was not just a technical strike, but was perceived as an attack on Iran's "national identity and independence," leading to reactions that transcended the technical level. Third, A War of Narratives: Both sides have attempted to present specific narratives of their actions in cyberspace. Analyzing these narratives allows for an understanding of how norms are constructed and retaliatory actions are justified. Fourth, Changing Traditional Equations: The complex and ambiguous nature of this rivalry demonstrates the practical limitations of traditional Realist and Liberal approaches, and thus serves as a suitable case study for proving the effectiveness of the constructivist theoretical framework.

The data for this research was collected qualitatively by examining the following sources:

A: Official Statements and Declarations: Including speeches, interviews, and official statements by Iranian and Israeli government and military officials.

B: Security Documents and Reports: Published reports from security agencies, think tanks, and international organizations related to cybersecurity.

C: Media News and Analysis: An analysis of news published in credible international and regional media outlets that reflect official viewpoints or expert analysis.

The collected data will be analyzed using interpretive coding. This method includes the following steps:

1 .Determining Initial Codes: In this stage, the data is carefully examined to identify sections related to the key concepts of the theoretical framework (identity, norms, and interaction).

2 .Interpretive Coding: Instead of merely describing the data, each piece of information (such as a sentence in a statement) is coded based on its social meaning and its relationship to constructivist concepts. For example: Phrases like "fake regime," "resistance forces," and "existential enemy" are analyzed as codes related to identity-building. The use of words like "violation of laws," "cyber aggression," or "red line" are used as codes to analyze norms and the normative vacuum. The trend of reciprocal attacks and responses will be examined as codes to analyze interaction patterns and the construction of mistrust. This methodological approach allows us to focus on "how it happened?" and "what did it mean?" instead of "what happened?", and to coherently and seamlessly demonstrate the connection between the theoretical foundations and the empirical findings.

3. Research Findings: A Constructivist Analysis of Cyber Rivalry in Southwest Asia

3.1. Identity Construction and Threat Perception in Cyberspace

This section examines the Stuxnet operation as a critical episode for understanding how cyber conflict reshapes security perceptions and strategic behavior in Southwest Asia. Rather than interpreting Stuxnet solely as a technical act of sabotage, the analysis emphasizes its broader implications for identity construction, threat perception, and strategic discourse. From a constructivist perspective, international politics is shaped not only by material capabilities but also by intersubjective meanings, shared understandings, and identity narratives that influence how states perceive threats and formulate security policies (Wendt, 1999; Katzenstein, 1996). Within this framework, cyber operations acquire political significance because they influence the ways in which states interpret their security environment and define their strategic identities.

The findings suggest that the Stuxnet operation did not fundamentally transform Iran's identity. Rather, it served as a critical discursive episode that reinforced pre-existing narratives of resistance, strategic rivalry, and asymmetric competition while extending them into the cyber domain. Long

before the attack, Iranian strategic discourse had already portrayed regional security as a persistent confrontation with technologically superior adversaries that required asymmetric responses (Bahgat & Ehteshami, 2017: 90). The cyberattack against Iran's nuclear infrastructure strengthened these existing narratives by demonstrating that cyberspace had become a new arena in which established security identities and threat perceptions could be expressed and reproduced.

This process of discursive construction is evident in the official response of Iran's political leadership. In a statement delivered in 2012, the Leader of the Islamic Revolution referred to Western acknowledgment of "internet and technical sabotage" through malware such as Stuxnet and criticized the International Atomic Energy Agency for failing to respond appropriately. He further questioned the absence of a timely response by the United Nations to threats against Iran's nuclear security, thereby situating the Stuxnet incident within a broader narrative of institutional silence, external hostility, and national vulnerability (khamenei.ir, 2012). From a constructivist perspective, this official discourse is significant because it framed the cyber operation not merely as a technical intrusion but as evidence of a hostile international environment. In doing so, it reinforced existing narratives of strategic competition and legitimized the securitization of cyberspace within Iran's national security discourse.

3.1.1. Threat Perception and Ontological Anxiety

Prior to the Stuxnet operation, Iran's threat perceptions were primarily embedded within conventional military thinking and regional geopolitical rivalries (Bahgat & Ehteshami, 2017: 90). The attack, however, exposed the existence of an invisible, technologically sophisticated threat capable of penetrating critical national infrastructure, including nuclear facilities. Such developments generate what the literature describes as geopolitical and ontological anxiety by revealing vulnerabilities that challenge established understandings of national security and strategic control (Eberle & Daniel, 2022: 2).

Rather than producing an identity transformation, the Stuxnet operation can be understood as an ontological disturbance that required discursive stabilization. Constructivist scholarship argues that states confronted with disruptive security events often respond by reconstructing narratives that preserve continuity, restore predictability, and maintain ontological security (Wendt, 1999). In the Iranian case, official discourse increasingly described the incident using securitized concepts such as cyber war, cyber aggression, and attacks on critical infrastructure, rather than portraying it simply as a technical malfunction or isolated cyber intrusion. This discursive shift incorporated cyberspace into Iran's broader security imagination and reinforced pre-existing narratives of strategic confrontation rather than creating a fundamentally new national identity.

3.1.2. Rearticulating Security Strategy: From Asymmetric Defense to Active Cyber Deterrence

The perceptual shock generated by the Stuxnet operation appears to have accelerated the integration of cyberspace into Iran's broader doctrine of asymmetric defense alongside its naval and missile capabilities. Asymmetric defense strategies are typically adopted by comparatively weaker actors seeking to offset the advantages of technologically superior adversaries through unconventional and cost-effective instruments (Anderson & Sadjadpour, 2018: 11). Within this strategic framework, cyberspace emerged as an additional operational domain that complemented Iran's existing approach to asymmetric competition.

Institutional developments following the attack illustrate this process of strategic adaptation. Iranian authorities expanded the responsibilities of the Civil Defense Organization in protecting critical infrastructure and established the Cyber Police (FATA) in 2011 to address emerging cyber threats. These developments indicate the gradual institutionalization of cyber capabilities within Iran's national security architecture. Rather than representing a fundamental shift in strategic thinking, these measures demonstrate how cyber capabilities were incorporated into an already established doctrine of asymmetric deterrence and strategic competition.

3.1.3. Cyber Instruments as "Imperfect Tools for Escalation"

From a constructivist perspective, Iran's growing reliance on cyber capabilities also reflects changing understandings of escalation, deterrence, and strategic signaling. Borghard and Lonergan (2019: 122) describe cyber operations as "imperfect tools for escalation" because several structural characteristics enable states to compete below the threshold of conventional armed conflict. First, attribution ambiguity complicates the identification of perpetrators, thereby reducing the likelihood of immediate military retaliation. Second, cyber operations generally impose lower political, economic, and military costs than conventional force, allowing states to calibrate their responses with greater flexibility. Third, many cyber operations produce limited or no immediate physical casualties, making escalation more manageable while preserving opportunities for strategic signaling.

For emerging cyber powers such as Iran, these characteristics provide opportunities to challenge technologically superior adversaries without engaging in direct military confrontation. Consequently, Iran's increasing reliance on cyber capabilities is best understood not as evidence of an identity transformation but as a strategic adaptation that reinforces an existing framework of asymmetric rivalry.

Overall, the Stuxnet operation should be understood less as a moment of identity transformation than as a critical discursive catalyst that reinforced pre-existing narratives of strategic competition and extended them into

cyberspace. By exposing previously unrecognized vulnerabilities and generating geopolitical and ontological anxiety, the attack encouraged Iranian policymakers to integrate cyber capabilities more systematically into national security planning. This process, in turn, contributed to a reciprocal dynamic in which both Iran and Israel increasingly interpreted each other's actions through a cyber-security lens, thereby reinforcing mutual mistrust, competitive signaling, and enduring patterns of strategic rivalry.

3.2. The Role of Norms and Normative Ambiguity in Escalating Instability

Building upon the constructivist framework developed by Wendt and the preceding analysis, the findings suggest that the Stuxnet operation did not fundamentally transform Iran's identity; rather, it extended pre-existing narratives of strategic rivalry into cyberspace. Within this expanded arena, the absence of clearly institutionalized and mutually accepted cyber norms—or, more precisely, the presence of normative ambiguity—created conditions under which new patterns of strategic interaction emerged. From a constructivist perspective, norms function as shared expectations that enable actors to interpret one another's behavior and distinguish legitimate from illegitimate conduct (Wendt, 1999: 171–178). When such expectations remain contested or underdeveloped, cyber operations are more likely to be interpreted as violations of implicit red lines, thereby reinforcing cycles of reciprocal retaliation.

Under conditions of normative ambiguity, the strategic meaning of cyber operations is determined less by their technical characteristics than by the interpretations attached to them by political actors. Consequently, offensive cyber operations—regardless of their scale or immediate objectives—may be discursively constructed as proxy warfare or even as acts of war, thereby legitimizing increasingly robust responses. Rather than reducing tensions, the persistent ambiguity surrounding attribution further intensifies mutual suspicion and contributes to the reproduction of strategic instability (Wendt, 1999: 246–308).

The Iran–Israel cyber rivalry provides a clear illustration of this dynamic. Cyber operations targeting critical infrastructure have progressively challenged implicit normative boundaries governing acceptable state behavior in cyberspace. Whereas cyber espionage and information collection were previously regarded as relatively tolerable practices, direct interference with critical civilian infrastructure increasingly came to be viewed as crossing an implicit threshold (Van Dine, 2017: 101–102). The Stuxnet operation represented a significant departure from this informal understanding and contributed to the gradual normalization of retaliatory cyber operations against similarly sensitive targets. As cyber interactions intensified, both actors increasingly redefined the boundaries of acceptable conduct through reciprocal practice rather than through mutually recognized international norms.

The events of April 2020 illustrate this process. Following allegations that cyber groups affiliated with Iran had targeted Israel's water-management facilities, Israeli authorities publicly attributed responsibility to Iran despite Tehran's denial (CFR, 2020). Beyond communicating technical attribution, these public statements served an important discursive function by constructing Israel as the victim of irresponsible cyber aggression and portraying Iran as an actor that had violated implicit norms protecting civilian infrastructure. This narrative framing subsequently provided political legitimacy for Israel's reported cyber operation against Shahid Rajaee Port by presenting it as a proportionate defensive response. In the absence of shared normative standards, both actors increasingly interpreted cyber incidents through narratives that reinforced their respective strategic objectives, thereby reproducing a self-reinforcing cycle of retaliation and mutual distrust.

A similar pattern can be observed in Iran's official response to the Stuxnet operation. Judicial and regulatory authorities framed the malware not merely as a technical intrusion but as an unlawful violation of national sovereignty and critical infrastructure. Official statements emphasized that those responsible for developing and distributing the malware should face legal accountability through appropriate judicial mechanisms. This legal discourse transformed Stuxnet into a norm-violating act requiring institutional and legal responses, further reinforcing the perception that cyberattacks against critical infrastructure constituted unacceptable breaches of implicit red lines (Tasnim News, 2016).

These developments have had important implications for cyber diplomacy. Repeated cycles of reciprocal cyber operations, combined with the absence of widely accepted behavioral norms, have significantly constrained regional efforts to develop confidence-building measures or institutional frameworks for governing cyberspace. As a result, cyber diplomacy has become increasingly fragile, with normative ambiguity contributing to the continued erosion of trust and the persistence of strategic competition between Iran and Israel.

The erosion of cyber diplomacy is reflected in several interrelated dimensions:

A. Ambiguous Role of Proxies and Plausible Deniability

The extensive use of proxy actors and strategies of plausible deniability constitutes a significant obstacle to diplomatic engagement in cyberspace. Both Iran and Israel have relied on indirect actors and ambiguous attribution to conduct cyber operations while minimizing the political and legal costs associated with formal responsibility (Torres, 2017: 211). From a constructivist perspective, these practices complicate the establishment of shared expectations regarding accountability, thereby reinforcing uncertainty and mutual distrust.

B. Limited Commitment to International Cyber Norms

Neither Iran nor Israel is a party to major international legal frameworks governing cyberspace, such as the Budapest Convention on Cybercrime. Although the two states differ in their legal and strategic rationales, their limited participation in multilateral cyber governance reflects the absence of a mutually accepted normative framework capable of regulating cyber behavior and facilitating confidence-building.

C. Absence of Bilateral Dialogue

In the absence of mutually recognized norms, opportunities for meaningful bilateral dialogue on cyber issues remain extremely limited. Rather than negotiating shared red lines or establishing confidence-building mechanisms, both actors have prioritized the development of offensive cyber capabilities as instruments of deterrence and strategic signaling—a logic that has gradually become embedded within their respective security discourses (Xu & Lu, 2021: 101).

Taken together, the repeated targeting of critical infrastructure, combined with the erosion of implicit normative constraints, has generated a self-reinforcing process of mistrust and strategic instability. Instead of encouraging restraint, each successive cyber operation reshapes expectations and legitimizes further retaliation, contributing to an enduring cycle of escalation. The following section examines how these interaction patterns continuously reproduce distrust between Iran and Israel.

3.3. Interaction Patterns and the Construction of Distrust

The preceding sections argued that the Stuxnet operation constituted an ontological and strategic shock that extended Iran's pre-existing security narratives into the cyber domain rather than fundamentally transforming its identity. Building on this argument, the present section examines how repeated interactions between Iran and Israel continuously generate and reproduce mutual distrust. From a constructivist perspective, international politics is shaped not only by material capabilities but also by patterns of social interaction through which actors construct identities, expectations, and perceptions of one another (Wendt, 1999: 2). Distrust, therefore, should be understood not as an inevitable consequence of conflict but as a socially constructed phenomenon that is reproduced through recurring cyber interactions (Mark, 2024: 41).

Cyber operations have increasingly become instruments of escalation without direct military confrontation. Given the political and military constraints associated with conventional warfare, cyber capabilities provide states with a strategic outlet for calibrated retaliation across multiple levels of intensity (Harknett & Smeets, 2022: 541). Attribution ambiguity enables both parties to conduct cyber operations while avoiding formal acknowledgment of responsibility, yet these actions nevertheless communicate strategic intentions to their adversary. This dynamic

contributes to what Harknett and Smeets describe as a cyber security dilemma, in which defensive measures undertaken by one actor are interpreted as offensive threats by the other, thereby reinforcing recurring cycles of escalation (Harknett & Smeets, 2022: 541–546).

The Iran–Israel cyber rivalry illustrates this dynamic particularly clearly. Reciprocal cyber operations have evolved beyond attempts to inflict material damage and increasingly function as mechanisms for producing and institutionalizing distrust at both governmental and societal levels. Allegations regarding cyber operations against Israel's water infrastructure provide a notable example. Through official attribution, Israeli authorities framed Iran as the aggressor and Israel as the victim of an attack against civilian infrastructure. Within an environment characterized by entrenched distrust, this narrative subsequently enabled the reported cyber operation against Shahid Rajaee Port to be presented as a legitimate defensive response intended to restore deterrence. Such reciprocal narratives continually reproduce adversarial identities by portraying hostile actions as necessary and justified responses to previous aggression, thereby reinforcing the cyber security dilemma and reducing opportunities for diplomatic de-escalation.

Intelligence assessments further suggest that both states have maintained persistent access to elements of each other's critical infrastructure for extended periods (CyberCX Intelligence, 2024). These long-term intrusions frequently target supply chains and third-party service providers, allowing access to be exploited for disruptive or destructive purposes when strategic circumstances require. Reported operations attributed to the Predatory Sparrow group against Iranian financial infrastructure, together with cyber activities attributed to Iran-affiliated actors targeting Israeli infrastructure, illustrate the persistence of this ongoing cyber confrontation. Even operations that initially serve intelligence-gathering purposes often evolve into disruptive or destructive activities as strategic competition intensifies (Anderson & Sadjadpour, 2018: 15).

Beyond their material consequences, cyber operations also perform important psychological and symbolic functions. Many are designed to erode public confidence, challenge governmental legitimacy, and reshape social narratives. The cyber intrusion into Iranian state television and the broadcast of anti-government messages, for example, produced relatively limited physical damage but carried considerable symbolic significance. By challenging the state's ability to control official channels of communication, such operations reinforced perceptions of vulnerability and contested existing narratives of state authority. From a constructivist perspective, these activities constitute a form of narrative competition, in which cyber operations seek to influence identities and collective perceptions as much as physical infrastructure (Bada & Nurse, 2020: 1).

The comparatively low cost and limited lethality of cyber operations further encourage their use as instruments of calibrated retaliation. As

Borghard and Lonergan argue, many cyber operations are intended less to achieve immediate operational effects than to generate psychological impact, demonstrate capability, and communicate strategic resolve (Borghard & Lonergan, 2019: 131, 137). Consequently, repeated cyber exchanges not only deepen bilateral distrust but also contribute to broader patterns of regional insecurity by institutionalizing adversarial expectations and reducing opportunities for confidence-building and diplomatic engagement.

3.4. Transformation in Diplomacy and the Emergence of New Arenas of Rivalry: Influence Operations and Narrative Warfare

The previous sections demonstrated how the cyber rivalry between Iran and Israel has generated a vicious cycle of reciprocal attacks and deepening distrust. As an extension of this process, the rivalry has expanded beyond the purely technical domain and physical infrastructure into the realm of perceptions and narratives—evolving into a form of narrative warfare (Pijpers, 2022: 62). By focusing on influence operations and narrative warfare, this section demonstrates how cyber conflict has transformed diplomatic dynamics and created new arenas of strategic competition. From a constructivist perspective, these developments depend not only on material capabilities but also on actors' ability to shape ideas, identities, and collective perceptions among the public and political elites (Bolton, 2021: 127).

Unlike destructive cyberattacks such as Stuxnet, influence operations in cyberspace are not intended to destroy physical infrastructure. Instead, their principal objective is to reshape the adversary's cognitive environment by manipulating perceptions and influencing autonomous decision-making. Such operations remain below the threshold of the use of force, enabling states to pursue strategic objectives without escalating into direct military confrontation (Pijpers, 2022: 51).

The principal instruments of this approach are strategic narratives and information warfare (Pijpers, 2022: 62). From the perspective of ontological security theory, information warfare can deliberately target a nation's ontological security (Bolton, 2021: 1). By distorting the information environment, these operations reshape the relationship between events and national narratives and, by fostering divisions within domestic narratives, intentionally generate ontological insecurity among a country's population (Bolton, 2021: 127). In this domain, perception itself constitutes a strategic form of power, and regional actors have rapidly adapted to this reality (Haberfeld & Azani, 2025: 9).

The rivalry between Iran and Israel, as two leading actors in gray-zone warfare (Azad et al., 2022: 1; Eisenstadt, 2021: 3), provides a compelling illustration of the emergence of narrative warfare. Both countries employ cyber capabilities not only to disrupt critical infrastructure but also to conduct influence operations aimed at intensifying domestic instability.

A. Iran's Influence Operations

Iran has utilized platforms such as TikTok to shape public perceptions of war and disseminate disinformation. Supported by artificial intelligence, these operations facilitate the rapid production and large-scale dissemination of deceptive content while requiring relatively limited financial and technical resources (Haberfeld & Azani, 2025: 9). Their principal objective is to deepen social polarization and undermine public trust in Israeli governmental institutions.

B. Israel's Cyberattacks on Iran's Critical Infrastructure

Beyond their technical objectives, Israel's cyberattacks on Iran's critical infrastructure seek to weaken Iran's official narrative of state control and resilience in the face of external threats. Repeated cyber operations targeting nuclear and energy facilities, when combined with coordinated information campaigns, reinforce a narrative portraying Iran as persistently vulnerable. From a constructivist perspective, this strategy can be understood as an effort to challenge and reconstruct Iran's narrative of power by emphasizing vulnerability rather than fundamentally redefining its national identity.

This strategic competition has gradually evolved into increasingly sophisticated forms of narrative warfare. Claims regarding the infiltration of Israeli security institutions, such as the Shabak, and the publication of allegedly classified documents by hacker groups attributed to Iran represent advanced examples of such operations. Although these claims have not been officially confirmed by Israeli authorities, targeting one of Israel's most sensitive security institutions is intended to generate ontological insecurity among political elites and the broader public. The implicit message is straightforward: if intelligence agencies cannot protect themselves, how can they ensure national security? Such narrative operations deepen public distrust while further complicating diplomatic interactions.

The process through which this operation generates ontological insecurity can be explained through the theoretical framework developed by Pijpers and Bolton.

Step One: Technical Attack and Symbolic Messaging

The alleged compromise of a security and intelligence institution such as the Shabak represents not merely a technical incident but also a powerful symbolic act. Whereas the compromise of a state broadcasting system primarily conveys a message to the general public, an attack targeting the Shabak sends a message directly to political and security elites. It demonstrates that even the state's most secure and sensitive institutions are vulnerable to penetration (Pijpers, 2022: 73).

Step Two: Publication of Documents and Narrative Construction

By publishing documents allegedly obtained from Shabak systems, the hacker group constructs a strategic narrative. At this stage, the objective is not necessarily to provide definitive technical proof of the intrusion but rather to establish a persuasive narrative. The publication seeks to convince both domestic and international audiences that Iran's intelligence capabilities exceed previous assumptions and are capable of penetrating the core of Israel's security apparatus. This narrative directly challenges Israel's longstanding image of intelligence superiority and invulnerability and illustrates the application of Pijpers' theoretical framework at the elite level.

Step Three: Generation of Ontological Insecurity

The operation subsequently undermines public perceptions of security. Citizens may begin to question whether a government incapable of protecting its own intelligence institutions can effectively guarantee national security against growing threats. Such doubts directly erode the target society's ontological security by reinforcing perceptions of instability and vulnerability (Bolton, 2021: 127).

Step Four: Erosion of Credibility and Narrative Replacement

Finally, the perceived compromise of a highly credible security institution such as the Shabak weakens public confidence in the Israeli government's official narratives. This erosion of credibility creates opportunities for alternative narratives—often promoted by opposition groups or foreign actors—to gain greater acceptance. Over time, this process diminishes the government's capacity to sustain its official narrative regarding its ability to manage national security threats.

A similar process of generating ontological insecurity can be observed in the cyberattack targeting Iranian state television. The compromise of Iran's national broadcasting system and the transmission of anti-government messages constitute a clear example of narrative warfare over public perceptions. From a constructivist perspective, the process unfolds as follows:

Step One: Technical Attack

The successful compromise of the state television broadcasting system constitutes a technical achievement while simultaneously conveying a powerful symbolic message (Pijpers, 2022: 73).

Step Two: Symbolic Communication

The broadcasting of anti-government messages and images excluded from the state's official narrative demonstrates that the government's informational boundaries are vulnerable to external interference (Pijpers, 2022: 73).

Step Three: Generation of Ontological Insecurity

This event challenges citizens' perceptions of security by prompting them to question whether a government unable to protect its own broadcasting system can effectively safeguard more critical infrastructure, including water, electricity, and energy systems. Such uncertainty directly undermines society's ontological security (Bolton, 2021: 127).

Step Four: Erosion of Trust and Narrative Replacement

Ultimately, the cyberattack weakens public trust in the government's official narratives while creating favorable conditions for alternative narratives promoted by opposition movements or foreign actors. As these competing narratives gain greater credibility, the state's ability to maintain its informational authority is progressively diminished.

The emergence of narrative warfare and influence operations has had a profound impact on regional diplomacy. This form of competition functions as a mechanism of "escalation without direct conflict" (Pijpers, 2022: 63), largely because it enables plausible deniability (Pijpers, 2022: 96). The difficulty of reliably attributing cyber operations undermines diplomatic efforts to de escalate tensions, as neither side acknowledges responsibility for hostile actions, thereby limiting opportunities for meaningful negotiations. Consequently, diplomacy is no longer confined to official channels of interstate negotiation; it has increasingly expanded into the public sphere, digital media, and social networking platforms, where competing narratives are constructed, contested, and disseminated.

In sum, influence operations and narrative warfare—as integral components of gray zone warfare—have transformed the nature of interstate rivalry from predominantly military confrontation into a contest over ideas, identities, and legitimacy. By targeting the cognitive and psychological dimensions of society, these operations generate unprecedented levels of distrust, further complicating diplomatic engagement and contributing to the long term instability of regional relations.

Conclusion

This study sought to answer the central research question: How do cyber wars reshape diplomatic and security dynamics in Southwest Asia? Drawing upon a constructivist theoretical framework and focusing on the cyber rivalry between Iran and Israel, the analysis demonstrates that cyber conflict represents far more than a transformation in military capabilities. Rather, it is fundamentally embedded in social interactions, identity construction, and cognitive processes that reshape regional politics.

The findings indicate that cyber warfare has transformed regional security and diplomacy at three interconnected levels.

Identity and Perceptual Dimension. Cyber operations such as Stuxnet did not merely inflict physical damage on Iranian infrastructure; they also generated an ontological crisis that contributed to redefining Iran's identity

from that of a passive target to an active and retaliatory cyber actor. This transformation in identity influenced Iran's security doctrine and reinforced a self perpetuating cycle of reciprocal cyber operations.

Normative Dimension. In the absence of internationally accepted norms governing state behavior in cyberspace, the cyber rivalry between Iran and Israel operates within a persistent normative vacuum. Under these conditions, offensive cyber activities are frequently interpreted as violations of implicit red lines, thereby intensifying retaliatory dynamics and strategic instability. Rather than reducing tensions, the ambiguity surrounding attribution has become a strategic resource that enables both parties to sustain competition within the gray zone while avoiding direct military escalation.

Interactional and Diplomatic Dimension. Repeated patterns of cyber interaction continuously reproduce and deepen mutual distrust. As a result, cyber diplomacy has become increasingly constrained, while the principal arena of competition has shifted from formal diplomatic negotiations to narrative warfare and influence operations. Within these new arenas, the primary objective is no longer the destruction of physical assets but the manipulation of perceptions, the contestation of identities, and the erosion of the adversary's political legitimacy—all of which have significant implications for domestic stability and international diplomacy.

From a theoretical perspective, this study demonstrates that constructivism provides a more comprehensive analytical framework for understanding cyber conflict than approaches that focus primarily on material capabilities. While Realist and Liberal theories explain important aspects of strategic competition, they are less capable of capturing the social, ideational, and normative dimensions that characterize cyberspace. This study argues that power in cyberspace derives not only from technological superiority but also from the ability to construct meaning, shape identities, and influence dominant narratives. In doing so, it contributes to the growing constructivist literature on cybersecurity and broadens the theoretical scope of international relations scholarship concerning cyber conflict.

The findings also carry important policy implications. Managing cyber rivalry in Southwest Asia cannot be achieved solely through expanding offensive or defensive cyber capabilities. More sustainable approaches to conflict management require efforts to reduce mutual distrust, reshape adversarial perceptions, and develop shared norms governing responsible state behavior in cyberspace. Accordingly, regional cyber diplomacy should extend beyond technical negotiations to include sustained dialogue on mutually recognized red lines, confidence building measures, and the mitigation of hostile strategic narratives.

Like all research, this study is subject to several limitations. Its exclusive focus on the Iran–Israel cyber rivalry provides analytical depth but limits the broader generalizability of the findings to other regional or international

cyber rivalries. In addition, the classified nature of cyber operations restricts empirical analysis to publicly available information and secondary sources, making it difficult to verify certain operational details.

Building upon the findings of this study, several promising avenues for future research emerge. First, comparative analyses of other cyber rivalries—such as those between China and the United States or Russia and NATO—could further evaluate the explanatory power of constructivist theory across different geopolitical contexts. Second, greater attention should be devoted to the role of non-state actors, including hacktivist networks and cybercriminal organizations, in shaping identities, norms, and patterns of interaction in cyberspace. Finally, future studies should examine how emerging technologies, particularly artificial intelligence and quantum computing, may transform narrative warfare, attribution processes, and the strategic use of plausible deniability in interstate cyber competition.

References

Anderson, C., & Sadjadpour, K. (2018). *Iran's cyber threat: Espionage, sabotage, and revenge*. Carnegie Endowment for International Peace.

Azad, T. M., Haider, M. W., & Sadiq, M. (2022). Understanding gray zone warfare from multiple perspectives. *World Affairs, 186*(1), 81–104. https://doi.org/10.1177/00438200221141101

Bada, M., & Nurse, J. R. C. (2020). The social and psychological impact of cyberattacks. In V. Benson & J. McAlaney (Eds.), *Emerging cyber threats and cognitive vulnerabilities* (pp. 73–92). Elsevier. https://doi.org/10.1016/B978-0-12-816203-3.00004-6

Bahgat, G., & Ehteshami, A. (2019). Iran's defense strategy: The navy, ballistic missiles and cyberspace. *Strategic Studies Quarterly, 13*(3).

Bahoosh Fardeghi, M. (2017). Examining the concept or metaphor of national security in structuralist theory. *Journal of Politics, 14*(37), 101–125. **(In Persian)**

Bolton, D. (2021). Targeting ontological security: Information warfare in the modern age. *Political Psychology, 42*(1).

Borghard, E. D., & Lonergan, S. W. (2019). Cyber operations as imperfect tools of escalation. *Strategic Studies Quarterly, 13*(3).

Council on Foreign Relations. (2020). *Attack on Israeli water utilities*. https://www.cfr.org/cyber-operations/attack-israeli-water-utilities

CyberCX Intelligence. (2024). *Cyber impacts of Iran–Israel military escalation*. CyberCX. https://cybercx.com.au/blog/cyber-impacts-of-iran-israel-military-escalation

Eberle, J., & Daniel, J. (2022). Anxiety geopolitics: Hybrid warfare, civilisational geopolitics, and the Janus-faced politics of anxiety. *Political Geography, 92*.

Eisenstadt, M. (2021). Iran's gray zone strategy. *PRISM, 9*(2).

Global Studies. (2024). Atlantis highlights in social sciences, education and humanities (Vol. 33). https://doi.org/10.2991/978-94-6463-646-8_4

Golmohammadi, V., & Jamshidi, T. (2022). Cyber deterrence and evolution in Israel's security-defense doctrine. *Journal of Political Geography Research, 7*(4). (In Persian)

Haberfeld, D., & Azani, E. (2025, June). Iranian TikTok campaign seeks to shape war perceptions using AI [Special report]. International Institute for Counter-Terrorism, Reichman University. https://ict.org.il/wp-content/uploads/2025/06/Haberfeld-and-Azani_Iranian-TikTok-Campaign-Seeks-to-Shape-War-Perceptions-using-AI_2025_06_20-4.pdf

Harknett, R. J., & Smeets, M. (2022). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies, 45*(4). https://doi.org/10.1080/01402390.2020.1732354

Katzenstein, P. J. (Ed.). (1996). *The culture of national security: Norms and identity in world politics*. Columbia University Press.

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

Koohsarian, H., Partovi, M., Akraminia, M., & Shakib, A. (2021). The impact of scientific and cyber threats on the armed forces of the Islamic Republic of Iran and national security. *Quarterly Journal of War Studies, 3*(10). **(In Persian)**

Mark, D. (2024). Influence of cyber warfare on diplomatic relations between rival states in Nigeria. *American Journal of International Relations, 9*(5), 40–51.

Mirzaei, M., & Qorashi, Y. (2024). Cyber Trojan horses in Asia: An analysis of the Israel–Iran confrontation after the Stuxnet attack. *Iranian Journal of Asian Studies, 1*(1). https://doi.org/10.22099/IJAS.2024.51157.1014 **(In Persian)**

Nasiri, B., Torabi, Gh., & Rezaei, A. (2024). *Cyber war and its consequences on Iran's national security*. Social Studies of Iranian History and Culture. **(In Persian)**

Noormohammadi, M. (2011). Soft war, cyberspace and security of the Islamic Republic of Iran. *Cultural Strategy*, (16). **(In Persian)**

Office of the Supreme Leader of the Islamic Republic of Iran. (2012, September 8). *Speech to officials of the Atomic Energy Organization and nuclear scientists*. https://farsi.khamenei.ir/news-content?id=101670

Pijpers, B. M. J. (2022). *Influence operations in cyberspace: On the applicability of public international law during influence operations in a situation below the threshold of the use of force* (Doctoral dissertation, University of Amsterdam).

Pour Ebrahimi, A., Safarnejad, D., & Kashef, H. (2017). Cyber defense strategies of the Islamic Republic of Iran against psychological warfare threats. *Quarterly Journal of Soft Warfare Studies, 6*(22). **(In Persian)**

Siman, B. (2022). *Hybrid warfare is not synonymous with cyber: The threat of influence operations* (Security Policy Brief No. 155). Egmont Institute.

Siman-Tov, D., & Even, S. (2020). *A new level in the cyber war between Israel and Iran*. Institute for National Security Studies. https://www.jstor.org/stable/resrep25542

Tasnim News Agency. (2016, November 5). Fototitr/Salehi: Babat-e hamle-ye Stuxnet moteshakerim, https://www.tasnimnews.ir/fa/news/1395/08/15/1231320/

Tasnim News Agency. (2016, November 7). The Atomic Energy Organization has not yet responded to the letter of the Prosecutor General's Office. https://www.tasnimnews.ir/fa/news/1395/08/17/1233536/

Torres Soriano, M. R. (2017). Proxy wars in cyberspace. *Journal of the Spanish Institute for Strategic Studies*, (9).

Van Dine, A. (2017). After Stuxnet: Acknowledging the cyber threat to nuclear facilities. In M. Cancian (Ed.), *Project on Nuclear Issues: A collection of papers from the 2016 Nuclear Scholars Initiative and PONI Conference Series* (pp. 100–114). Center for Strategic and International Studies.

Wendt, A. (1999). *Social theory of international politics*. Cambridge University Press.

Xu, M., & Lu, C. (2021). China–U.S. cyber-crisis management. *International Strategy Review, 3*(1). https://doi.org/10.1007/s42533-021-00079-7