OPEN ACCESS

Middle East Research Journal of Humanities and Social Sciences
ISSN 2789-7761 (Print) | ISSN 2958-2040 (Online)
Frequency: Bi-Monthly
DOI: https://doi.org/10.36348/merjhss.2026.v06i02.001

KUWAIT SCHOLARS PUBLISHER
Website: http://www.kspublisher.com/
Email: office@kspublisher.com

Study of the Impact of Cyber Threats on Community Security

Ali Adel Hamza[1*]
[1]College of Veterinary Medicine, Al-Qasim Green University, 51013 Babylon, Iraq

Abstract: Today, the world is undergoing a number of revolutions and shifts in all areas, due to the significant revolution in information communication technology. The growth of trans connectivity in all spheres has given rise to a new domain for relations among people, communities and states: cyberspace. This space is characterized by very rapid development and great ambiguity, and the misuse of cyberspace has created an environment full of risks, threats, and conflicts, posing a serious threat to society and the state. Concepts of power, conflict, and war have changed and become linked to the nature of cyberspace. The emergence of cyber threats represents a new form of threat that relies on the use of modern digital technologies to achieve multiple objectives. Many actors have threatened the security of societies by spreading their ideas and values on social networks to reach as many individuals as possible, recruiting and teaching them how to use explosives, hacking websites, and other illegal criminal activities, infiltrating and spying on sensitive networks, and sending threatening messages to countries to coerce them. With the emergence of this cyber-threat to societal stability, countries including Iran and Saudi Arabia have hastened to establish civil and military bodies and institutions, enact legal legislation, and develop specific strategies to confront current and future cyber-threats to defend their security. Additionally, they are working at regional and international levels to create a safer cyberspace.

Keywords: Cyber Threats, Community Security, Cybersecurity, Cybercrime.

Research Paper

***Corresponding Author:**
Ali Adel Hamza
College of Veterinary Medicine, Al-Qasim Green University, 51013 Babylon, Iraq

How to cite this paper:
Ali Adel Hamza (2026). Study of the Impact of Cyber Threats on Community Security. *Middle East Res J. Humanities Soc. Sci, 6*(2): 30-38.

Article History:
| Submit: 03.02.2026 |
| Accepted: 04.03.2026 |
| Published: 07.03.2026 |

INTRODUCTION

Cyberspace has become one of the most prominent arenas of interaction and conflict in the contemporary international system, in light of the rapid transformations brought about by the information and communication technology revolution and the accompanying unprecedented expansion in reliance on digital systems across various aspects of political, economic, social, and cultural life. Security is no longer confined to its military traditional aspects, and other dimensions, like cybersecurity (the most important of them), have added to the concept, showing that it is a relevant factor for the internal security and societal security of the State.

Cyberspace misuse has resultant in a rise of non-conventional threats of a transnational nature that are vexing and challenging to trace, which affect the individuals, institutions cot-ntries interchangeably. This has affected the society security system negatively giving rise to destruction of ethics, spread of hate mongering ideologies, manipulation in public opinion and damaging infrastructure and economy. The risk of such threats goes up in societies which undergo fast digital opening without matching legal and enough technical and human capacities.

The Importance of the Study

This study is important as it emphasises that the relationship between cyber threats and societal security is complex, which to date remains an unsolved security challenge at both theoretical and practical levels. It is also valuable in exploring consequences of these threats on several levels (individual, society and state) related to the latter's responses –with empirical emphasis on those of Iran and Saudi Arabia, in framing strategies and institutional/legislative frames– for coping with cyber risks. The present study contributes to how the understanding of the security concept is changing from traditional-security oriented towards comprehensive.

The Study's Problem Statement

The main research question of this study is as follows:

- How much cyber-threats are involved in societal security and how have, at the status of

changing nature of threat/security, states particularly Iran and SA reacted to that?

- This primary research question gives rise to several sub-questions, in particular:
- What is Cyber threat, Characteristics and Trend?
- How do cyber threats affect social security at multiple levels?
- What are the risk mitigation measures that countries have followed?
- Does Community Security in Cyberspace lead to increased internal stability?

Study Hypothesis

Based on the discussion above, this article assumes that cyber threats escalation directly undermines societal security through individuals, institutions and value/cultural structures of the state. It also suggests that the effectiveness of states in facing these threats depends on the convergence of their cyber strategies, updating laws, improving technical and human resources and enhancing regional and international cooperation.

Study Methodology

This research used a descriptive-analytical method, describing the phenomenon and analyzing dimensions of cyber threats and their consequences on societal security. It also used a comparative model to analyse Iran and Saudi Arabia's handling of cyber threats. It further applied Copenhagen School's widened security analysis, especially the concept of "securitization" to map out the process that a cyber-threat moves from a mere technical issue to an societal-security issue.

Section One: Cyber Threats

The virtual war has seen several developments and tensions in the recent past, on ground and in the cyber world. The most outstanding of these has been the current wild growth of cyber threats on the Web: both states, and organizations, and people have initiated this process that spreads moral and material losses. Cyber-threats have become one of the most urgent issues that affect states, governments as well as ordinary people, considering the variety of agents involved in them and their impact, not being easy to track where they come from or who is behind them and even expensive consequences. As a result, cyberspace has become a battlefield for confrontations as shadow wars, including espionage, hacking and databases manipulation that threatens national security and social order of some countries. This section will address:

First Requirement: The Concept of Cyber Threats

The primary challenge in evaluating the provisions of national and international law regarding the regulation of cyber threats lies in defining the nature and scope of the issue at hand. Activities occurring in cyberspace, considered the fifth domain after land, sea, air, and space, may not conform to the traditional principles governing conflict. The armed element is within the framework of the law of war, and therefore we will address the concept of cyber threats through the following paragraphs:

First: The Meaning of Cyber (Cyber) Linguistically

Before the word "cyber" meant anything, there was the field of cybernetics, or control science, which emerged in the late 1940s by a group of specialists in various fields such as biology, engineering, and social sciences. This term, cybernetics, was first used academically by Norbert Wiener in 1948 when he used it to refer to a self-regulating mechanism in his book titled "Cybernetics," meaning control and communication in the animal world and mechanical machines 1)[1] (.

Understanding how these systems operate necessitates examining the origin of the word "cyber," which derives from the Greek word "Kubevav" (Kubernetes2)[2](,meaning "which means helmsman" 3)[3](. This term initially appeared in science fiction literature, signifying remote command or control 4)[4](.

Secondly: Cyber Threats as a Term

For over a decade, analysts have speculated about the potential consequences and widespread material and economic damage resulting from electronic development, such as disrupting the stock market, shutting down or remotely detonating a nuclear reactor, causing power outages for air navigation systems, manipulating the flight paths of civilian aircraft, and other incidents caused by technologies unfamiliar to the international community [5[5]].There are two main, differing approaches to defining these threats [6].6)

1[1] -Norbert Wiener, "Cybernetics or control communication in the machine", M.I.T., Press, Second Edition, Cambridge, Massachusetts, 1948 ،p18.

2- Mustafa Tlass, The Scientific and Technological Revolution and the Development of the Armed Forces, Dar Tlass for Studies, Translation and Publishing, 3rd Edition, Damascus, 2003, p. 318

3[3] -Oxford Dictionaries. Blog. Oxford dictionaries. Com

4[4] -Jullia Cresswell, "Oxford Dictionary of word origins. Cybernetics" , Oxford Reference online, Oxford University Press, 2010

5[5] - Saham Hassan Ali Al-Shammari, "Manifestations of Cybersecurity and Media Practice and their Relationship to the Virtual Psychological Warfare Industry," International Studies Journal, Center for Strategic and International Studies, University of Baghdad, Issue 38, 2020, p. 150

6[6] -Oona A. Hathaway, Rebecca Crootof , Philip Levitz, Haley Nix, Aileen Nowlan , William Perdue & Julia Spiegel, "The law of Cyber-Attack", California law review ,2012 ,p.824

1- The Narrow Approach

This approach focuses on the threat itself, and it is the approach adopted by the United States and its allies. An example of a definition within this approach is that adopted by the US Strategic Command in 2007 regarding the use of electronic means for military purposes. It defined it as "the manipulation of computer system operations to prevent adversaries from effectively using them, as well as the infiltration of information systems and communication networks to collect, acquire, and analyze the data they contain" [7].7)

The first official definition of its kind, published by the Joint Chiefs of Staff in 2011 after the establishment of the US Cyber Command, is found in the Dictionary of Military Uses. It defines a cyber-threat as "hostile activity using computers, networks, or related systems, aimed at disrupting or destroying an adversary's cyber-systems, necessarily on targeted computer systems or the data itself. The activation or impact of a cyber-threat may be separated by time or space from the cyber-activity" 8)[8](.It is also defined as "the environment in which people connect with each other through devices connected to the Internet" [9].9)

2- The Broad Approach

In contrast to the narrow approach officially adopted by the United States, the Shanghai Cooperation Organization (SCO) 10)[10] (adopted a more expansive approach to cyber threats. This organization expressed concern about the threats posed by the potential misuse of modern information and communication technologies for purposes that undermine international security and stability, both military and civilian 11)[11](.Members of this organization (i.e., proponents of the broad approach) consider the dissemination of information harmful to the political, social, and economic systems, as well as the spiritual, moral, and cultural spheres of other countries, to be among the main threats to cybersecurity [12].12)

It is clear to the researcher that the SCO has adopted a broad view of cyber threats, encompassing any use of technology to undermine political stability. The discrepancy in the content of these two approaches (the concept of cyber threats) highlights the urgent need for a clear and internationally agreed-upon definition of such threats.

Third: The Emergence of Cyber Threats

The Emergence of Cyber Threats is Directly Linked to Two Significant Events

1. The first event: The introduction of computers in the mid-1950s as a tool for processing and storing information digitally [13].13)
2. The second event: The emergence of the World Wide Web (the Internet), which revolutionized human life by enabling communication and the transmission of information at extremely high speeds through a torrent of data sent via the Internet [14].14)

Fourth: Characteristics of Cyber Threats

These features of the cyber threats include:

Modernity and Development:

The features of cyber threats are modern technology oriented, being the achievement of human technological development. The electronic computer has, on the other hand, become a tool (in all senses of the word) and an environment where this kind of threat actively plays out () g_{\text{K}}. They are therefore also subject to ongoing development, diversification and advance in both technology and method as they relate to technological advancement in general and the protection of essential non bilateral national interests [15].15)

2- Its Reciprocal Nature:

It is both an opportunity and a threat. In the realm of defensive measures, cyber threats are an opportunity because they represent a tool for acquiring information. They provide a wealth of information about the characteristics of the enemy's electronic equipment

7[7] -K. Saalbach, "Cyber war, Methods and Practice", version 2.0, university of Osnabruck-17 Jun 2014, p.8.

8[8] -James E. Cartwright, Memorandum for Chiefs of the Military Serve. Commanders of the Combatant Commands, Dirs. Of the Joint Staff Directories on Joint Terminology for Cyberspace Operations ،5 No. 2011, p18.

9[9] -Mohammed Al-Amin Al-Bashri, Investigating Computer and Internet Crimes, Arab Journal of Security Studies and Training, Riyadh, Saudi Arabia, 1422 AH, p. 10

10[10] -Shanghai Cooperation Organization (SCO): It was founded in Shanghai on June 15, 2001 and became an official organization according to the principles of international law in 2002. It consists of China, Russia, and most of the former Soviet republics in Central Asia, as well as observers including Iran, India and Pakistan. Its objectives include combating terrorism, extremism and separatist movements, and countering the arms trade. However, some see it as a military alliance to confront the North Atlantic Treaty Organization (NATO).

11[11] -Oona Hathaway, op. cit., p.825

12[12] -Shanghai Cooperation Agreement, Annex I, p. 203

13[13]-Christopher c. joyner and Catherine Lotrionte," Information Warfare as International Coercion: Elements of a Legal Framework", European Journal for International Law, Vol. (12). london.2001. p.825

14[14] -Ibid.p.826.

15[15]- Ali Abdul Rahim Al-Aboudi, "The Obsession with Cyber Warfare and its Repercussions on International Peace and Security," *Journal of Political Issues*, College of Political Science, Al-Nahrain University, Issue 57, Baghdad, 2019, p. 99.

and about the conditions and trends of the expected combat zone [16].16)

3- Difficulty in Proving: Cyber threat perpetrators use anonymous websites and encryption to conceal their identities during their attacks (17[17].

4- Transnational Nature:

One of the most important characteristics of cyber threats is their transcendence of geographical boundaries, thus acquiring an international nature, especially after the emergence of the internet [18].18)

5- Material Cost:

Cyber threats are less materially costly than traditional threats. A war can be waged at the cost of a tank using new weapons and human expertise [19].19)

6- Change in the Nature of the Parties and Objectives:

For the parties involved, the information revolution has created a fifth arena of warfare, not limited to states as is the case in traditional warfare [20].20)

7- Cyber Threats Are Characterized by Their Immense Destructive Capabilities Without Requiring A Physical Presence on the Battlefield:

Cyber-threat perpetrators do not need to be physically present at either the location where the threat originates or the location where its effects are felt [21].21)

The researcher believes that cybernetics in the twenty-first century is a significant part of the lives of individuals and both formal and informal institutions worldwide; therefore, all these parties, whether individuals, governments, or organizations, may face risks from any party within this virtual space. Hence, there must be regulations that protect users from these risks. There are important proposals from various countries in this regard, which should be taken into consideration according to the needs of each individual and institution.

Section Two: The Dangers of Cyber Threats to Community Security

First: The Dangers of Harming Individuals

One of the most significant and prominent flaws in the new governance arrangements was the political structure that governed the joints of the political system and state institutions. Social components became hostage to the orientations and interests of the leaders and political parties they claimed to represent. The political structure later transformed into a system of sectoral leadership. This involves targeting a specific group of individuals or a particular person to obtain important information related to their personal account, whether it be their bank account or online presence. This constitutes the following crimes:

1. **Identity Theft:**

In this case, the perpetrator lures the victim and extracts information from them indirectly. They target private information to exploit it for financial gain, defame individuals, or sabotage or corrupt relationships, whether social or professional (22[22].

2. **Threatening Individuals:**

Here, the perpetrator may steal private personal information, whether true or false, and then send it via social media or email to numerous individuals. The purpose is to defame the victim and psychologically destroy them.

3. **Intolerance and Hatred:**

Intolerance in all its forms leads to the exclusion of others and causes armed conflicts that entrench hatred, which contradicts pluralism, dialogue, and tolerance.

4. **Cyber-Fraud:**

This refers to "deliberate conduct or actions by an individual or a group of individuals that burden or cause additional burdens to any other parties as a result of using unethical practices to obtain an unfair or illegal advantage" [23].23)

Second: Risks of Harm to Institutions:

1- **System Breaches:**

Cybercrimes cause significant losses to institutions and companies, including financial losses

16[16]-Faisal Muhammad Abdul Ghaffar, "Electronic Warfare", 1st ed., Al-Janadriyah Publishing and Distribution, Amman, 2016, p. 30.

17[17] - Israa Sharif Al-Kaoud, "The Cyber Impact on the National Security of Active States (The United States as a Model)," *Journal of Political Science*, College of Political Science, University of Baghdad, Issue 64, 2022, p. 10.

18[18] -Shaikha Hussein Al-Zahrani, "Confronting International Law with Cyber Attacks," 1st ed., Dar Al-Nahda Al-Arabiya, Dubai, 2021, p. 24.

19[19] -Ashraf Al-Saeed Ahmed, *Electronic Piracy*, Dar Al-Nahda Al-Arabiya, Cairo, 2013, p. 46.

20[20]-Adel Abdel Sadek, Cyberspace Weapons in Light of International Humanitarian Law, Library of Alexandria, Alexandria, Egypt, 2016, p. 59.

21[21] -Sulafa Tariq Al-Shaalan, Adapting the Use of Electronic Warfare in Armed Conflicts in Accordance with International Humanitarian Law, Kufa Journal of Legal and Political Sciences, College of Law - University of Kufa, Volume 9, Issue 26, 2016, p. 6

22[22]-Alaa Muhammad Rahim, Security and Emerging Crimes: A Socio-Political Study, International Studies Journal, Center for Strategic and International Studies, University of Baghdad, Issue 62, 2023, p. 11

23[23] - Nihad Kreidi, Crime and Fraud in the Electronic Environment, Beirut, 2008, pp. 14-16.

and system damage. The criminal breaches the information systems of institutions and companies to obtain important information and then uses this information for personal purposes, such as stealing money and destroying the company's support systems for managing companies. This causes serious losses to the institution. It is also possible to steal the personal information of employees of institutions and companies and incite or blackmail them in order to destroy the internal systems of institutions. Then, in most cases, criminals install spyware on the systems and control them; to achieve some material and political gains, cybercrimes related to hacking networks, accounts, and systems certainly bring economic losses to the country, and they threaten the national security of the state, especially if they develop and are not controlled and the hacking criminals are not combated. Cybercrimes represent 17% and are increasing day by day, and if this indicates anything, it indicates that we are all in danger. Also, hacking and controlling websites by criminals and then using them to destabilize the country's security, control the minds of young people, and incite them to carry out illegal acts [24].24)

2- **System Destruction:**

This type of destruction utilizes well-known methods, such as computer viruses. These viruses spread within the system, causing damage, chaos, and destruction. This results in significant losses for organizations and can even destroy the main server used by institutions to facilitate their operations. This is achieved by hacking employee accounts and then accessing all accounts simultaneously, causing a complete server failure and subsequent destruction, leading to losses for the organization.

3- Financial Crimes:

a. **Bank Account Seizure:** This involves hacking into bank accounts, including those belonging to the government and private institutions, as well as stealing and seizing credit cards.
b. **Intellectual Property and Literary Rights Violation:** This refers to creating pirated copies of software or files and selling them online 25)[25].

Third: Threats Targeting State Security:

a. **Spyware:** Spyware has become widespread in technological circles. Some of it is used for political, economic, and military purposes, as well as for stealing intellectual property. (26[26]. Criminals install spyware in various ways. Once they succeed, they steal information, access military data, or steal intellectual property or inventions. Therefore, it is one of the most dangerous cybercrimes.
b. **Terrorist Organizations' Use of Deception:** Terrorists rely on modern communication methods and the internet to mislead others, which can lead to destabilizing the country and creating chaos in order to implement political interests and terrorist plots. They also manipulate the minds of young people to persuade them of personal gain [27].27)

Third Section: Integrating Community Security within Cyberspace

The expanding relationship between states and cyberspace, and the resulting cyber-warfare, has led to numerous risks to national security and a shift towards international political interactions. The most prominent of these risks include:

1. The proliferation of cyber threats that threaten essential state structures -civilian and military alike. This indirectly takes effect by intermediaries and service providers that may paralyse information systems carried out on the premises of these facilities. The strategic implications are that whoever owns and has the capability to execute attacks with this class of power, it is very significant in peacetime as well as during war [28].
2. While the multiplication and consolidation of power which is raising the rate on cyber space, was termed as institution power in international policy. This means that it is a force in power among actors, which allows them to obtain their equations of values and interests at the expense of the others [29], as well as in determining knowledge elements or partial parameters orienting the public action.

The US is one of the great powers that has arisen because of cyberspace. Following the end of the Cold War, when the United States held and monopolized power resources, we are witnessing a diffusion of power that is not contained by states but includes non-state actors as well as individuals [30].

3-Militarization of Cyberspace

Whose goal is to prevent any threat coming form cyberspace prompting the rise of cyber defense and security policy. This has led to a cyber arms race to

24[24]- Ghada Nassar, Terrorism and Cybercrime, Cairo: Al-Arabi Publishing and Distribution, 2017, p. 21.
25[25] -Ahmed Hossam Taha Tamam, Crimes Arising from Computer Use, Criminal Protection of Computers, PhD Thesis, Unpublished (Tanta University: Faculty of Law, 2000) pp. 210-211.
26[26] -Abeer Hamid Siham Mahdi, Ammar Hamid Yassin, The Problem of Identity in Iraq: A Vision of Challenges and the Future of Building an Iraqi National Identity after 2003, The Political and International Journal, Issue 28-29, 2015 , p389.
27[27] -Mohamed Ali Al-Aryan, Cybercrimes, Alexandria: University Publishing House, 2004, pp. 67-68.

protect national infrastructure and security and to invest in developing cyber capabilities within militaries.

4- Preparing for future wars, as many countries have adopted information warfare as a strategy for the future. This strategy aims to disrupt and instigate chaos in adversaries' decision-making processes by penetrating their systems and exploiting and transferring their information [28].28)

5- Upgrading Defensive and Offensive Capabilities:

Countries have sought to modernize their defensive activities to counter the risks of cyber warfare, investing in and securing information infrastructure, upgrading military capabilities, and enhancing their readiness for such warfare through training [29].29)

6- However, the problem of the world entering a cyber-arms race remains in determining the nature of the weapons possessed by others. How can the international community have the capacity to intervene quickly to contain them? It is not possible to activate inspection as a monitoring mechanism, as is the case with nuclear weapons. Building military capabilities in the cyber domain requires essential elements, including:

First:

Acquiring modern technology and cyber-protection systems and developing offensive human capabilities to achieve technological superiority.

Second:

Developing offensive capabilities, which depends on building indigenous capabilities or utilizing specialized individuals and companies, as well as developing the capacity to counter cyberattacks.

Third:

Working to provide budgets allocated to developing offensive and defensive capabilities, especially since their low cost means they do not require huge budgets compared to what is spent on traditional armies. The requirements for the availability of international cybersecurity lie in ensuring the integrity of electronic defenses [30].30)

Conflicts in cyberspace have increased due to the lack of trust between countries, in addition to... The tremendous developments in cyberspace have prompted states to accelerate changes in their security doctrine by including cyber-power as a key determinant of a state's strength and its ability to resolve conflicts. This has contributed to the existence of conflicts and wars in cyberspace between international and non-state actors. Consequently, the issue of cyber warfare has become securitized, making it a significant issue affecting national and societal security 31[31] .Cyber-threats have caused numerous risks and threats to the state's societal security, whether through their methods of operation, such as cyber-espionage and cyber-attacks, or through the tangible results they produce at all levels, including 32[32].

First: The Military Level

Cyber threats have led to an escalation of cyber risks, especially given the vulnerability of vital state facilities to attack. This vulnerability impacts the functions of these facilities, and controlling the execution of such attacks is a strategic tool. Cyber warfare has played a significant role in the militarization of cyberspace, thus escalating capabilities in the cyber arms race and leading to the adoption of cyber defense policies in the field of developing cyber warfare tools within modern armies. Cyber warfare has penetrated state military plans, helping to identify the nature of a state's military power and its military tactics. This, in turn, helps control the confrontation with targeted states, whether on the traditional battlefield or in cyberspace 33[33].

Second: The Economic Level

Cyber threats may try to shut down the targeted state's internet entirely, which would stop banking and e-government transactions and allow credit card numbers and other information needed for online shopping to be stolen. As a result, the state's financial system is disrupted, which paralyzes important industries and other sectors 34[34].

[34] -E.Nakashima, U.S.Accelerating cyber-weapon Research, the Washington post, online e-article, https://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/13/03/2012/gIQAMRGVLS_story.html .

[29][29]- Adel Abdel Sadek, Cyber Power: Weapons of Mass Proliferation in the Cyber Age, International Policy Magazine, Issue 188, April 2012.

[30][30]-Omar Hamed Shukr, Cyberspace: The Fifth Field, Political Science and International Relations website, 2019, available at the following link: https://www.elsiyasa-online.com/.

[31][31] -Jassim Muhammad Al-Basili, Electronic Warfare: Its Foundations and Impact on Wars, 2nd ed., Kuwait, Arab Foundation for Studies and Publishing, 1990.

[32][32] -Inji Muhammad Mahdi, Electronic Jihad: A Study of ISIS and the United States' Strategy for Confronting It, Journal of the Faculty of Political Science and Economics, Cairo University, Vol. 22, No. 2, April 2021

[33][33] -Salim Dahmani, The Impact of Cyber Threats on National Security: The United States as a Case Study, Master's Thesis, Mohamed Boudiaf University, Algeria, 2017.

[34][34]-Al-Mubaydeen, Safwan, E-Government: International Models, Applications, and Experiences, First Edition, Jordan, Dar Al-Yazouri Scientific Publishing and Distribution, 2020.

Third: The Psychological Level and the Cultural Level

By attacking websites and announcing a state of emergency, cyber attackers may try to instill fear and psychological warfare among the populace 35[35].

Cyber threats may aim to distort the identity of the country by promoting the ideas of the attacking state through methods that target the country's youth and influence their thoughts and beliefs. This is known as cultural invasion, which aims to penetrate the intellectual structure of societies by infiltrating minds through the implantation of ideas that destroy creativity and hinder comprehensive development in the country 36[36] .This is what many non-state actors use, such as terrorist organizations, which target young people, leading them to adopt a path against their country and immersing them in extremist ideas. All of this is done through social media and satellite channels 37[37].

Fourth: The Political Level

Cyber threats may aim to incite sedition in the country and incite the people against the ruling authority through hate speech by addressing the people and claiming that there are many dangers surrounding the country and that the ruling authority does not provide the basic needs of the people, as well as The people of the targeted country demand their stolen rights, leading to demonstrations that may develop into non-peaceful revolutions aimed at sabotage and destruction of the targeted state. All of this is facilitated by social media platforms. This goal contributed to the 2011 Arab Spring revolutions, which led to the overthrow of numerous Arab governments. Some countries have not been able to recover after these revolutions, making them areas of competition between major powers and even allowing terrorist organizations to establish a presence in these countries 38[38]. The concept of hybrid systems emerged from the literature of the third wave of democratization in the 1990s as part of the transformation.

CONCLUSION

Based on the foregoing, the concept of security is characterized by its ambiguity and the lack of consensus among specialists regarding its meaning. For a long time, a traditional, realist view of security dominated, reducing it to the military sphere. Realists presented an anarchic view of the international system, in which each state strives to enhance its capabilities, viewing other states as threats to its security, and aiming to preserve its sovereignty and ensure its survival and continuity.

However, realist assumptions for understanding and interpreting international reality proved incapable of keeping pace with the new conditions of the Cold War era. This created space for scholars and theories that reinterpret what is 'security', particularly as the dynamics of globalisation, media and communication technologies, and a pattern of economic exchange unfurled. Therefore, a new kind of security concept was needed to be redefined responding to the changes in the post-Cold war period. The early 1990s was a turning point in conceptualization of the term security at both theoretical and practical levels. The concept of security was rethought and several thinkers attempted to deconstruct the traditional understanding of security by expanding its boundaries.

The Copenhagen School of Security Studies played a significant role, introducing an alternative conception of security that was anchored in a broad regime including political, economic and socio-cultural levels. One of its main representatives, Barry Buzan had proposed a comprehensive security model with five interconnected dimensions: military, political, economic, environmental and social. This model redefined security as a variable that one could move about from issue to issue, and underpinned Buzans notion of "securitisation".

First: Results

The study had several findings based on its collection of data, some most significant were:

Cyber risks can cause and create serious damages to societal security, which will strike basic social values, psychological/cultural/political stability etc.

Cyber space is global, low cost and high impact source of threat - state and non-state actors have found the cyber domain to be convenient playing field.

The research found that social security has been revealled to be at further risk of threat from cyberspace,

35[35]- Faisal Muhammad Abdul Ghaffar, Electronic Warfare, First Edition, Jordan, Al-Janadriyah Publishing and Distribution, 2016.

36[36] -Salah Haider Abdul Wahid, Cyberspace Wars: A Study of Their Concept, Characteristics, and Ways to Confront Them, Thesis submitted in partial fulfillment of the requirements for the degree of Master of Political Science, Middle East University, Faculty of Arts and Sciences, 2021.

37[37] -Salah Haider Abdul Wahid, Cyber Warfare: A Study of its Concept, Characteristics, and Countermeasures, Master's Thesis in Political Science, Middle East University, Faculty of Arts and Sciences, 2021.

38[38] -Muhammad Salem Ghoneim, Towards an Integrated Model for Studying Presence in Cyberspace: Al-Hajrasi as a Model, Scientific Journal of Libraries, Documents, and Information, Volume 1, Issue 1, January 2019

than actual dangers in real space due to the heavy usage of various social media applications.

The Iranian and Saudi context showed signs of the construction of cybersecurity institutions, i.e., through a continuous trend toward institutionalization in which special bodies are established and particular national laws and strategies have been adopted.

The report found that a lack of common international definitions of cyber threats is the main obstacle to international cooperation in this area.

Second: Recommendations

In Light of the Findings, the Study Recommends the Following:

1. The necessity of developing clear national and international legislation that criminalizes cyber threats and defines accountability mechanisms.
2. Enhancing public awareness and cybersecurity literacy, particularly among youth, to mitigate the risks of digital manipulation and misinformation.
3. Investing in building human and technical capacities in cybersecurity through continuous training and development.
4. Strengthening regional and international cooperation to exchange information and expertise on cyber threats.
5. Integrating community security into national cybersecurity strategies as a fundamental component of comprehensive security.
6. Encouraging future academic research that addresses the relationship between cybersecurity and social and cultural transformations in Arab societies.

SOURCES

1. Abeer Hamid Siham Mahdi, Ammar Hamid Yassin, The Problem of Identity in Iraq: A Vision of Challenges and the Future of Building an Iraqi National Identity after 2003, The Political and International Journal, Issue 28-29, 2015, p. 389.
2. Adel Abdel Sadek, Cyber Power: Weapons of Mass Proliferation in the Cyber Age, International Policy Magazine, Issue 188, April 2012.
3. Adel Abdel Sadek, Cyberspace Weapons in Light of International Humanitarian Law, Library of Alexandria, Alexandria, Egypt, 2016, p. 59.
4. Adel Abdel-Razzaq, Cyberspace and International Relations: A Study in Theory and Application, Cairo: The Academic Library, 2016, pp. 22-26.
5. Ahmed Hossam Taha Tamam, Crimes Arising from Computer Use, Criminal Protection of Computers, PhD Thesis, Unpublished (Tanta University: Faculty of Law, 2000), pp. 210-211.
6. Alaa Muhammad Rahim, Security and Emerging Crimes: A Socio-Political Study, International Studies Journal, Center for Strategic and International Studies, University of Baghdad, Issue 62, 2023, p. 11
7. Ali Abdul Rahim Al-Aboudi, "The Obsession with Cyber Warfare and its Repercussions on International Peace and Security," *Journal of Political Issues*, College of Political Science, Al-Nahrain University, Issue 57, Baghdad, 2019, p. 99.
8. Al-Mubaydeen, Safwan, E-Government: International Models, Applications, and Experiences, First Edition, Jordan, Dar Al-Yazouri Scientific Publishing and Distribution, 2020.
9. Asaad Tarish Abdul-Ridha and Ali Ibrahim Mashhal Al-Maamouri, Cybersecurity and its role in the spread of the phenomenon of terrorism in Iraq after 2003, International Studies Journal, Center for International and Strategic Studies, University of Baghdad, Issue 80, Baghdad, 2020, p. 161.
10. Ashraf Al-Saeed Ahmed, *Electronic Piracy*, Dar Al-Nahda Al-Arabiya, Cairo, 2013, p. 46.
11. Christopher C. Joyner and Catherine Lotrionte, "Information Warfare as International Coercion: Elements of a Legal Framework," European Journal for International Law, Vol. (12). London. 2001. p. 825.
12. David Held et al., Global transformations: politics, economics, and culture California: Stanford University Press, 1999.
13. E. Nakashima, U.S. Accelerating Cyber Weapon Research, The Washington Post, online e-article:
14. https://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/13/03/2012/gIQAMRGVLS_story.html.
15. Faisal Muhammad Abdul Ghaffar, *Electronic Warfare*, 1st ed., Al-Janadriyah Publishing and Distribution, Amman, 2016, p. 30.
16. Faisal Muhammad Abdul Ghaffar, Electronic Warfare, First Edition, Jordan, Al-Janadriyah Publishing and Distribution, 2016.
17. Ghada Nassar, Terrorism and Cybercrime, Cairo: Al-Arabi Publishing and Distribution, 2017, p. 21.
18. Ibid., p. 826.
19. Inji Muhammad Mahdi, Electronic Jihad: A Study of ISIS and the United States' Strategy for Confronting It, Journal of the Faculty of Political Science and Economics, Cairo University, Vol. 22, No. 2, April 2021
20. Israa Sharif Al-Kaoud, "The Cyber Impact on the National Security of Active States (The United States as a Model)," *Journal of Political Science*, College of Political Science, University of Baghdad, Issue 64, 2022, p. 10.
21. James E. Cartwright, Memorandum for Chiefs of the Military Service. Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories on Joint Terminology for Cyberspace Operations, 5 No. 2011, p. 18.
22. Jassim Muhammad Al-Basili, Electronic Warfare: Its Foundations and Impact on Wars, 2nd ed., Kuwait, Arab Foundation for Studies and Publishing, 1990.

23. Joseph S. Nye. The future of power, New York: Public Affairs, 2011, 24.
24. Jullia Cresswell, "Oxford Dictionary of word origins. Word Origins."Cybernetics,"Word Origins."," Oxford
25. K. Saalbach, "Cyber warWar, Methods and Practice,"War,Practice," version 2.0, University of Osnabrück, 17ck, 17 Jun 2014, p. 8.
26. Mohamed Ali Al-Aryan, Cybercrimes, Alexandria: University Publishing House, 2004, pp. 67-68.
27. Mohammed Al-Amin Al-Bashri, Investigating Computer and Internet Crimes, Arab Journal of Security Studies and Training, Riyadh, Saudi Arabia, 1422 AH, p. 10
28. Muhammad Salem Ghoneim, Towards an Integrated Model for Studying Presence in Cyberspace: Al-Hajrasi as a Model, Scientific Journal of Libraries, Documents, and Information, Volume 1, Issue 1, January 2019
29. Mustafa Tlass, The Scientific and Technological Revolution and the Development of the Armed Forces, Dar Tlass for Studies, Translation and Publishing, 3rd Edition, Damascus, 2003, p. 318
30. Nihad Kreidi, Crime and Fraud in the Electronic Environment, Beirut, 2008, pp. 14-16.
31. Norbert Wiener, "Cybernetics or control communication in the machine"machine," M.I.T., Pressmachine,"M.I.T. Press,, Second Edition, Cambridge, Massachusetts, 1948 ، p18.,M.I.T. Press, p. 18.
32. Omar Hamed Shukr, Cyberspace: The Fifth Field, Political Science and International Relations website, 2019, available at the following link: https://www.elsiyasa-online.com/
33. Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel, "The law, p. 18.Law of Cyber-Attack,"LawCyber-Attack," California Law Review, 2012, p. 824; Oona Hathaway, op. cit., p. 825.
34. Oxford Dictionaries. Blog. Oxford Dictionaries. Com Reference online, Oxford University Press, 2010
35. Saham Hassan Ali Al-Shammari, "Manifestations of Cybersecurity and Media Practice and Their Relationship to the Virtual Psychological Warfare Industry," International Studies Journal, Center for Strategic and International Studies, University of Baghdad, Issue 38, 2020, p. 150
36. Salah Haider Abdul Wahid, Cyber Warfare: A Study of its Concept, Characteristics, and Countermeasures, Master's Thesis in Political Science, Middle East University, Faculty of Arts and Sciences, 2021.
37. Salah Haider Abdul Wahid, Cyberspace Wars: A Study of Their Concept, Characteristics, and Ways to Confront Them, thesi submitted in partial fulfillment of the requirements for the degree of Master of Political Science, Middle East University, Faculty of Arts and Sciences, 2021.
38. Salim Dahmani, The Impact of Cyber Threats on National Security: The United States as a Case Study, Master's Thesis, Mohamed Boudiaf University, Algeria, 2017.
39. Shaikha Hussein Al-Zahrani, "Confronting International Law with Cyber Attacks," 1st ed., Dar Al-Nahda Al-Arabiya, Dubai, 2021, p. 24.
40. Sulafa Tariq Al-Shaalan, Adapting the Use of Electronic Warfare in Armed Conflicts in Accordance with International Humanitarian Law, Kufa Journal of Legal and Political Sciences, College of Law - University of Kufa, Volume 9, Issue 26, 2016, p. 6
41. Shanghai Cooperation Organization (SCO): It was founded in Shanghai on June 15, 2001, and became an official organization according to the principles of international law in 2002. It consists of China, Russia, and most of the former Soviet republics in Central Asia, as well as observers including Iran, India, and Pakistan. Its objectives include combating terrorism, extremism, and separatist movements and countering the arms trade. However, some see it as a military alliance to confront the North Atlantic Treaty Organization (NATO).