THE IMPACT OF CYBER SPACE AS FIFTH DOMAIN ON THE THEORIES OF INTERNATIONAL RELATIONS

Researcher

Hussain Muhammad

Roll No: 53-FSS/PHDIR/S21

Supervisor

Professor Dr Muhammad Khan

DEPARTMENT OF POLITICS AND INTERNATIONAL RELATIONS
FACULTY OF SOCIAL SCIENCES
INTERNATIONAL ISLAMIC UNIVERSITY ISLAMABAD

2025

THE IMPACT OF CYBER SPACE AS FIFTH DOMAIN ON THE THEORIES OF INTERNATIONAL RELATIONS

Hussain Muhammad

Reg No: 53-FSS/PHDIR/S21

Submitted in partial fulfillment of the requirements for the PhD. Degree in the Discipline of Social Sciences with specialization in International Relations at the Faculty of Social Sciences

Supervisor:

Professor Dr. Muhammad Khan
Department of Politics and International Relations

DEDICATION

To my family. My father, Muhammad Irfan, who invested in every possible way in all his children, and my mother, Musarrat Bibi, who has always been my emotional panic room. And my sisters Wajeeha, Tahira, and Sadia for keeping me caffeinated during my long hauls of reading and writing.

TABLE OF CONTENTS

ACKNOWLEDGMENT i

List of Abbreviations ii

ABSTRACT iii

CHAPTER-1 1

1. Introduction 1

1.1 Background 1

1.1.1 Iran's Cyber Attack against Sands Corporation 2

1.1.2 North Korea's Cyber Attack on Sony Pictures 3

1.1.3 Russian Hacking of Democratic National Committee's Emails 3

1.1.4 Waning Deterrence in the Fifth Domain 4

1.1.5 Critical Infrastructure Security 5

1.2. Problem Statement 6

1.3 Significance of Study 7

1.4. Objectives of the Study 7

1.5 Research Questions 7

1.6. Delimitations of the Study 8

1.7 Literature Review 8

1.7.1 Skepticism Towards Escalation 14

1.7.2 Research Gap 16

1.7.3 Theoretical Framework 16

1.8 Methodology 21

1.8.1 Research Design 22

1.8.2 Operational Definitions 22

1.8.3 Procedure (Data Collection) 22

1.8.4 Data Analysis 23

1.9 Organization of the Study 24

CHAPTER 2 26

2.. Evolution of Cyberspace 26

2.1 Etymology of Cyberspace 26

2.2 Varying Definitions of Cyberspace 27
2.3 Birth of the Internet 28
2.4 Popularization of the Idea 29
2.5 Cybersecurity: From a Movie Script to Policy 30
2.6 Economic Impact of Cyberspace 31
2.7 Strategic Importance and Militarization of Cyberspace 32
2.8 Temporality, Cyberspace, and International Relations 35
2.9 Spatiality in Cyberspace and International Relations 39
2.10 Ubiquity in Cyberspace 40
2.11 Anonymity in Cyberspace (Attribution Problem) 41
2.12 Defenders' Dilemma in a Pro-Offense Domain 45
CHAPTER-3 49
3. Cyberspace: New Threat Vectors 49
3.1 Information Warfare and Influence Operations 52
3.2 Security Concerns in Cyberspace 53
3.2.1 Cybercrime 54
3.2.2 Cyberterrorism 55
3.2.3 Cyberespionage 56
3.2.4 Critical Infrastructure Protection 57
3.2.5 Data Privacy 59
3.3 Structure of Cyberspace 61
3.3.1 Software and Applications 62
3.4 Cyber Threats and Vulnerabilities 63
3.4.1 Malware 63
3.4.2 Phishing and Social Engineering 66
3.4.3 Distributed Denial of Service (DDoS) Attacks 67
3.4.4 Advanced Persistent Threats (APTs) 68
3.4.5 Zero-Day Vulnerabilities 69
3.4.6 Insider Threats 70
3.4.7 Vulnerabilities in IoT Devices 71
3.5 Resilience and Defense in Cyberspace 72
3.5.1 Cyber Resilience 72

3.5.2 Defense Mechanisms 73
3.6 Incident Response and Recovery 75
3.7 Cybersecurity Frameworks and Standards 76
CHAPTER-4 ..... **78**
4. Cyberspace and Realism **78**
4.1 State-Centrism 78
4.2 Anarchy 79
4.3 Power and Security 80
4.4 National Interest 81
4.5 Balance of Power 81
4.6 Rational Actor Model 82
4.7 Survival 83
4.8 Relative Gains 84
4.9 Conflict and Competition 85
4.10 Human Nature 86
4.11 New Realities of Cyberspace 87
4.12 Realism in Cyberspace: Beyond Statism 89
4.13 Erosion of Sovereignty and Realist Response 91
4.14 Cyberspace as a New Arena for Power Struggles 93
4.15 Cyber Deterrence and Defense 96
4.16 Interstate Competition and Cyber Power 99
4.17 Institutional Responses and Cooperation 100
4.18 Impact on Traditional Concepts of Security 102
3.19 Cyberspace and Realist Principles 104
4.20 Anarchic Nature of Cyberspace 105
4.21 Cyber Power and National Security 107
4.22 Cyber Warfare and National Security 108
4.23 Cyber Warfare and National Strategies: 109
4.24 State-Sponsored Cyber Attacks 111
4.25 National Security in Cyber Age 113

4.26 Power Dynamics in Cyberspace 114
4.27 Cyber-skeptics 115
4.28 Limitations of Realist Theory in Cyberspace 117
CHAPTER-5 ..... **119**
5. Cyberspace and Liberalism **119**
5.1 Democratic Peace Theory 120
5.2 Interdependence and International Institutions 124
5.3 Human Rights and Individual Freedoms 129
5.4 Economic Liberalism in International Relations 130
5.5 Cyberspace and Liberal Principles 132
5.6 Liberalist Perspectives on Cyberspace 133
5.7 China's Approach to Cyberspace 135
5.8 Cyberspace across Cultures 136
5.9 Cyberspace Governance 138
5.9.1 Digital Divide 139
***5.9.2* International Cooperation in Cyberspace** 140
5.9.2.1 Joint Cyber Exercises 141
5.9.2.2 Cyber Governance 142
5.9.2.3 Norm Development 143
5.10. Regional Organizations 144
5.10.1 European Union 144
5.10.2 ASEAN Cybersecurity Cooperation 145
5.11 Case Study: Budapest Convention on Cybercrime 146
5.12 Policy Implications 147
CHAPTER-6 ..... **149**
6. Cyberspace and Constructivism **149**
6.1 Key Concepts in Constructivism 150
6.1.1 Norms as Determinants of States' Conduct 151
6.1.2 Identity as a Determinant of State's Conduct 152
6.2 Constructivist Perspectives on Cyberspace 152
6.2.1 Cyberspace and Constructivist Principles: 153

6.2.2 Cyber Norms Development 156
6.2.3 Contestation of Norms in Cyberspace 158
6.3 Ethics in Cyberspace 160
6.4 Identity and Perception in Cyberspace 162
6.4.1 Cyber Diplomacy 162
6.4.2 Public Diplomacy 163
6.5 Influencing Perceptions 165
6.5.1 Information Warfare 165
6.5.2 Cyber Propaganda 166
6.6 Social Constructs in Cyberspace 167
6.6.1 Digital Rights and Freedoms 167
6.6.2 Security and Rights Tradeoff 168
6.7 Case Studies 169
6.7.1 The UN Group of Governmental Experts (GGE) on Cyber Norms 169
6.7.2 Russia's Information Warfare in the 2016 US Presidential Election 170
6.8 Policy Implications 171
CHAPTER-7 173
7. Overarching Cyber-Responsive Policies 173
7.1 Comprehensive Cybersecurity Strategies 173
7.2 Cyber Defense and Resilience 174
7.3 Public-Private Partnerships (PPP) 175
7.4 Strengthening International Norms 177
7.5 Multilateral Agreements 178
7.6 Bilateral Arrangements for Cybersecurity 179
7.7 Digital Rights and Freedoms in Cyberspace 180
7.8 Ethics in the Cyber Realm 181
7.9 Cyber Governance 183
7.10 Multi-Stakeholder Internet Governance 184
7.11 Regulatory Frameworks 184
7.12 Future of Cyber Diplomacy 186
7.13 Cybersecurity and Global Stability 187

CHAPTER-8 ..... **190**
8. Pakistan's Realization Episodes and Response **190**
8.1 Pakistan's Cyber Threat Matrix 191
8.1.1 Data Security 193
8.1.2 Phishing 193
8.1.3 Ransomware 194
8.1.4 Distributed Denial of Service (DDoS) 195
8.2 K-Electric Attack 197
8.3 Cyber-attack on Pakistan Airforce 198
8.4 Pakistan's Lagging Cyber Defense 201
8.5 Raising the Cyber Guard 203
8.6 Pakistan's Cyber Capabilities 205
8.6.1 Pakistan Computer Emergency Response Team (PKCERT) 205
8.6.2 National Centre for Cyber Security (NCCS) 206
8.7 National Cyber Security Policy 2021 207
8.8 Cyber Security Strategy 2023-2028 for Telecom Sector 208
8.9 Computer Emergency Response Teams (CERTs) Rules, 2023 209
8.10 National Cyber Crimes Investigation Agency (NCCIA), 2024 210
8.11 Cybersecurity Risk Governance 211
8.12 Insights from Interviews with Experts 214
8.12.1 Insights from Interview with Mr. Ammar Hussain Jaffri 214
8.12.2 Insights from Interview with Dr. Salman Ali 216
8.12.3 Insights from Interview with Dr. Yasir Masood 217
8.12.4 Insights from Interview with Dr. Baqir Malik 219
8.12.5 Insights from Interview with Dr. Muhammad Shoaib 220
Conclusion **222**
References **225**
Appendices **264**
Appendix 1: Transcript of the Interview with Mr. Ammar Hussain Jaffri 264
Appendix 2: Transcript of the Interview with Dr. Salman Ali 267
Appendix 3: Transcript of the Interview with Dr. Yasir Masood 270
Appendix 4: Transcript of the Interview with Dr. Baqir Malik 273
Appendix 5: Transcript of the Interview with Dr. Muhammad Shoaib 277

ACKNOWLEDGMENT

I owe the best parts of this dissertation to my research advisor, Prof. Dr. Muhammad Khan, and the shortcomings are mine. He has been accessible throughout the course of writing this dissertation and has always provided the right dose of motivation and critical evaluation to administer to his research students.

I want to thank the entire faculty of the Politics and I.R. department, who, with their varying expertise, added value to me as a student of international relations. I also thank the department's office administration staff for doing the paperwork and keeping everything moving.

List of Abbreviations

APT	Advanced Persistent Threat
CIA	Central Intelligence Agency
DDoS	Distributed Denial of Service
DoD	Department of Defense
DoS	Denial of Service
IAEA	International Atomic Energy Agency
ICT	Information and Communications Technology
NICE	National Initiative for Cyber Education
NIST	National Institute of Standards and Technology
OSINT	Open-source Intelligence
SoC	Security Operations Center

ABSTRACT

The history of international relations as a discipline extends back centuries, and scholars have proposed multiple explanations and delineations to elucidate interactions between states, such as war and peace. All these theories have one primary foundation: their assumptions are rooted in the physical domain. However, with the emergence and extensive use of cyberspace as the fifth domain, states are now interacting more in the virtual arena than in the physical realm. This phenomenon has rendered some of the mainstays of traditional theories either entirely obsolete or diminished their explanatory power because the operational environment has fundamentally changed. State interactions, previously constrained by spatial and temporal factors, have now increased significantly in both frequency and complexity. Furthermore, factors such as attribution, deterrence challenges, the instrumental role of non-state actors in cyberspace, and the pro-offense architecture of cyberspace make it challenging for traditional theories to explain events and delineate a blueprint for the foreseeable future. Cyberspace, which was previously conveniently dismissed as a domain of low politics, has now risen to the highest tier of high politics. However, theoretical development in international relations is yet to catch up with the pace of new technologies. This study tracks how international relations theories have adapted and responded to the new challenges emerging from the manmade realm of cyberspace.

KEYWORDS: Cyberspace, Fifth Domain, Advanced Persistent Threat (APT), Cybersecurity, Cyber-IR (Cyber International Relations

CHAPTER-1

1. Introduction

1.1 Background

Previously, the domains of warfare were limited to four, including land, sea, air, and space. However, the attack on the Iranian nuclear facility at Natanz, the news of which spread in 2010, clarified that a fifth domain already existed. In 1984, William Gibson dismissed cyberspace as a consensual hallucination; this attack made it clear that cyberspace was not only a reality but also emerged as a fifth domain of warfare (Robins, 1995). When the United States and Israel launched a joint cyber-attack on the Iranian nuclear enrichment facility at Natanz, it marked the first time that a cyber-attack was launched against physical infrastructure, ultimately destroying it. This highly sophisticated malware, named Stuxnet, was so deceptive that it manipulated the speed of nuclear centrifuges while transmitting incorrect data to display panels, consequently destroying many Iranian centrifuges while operators were clueless about what went wrong. The malware was activated only on systems responsible for the control valves of nuclear centrifuges, and this capability made it a guided virtual weapon (T. M. Chen & Abu-Nimeh, 2011).

This attack also drew attention to the challenges of cyber policy and security in global politics. It was the first reported incident where the impact of an attack in the virtual domain transcended into the physical arena and not only posed new challenges to states regarding national security but also opened a new frontier for the international relations theory. On this frontier, traditional notions of state security were rendered irrelevant because there were no temporal or spatial constraints in cyberspace. The stopping power of geography and different time zones became irrelevant because of the instantaneous flow of information and the execution of cyber-attacks in real-time. However, this fifth domain is not entirely disruptive

and perilous but offers a unique benefit: when a weapon is used in this domain, it becomes obsolete and cannot be used in the future (Clarke & Knake, 2020).

Every known vulnerability is fixed by regular security patch releases from software developers, and an entire discipline of penetration testing and bug bounty has evolved around such vulnerabilities. Penetration testing and bug bounties involve white-hat hackers and cybersecurity professionals who attack systems with prior knowledge and permission from stakeholders to identify security vulnerabilities and strengthen defenses against attacks by black-hat hackers. However, these practices and programs have their own shortcomings. The probability of finding additional bugs and vulnerabilities in any particular program diminishes rapidly, which also decreases the monetary incentive for bug bounty hunters, and they prefer moving on to newer software releases (Maillart et al., 2017).

1.1.1 Iran's Cyber Attack against Sands Corporation

In 2013, Sands Casino Corporation, owned by the conservative magnate Sheldon Adelson, was attacked by Iranian hackers. The attack was launched in response to an interview in which Adelson criticized Obama's foreign policy towards the Iranian nuclear program and argued that the United States should detonate a nuclear missile over an Iranian desert, sending a signal that the US would not permit Iran to continue to develop its nuclear weapons. Iran responded by launching a cyber-attack against the Sands Corporation, hacking the corporate computer network, and forcing the network to be disconnected and cleaned (M. Libicki, 2017, p. 5). This attack cost the Sands Corporation more than $40 million, highlighting the asymmetry of cyber-attacks (Brandom, 2014). Launching the attack cost Iran very little, but it was highly effective in signaling the will to continue the nuclear program.

1.1.2 North Korea's Cyber Attack on Sony Pictures

In 2014, when Sony declined to cancel the release of a comedy film, '*The Interview, '* in which two Americans were shown to execute Kim Jong Un, North Korea launched a cyber-attack against movie studios, stealing massive amounts of internal and highly embarrassing information before taking down the company's computer network and destroying about 70 percent of its computers (Sullivan, 2015). The attack cost Sony millions of dollars and resulted in the publication of a host of embarrassing emails, criticism of Hollywood stars, secret contract information and draft scripts. Ultimately, the President of Sony Studios, Amy Pascal, was forced to resign. The attack itself was called an "act of war" by John McCain, who campaigned against Obama for the Presidency. However, Obama dubbed it as cyber vandalism and stated that the United States would respond proportionally and in a time and place of its own choosing (Sheppard, 2014). North Korea blamed the U.S. for the forced shutdown of North Korea's Internet network, consisting of approximately 28 websites at the time, as a result of an American counterattack (J. Kim, 2014). However, the attack illustrated the disproportionate vulnerability of the United States to such attacks.

1.1.3 Russian Hacking of Democratic National Committee's Emails

Another example is the Russian attempt to steal Democratic National Committee emails ahead of the 2016 presidential elections and to spread disinformation and fuel political distrust and polarization in the United States (Sanger & Schmitt, n.d.). Similarly, Chinese efforts to steal commercial and defense secrets from US computer networks point to the same disproportionate vulnerability (Sanger et al., n.d.). These instances highlight the unique nature of cyber conflict and the challenge of developing a clear response to such attacks. This is further complicated by the number of actors involved in the process. Currently, seven countries possess advanced cyber-attack capabilities: China, Iran, Israel, North Korea, Russia, the United Kingdom, and the United States (US). Other countries, including Mexico and Vietnam, are

working quickly to develop them. A host of non-state actors can launch their own attacks with or without state support. For instance, a ransomware group named Conti crippled the entire IT infrastructure of Costa Rica and demanded a ransom of $20 million, which the government refused to pay and declared an emergency. It was just another reminder of the disruptive power in the hands of both state and non-state actors.

1.1.4 Waning Deterrence in the Fifth Domain

In 2017, Secretary of Defense Jim Mattis sent President Trump a classified memo containing startling recommendation. The United States should declare itself willing to take extraordinary steps, including the use of nuclear weapons, in response to a foreign cyberattack against critical American infrastructure. Although no formal policy declaration was made, cyber warfare presented a conundrum for U.S. policymakers. The U.S. is both disproportionately powerful in its cyber-attack capabilities and disproportionately vulnerable because of its widespread reliance on computer and Internet technologies. Cyber weapons are relatively cheaper to develop and easier to hide, and in today's world, where everything is connected, they can be highly disruptive. From phones to cars and from electric grids to water and sewage connections, almost every aspect of modern life can be disrupted and destroyed by malicious code. The fundamental problem is that cyberattacks are difficult to categorize and label. Are they acts of war? Terrorism? Espionage? Or vandalism? Should they be treated as criminal activities? Or acts of war by a state? Who should be responsible for bearing the burden of preventing and ultimately addressing the impact of cyber-attacks? Today, cyber operations exist in a grey area between war and peace, and determining a proportionate response, even if responsibility can be attributed, is incredibly difficult.

Before getting into the legal debates over cyber-attacks, it is useful to briefly consider the different actions that fall under the banner of "cyber operations." A part of the challenge we face is that a wide variety of activities, ranging from stealing sensitive information to

destroying physical infrastructure, conducted by a wide variety of state and non-state actors, all fall under the label of cyber-attacks. This fluid nature of the problem is at the core of the complexity of international cyber relations.

> The US Committee on National Security Systems (CNSS) defines cyber attacks as
>
> "An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure, or of destroying the integrity of the data, or stealing controlled information."(*Cyber Glossary - C | National Security Archive*, n.d.)

This definition seems straightforward, but whether it is seen as a crime, terrorism, or a cyber act of war is subject to factors such as the nature of the attack and the identity and goals of the perpetrator, which are all difficult to determine in most cases.

1.1.5 Critical Infrastructure Security

In February 2021, an unknown hacker breached the control facilities of a water processing plant in Oldsmar, Florida. The hacker increased the level of sodium hydroxide, the main ingredient in liquid drain cleaners used to control the acidity and remove metals from drinking water (Robles & Perlroth, 2021). The level was increased to 100 times the normal limit. The attacker then logged out of the system after the attack. Fortunately, a computer operator at the plant noticed an increase and quickly lowered the levels to safe limits. A similar attack by another state would likely be seen as an act of sabotage or even an act of war and could provoke a harsh military or espionage response. Unlike the threat of nuclear war during the Cold War, deterrence does not appear to be an effective method for preventing cyberattacks. The United States insists that it will continue to engage in offensive cyber operations targeting Iran, North Korea, Russia, and others, while simultaneously maintaining that it will respond with force to similar efforts targeting American cyber and physical infrastructure is untenable.

Another complicating factor is the ambiguity of international law governing cyberspace. Under international law, states are legally justified in their use of force in self-defense or when international law itself is violated. However, cyber-attacks may or may not violate international law, particularly when the goal of such attacks is espionage rather than physical damage. In this case, international law permits retorsion, a proportional attack, or a response of a similar kind. However, retorsion itself is hardly an effective deterrent, particularly when the United States and other advanced industrial economies are uniquely vulnerable to cyberattacks. Retorsion, which involves unfriendly but legally permissible acts in response to another state's unfriendly acts, can be applied to the cyber domain. However, the application of international law principles to cyberspace is still in its infancy. Although cyber-attacks may not always constitute an "armed attack" in the traditional sense, they can still be viewed as a form of intervention that threatens national security. The UN Charter principles are likely to be relied upon to define the legal boundaries of cyberspace and the permissible responses (Joyner, 2001). Joyner contends that while retorsion is generally allowed under international law in response to cyber-attacks, the specific application in cyberspace is still developing. There is a need for clearer rules regarding permissible responses and self-defense in information warfare situations.

1.2. Problem Statement

The emergence of cyberspace has provided a virtual arena for real-time international information exchange. This speed and fluidity have proven to be of immense value to human development but have also created new vulnerabilities that cannot be addressed through traditional conceptions of security because the threats are not physical. This fluid nature of the threats emanating from cyberspace has rendered spatial and temporal factors irrelevant, which is why international relations theory finds cyberspace anomalous. This study addresses the question of how cyberspace opened a new frontier for international relations theory and

how the theory adapts to this new challenge.

1.3 Significance of Study

This study is important in the contemporary world because new and disruptive technologies have outpaced social scientists, who are struggling to catch up and answer the pressing questions arising from the pervasive use of these technologies. Cyberspace is no longer a consensual hallucination, as Gibson claimed. This reality has transformed everything from individual consumption preferences to the conduct of war. Today, Fortune 500 companies cannot exist without cyberspace; global capital flows depend on cyberspace; and instantaneous communication has significantly facilitated global logistics and supply chains in multiple ways. However, this increasing reliance on cyberspace has created vulnerabilities that can cause major disruptions and exploitation by hostile actors. A distributed denial-of-service (DDoS) attack can push countries offline, and its use by Russia has already been observed in both Estonia and Georgia. This study attempts to chart the response of international relations theory to interstate conflicts in cyberspace.

1.4. Objectives of the Study

This research is being carried out to further the following objectives

1. To examine the disruptive impact of cyberspace as the fifth domain of warfare on traditional conceptions of security.
2. To analyze the response of major international relations theories to the increasing salience of cyberspace as a new arena of conflict between states.
3. Building on different case studies and evaluating their explanatory value for the general theory of International Relations.

1.5 Research Questions

The questions for this study are as follows:

- **Main Question**

Why are the major theories of international relations struggling to account for the new

dynamics introduced by cyberspace as a fifth domain?

- **Sub Questions**

1. Why does the realist theory of international relations find cyberspace anomalous?
2. Why does the liberal theory of international relations find cyberspace anomalous?
3. Why does constructivist theory of international relations find cyberspace anomalous?

1.6. Delimitations of the Study

Cyberspace is inherently a technical domain, and there are various areas of specialization, ranging from malware analysis, penetration testing, digital forensics, and incident response to critical infrastructure security, such as Supervisory Control and Data Acquisition (SCADA) systems widely used in industrial facilities such as water filtration plants, oil refineries, and nuclear facilities. However, this study is restricted to the social science approach towards cyberspace and will not transcend into the technical domain. Technical terminologies and concepts will be used only if they are irreducible to the debate, to avoid discounting the analytical value of this study's findings.

1.7 Literature Review

This literature review evaluates and summarizes the state of knowledge and practice on this topic. To conduct research on any topic, literature review provides an appropriate point of departure to avoid repetition of what has already been written. A review of the literature shows how literature on any topic has historically evolved, what the major contentions were, and why some explanations were discarded in favor of others.

In his book *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, David Sanger extensively debates the disruptive impact of cyberspace on world politics and attempts to answer the difficult question of what can be an appropriate response to deter cyber-attacks

(Sanger, 2018). Are counter cyber offensives effective, or should states escalate to the use of traditional deterrence mechanisms like economic sanctions, conventional military, and nuclear options? He proposes certain options for making sense of the cyberspace security landscape.

First, he asserts that we must work to clarify the respective roles of the government and the private sector in cyber defense. The state cannot abandon private actors to defend themselves against foreign state-sponsored cyber-attacks, such as those launched by North Korea, Iran, or China. Instead, state and private actors must work in conjunction with one another to develop a coherent response. Second, the United States needs to adjust its cyber strategy and move away from conventional understandings of war and peace. Cyber operations exist in the gray area between war and peace, and cyber policies must acknowledge this fact. Third, the United States should respond with criminal prosecutions of cyber-attackers, where appropriate. However, it must also draw clear red lines on issues of importance, signaling to other states what areas the United States views as off-limits to cyber intrusion. The Biden administration did this in an early meeting with Russian officials in 2020, when it warned Russia that attacks against critical infrastructure in the United States were off-limits and vowed that the United States would take any necessary action to prevent such attacks.

Fourth, the United States needs to move away from the policy of strict secrecy surrounding its cyber operations. Deterrence only works when the opponent knows what you are willing and capable of doing in response to their attack. Maintaining excessive secrecy around cyber operations, an outgrowth of the bureaucratic positioning of US cyber operations in traditionally espionage-focused institutions like the National Security Agency, weakens the effectiveness of deterrence policies. Fifth, the United States must acknowledge that it is not the only actor with advanced cyber capabilities and that other states possess the technical knowledge and capability to carry out devastating attacks. Sixth, because of this, the United

States must develop a clear playbook for responding to cyber-attacks and be willing to use it in response to such attacks. It must have the capability to determine the origin of attacks, call out adversaries publicly when they attack, and respond appropriately. Finally, the United States must work with other cyber actors to develop a clear and comprehensive set of shared international norms governing cyber operations.

In his book, '*The Virtual Weapon and International Order,* Lucas Kello extensively discusses how all three stabilizing factors of world politics are irrelevant in the cyber arena (Kello, 2017). IR theory has a usual point of departure, which is units, and a given rule that powerful states are at the core of the international system while weaker states act as subordinates. In the cyber arena, paradoxically, the more technologically advanced states are by default more vulnerable due to their higher levels of automation and reliance on ICT. This means that it is easier to mount an offense in cyberspace than to defend it, and the cost of offensive cyber operations is considerably lower than that of any other warfare domain. Similarly, the preservation of the prevailing order that curtails revisionism because states have shared interests does not apply to the fifth domain. The third factor is the absence of consolidated norms and regulations that otherwise work as a stabilizing factor even in the absence of any higher authority. With these three major differences, theorizing in cyber international relations must start from a different point. In world politics, private actors rarely assume a central role, but in cyberspace, these actors wield roughly the same power as any state.

Nazli Choucri and David Clark in their book *'International Relations in the Cyber Age: The Co-Evolution Dilemma'* contend that cyberspace has now shifted from low politics to high politics due to its ubiquity, scope, and scale (Choucri & Clark, 2018). However, both international relations and cyberspace are simultaneously evolving, and the evolution of

cyberspace is faster than theorizing in international relations. They dubbed this dynamic the co-evolution dilemma, the primary reason regulators fail to catch up with 21st century technology through the tools of the 20th century. The centrality of cyberspace for national security is evident from the formation of a cyber command in the U.S. Department of Defense. In the budgetary allocation requests for the fiscal year 2023, the Pentagon asked for $11 billion to renew cyber-related capabilities.

Jon R. Lindsay, in his article *"Stuxnet and the Limits of Cyber Warfare"* takes an alternate position and questions the utility of offensive cyber-attacks like Stuxnet, which was used to target Iran's uranium enrichment facility at Natanz. He argues that Stuxnet temporarily derailed nuclear enrichment for a year, but Iran was able to recover, and consequently, concerns regarding an aerial strike on Iran's nuclear facility by Israel grew again by 2012. Similarly, he dismisses the idea of a revolution in military affairs with the emergence of cyberspace (J. R. Lindsay, 2013).

Richard A. Clarke and Robert K. Knake, in their book *"Cyberwar: The Next Threat to National Security and What to Do about it"* argue that the threat emanating from the cyber domain is more complex and difficult to counter because it requires a unified response at the national level, and the role of all stakeholders is equally important (Clarke & Knake, 2012). The military cannot singlehandedly counter this new threat because of the involvement of the human element, which is prone to social engineering and is therefore the weakest link in cybersecurity. To address this problem, overarching compliance mechanisms are needed across all industries and areas critical to national security. They also identify the problem of regulation; although the Internet started as a military project, its rapid commercialization has attracted strong criticism of any attempts to regulate it by those who see it as a free and open domain and want minimal government intervention in it. They also discussed the paradox of

centralization and automation; the United States is more vulnerable to threats originating from cyberspace because it heavily relies on the Internet in all domains. This dependence creates vulnerabilities that can be exploited by hostile actors. Therefore, cyberwar for the United States is more than a buzzword and should be dealt with accordingly.

Joseph S. Nye, the former dean of social sciences at Harvard, in his article *"Nuclear Lessons for Cyber?"* discussed the emergence and increasing relevance of cyberspace and the apparent lack of consensus in the international relations community through the lens of revolution in military affairs (J. S. Nye, 2011). A revolution in military affairs alludes to the change in the nature and conduct of war due to technological advances such as gunpowder, which altogether changed warfare. Similarly, the Napoleonic wars ended the era of armies camping before each other in the battleground or conducting war through sieges in favor of agility and speed. With the emergence of nuclear weapons, warfare assumed a different dimension, and nuclear weapons were seen as an arrangement to avert war instead of waging it because of the massive destructive power that led to the idea of Mutually Assured Destruction (MAD). Nye argues that, exactly as Moore's law suggested, computing power has multiplied while the cost of computing has decreased considerably, and today, billions of people have access to the Internet and emerging technologies. Political scientists and analysts are struggling to keep up with the pace of this technological transformation. Nye states,

> "In comparison to the nuclear revolution in military affairs, strategic studies of the cyber domain are chronologically equivalent to 1960 but conceptually more equivalent to 1950. Analysts are still not clear about the lessons of offense, defense deterrence, escalation, norms, arms control, or how they fit together into a national strategy".

Adam P. Liff, in his article *"Cyberwar: A New 'Absolute Weapon'? The Proliferation*

of Cyberwarfare Capabilities and Interstate War" also highlights the existing gap in the international relations literature regarding the implications of cyberspatialities (Liff, 2012a). While scholars such as Bernard Brodie have highlighted the effect of nuclear weapons on states' interactions, I.R. scholarship has yet to come up with a comparable evaluation of how cyberwarfare capabilities are likely to impact the relations between states. Although there is some literature on the topic by policy practitioners, it does not address the important theoretical questions regarding the interaction of cyberspace and international relations. Liff analyzes cyberspace as a transformative but non-revolutionary domain of warfare, challenging the notion that cyber capabilities inherently increase the likelihood of interstate conflicts. His work emphasizes the strategic implications of cyberwarfare while situating it within established international relations (IR) theories.

He rejects the idea that cyber capabilities are a new "absolute weapon" akin to nuclear arms. While cyber operations enable states to disrupt adversaries' infrastructure or political systems, he argues that they lack the coercive finality of nuclear weapons. Unlike nuclear strikes, cyber-attacks rarely produce decisive outcomes, reducing their utility in compelling adversaries to surrender. (Liff, 2012b) Applying the bargaining model of war, Liff contends cyberwarfare may reduce the probability of conventional conflict by providing non-kinetic avenues to signal resolve (e.g., disruptive attacks on power grids) and mitigating private information through cyber espionage, improving crisis communication.(Junio, 2013)

However, he acknowledges that cyber operations can exacerbate commitment problems, as states might exploit temporary advantages preemptively. He identifies distinct attributes that shape cyber conflict, including low barriers to entry, small states, and non-state actors' asymmetrical edge, anonymity complicating retaliation, and escalatory dynamics. He argues that coercive intent distinguishes cyberwarfare (state-aligned and

strategic) from cybercrime. Attacks are conducted to achieve strategic, political, or military ends, such as degrading, neutralizing, or destroying an adversary's combat capabilities. He also refines the concept of cyber warfare to include only computer network attacks (CNA) and computer network defense (CND) that have direct political and/or military objective (Liff, 2012b)

1.7.1 Skepticism Towards Escalation

While cyber-attacks like Stuxnet demonstrate disruptive potential, Liff argues that they do not fundamentally alter states' cost-benefit calculations. Historical precedents (e.g., Cold War espionage) suggest that cyber operations will be integrated into existing strategies rather than triggering novel forms of warfare. Liff downplays the escalation risk in cyberspace by emphasizing the unique characteristics of cyber operations that inherently limit their potential to escalate into broader conflicts. His analysis suggests that while cyberspace is a domain of strategic interaction, it does not inherently lead to escalation because of several mitigating factors. These include the complexity and unpredictability of cyber operations, their limited ability to impose significant costs, and the strategic value of maintaining secrecy and plausible deniability of such operations. These factors collectively contribute to a strategic environment in which escalation is less likely than traditionally assumed.

Liff's analysis has been questioned for downplaying the escalation risks in case of cyber-attacks on critical infrastructure (e.g., healthcare systems) that can provoke unintended retaliation. The 2015 cyber-attack on Ukraine's power grid, attributed to Russian actors, caused outages for 225,000 customers and was interpreted as a coercive act during an ongoing war. Similarly, ransomware attacks (e.g., Colonial Pipeline, 2021) blend criminal profit motives with disruptive effects on national infrastructure, creating ambiguity regarding the perpetrator's intent. Critics contend that even non-state criminal groups can inadvertently escalate tensions between nations by destabilizing critical systems. He banks on unitary

rational actor models and overlooks bureaucratic politics (e.g., military cyber commands pursuing organizational interests) as a driver of conflict. Liff views cyberspace as a domain that amplifies traditional state competition but does not upend the core IR principles. His work urges policymakers to avoid overhyping cyber threats while integrating cyber capabilities into broader deterrence frameworks.

While Liff's analysis highlights the factors that mitigate escalation risks in cyberspace, other scholars argue that the potential for escalation remains significant because of attribution challenges and the possibility of second-order effects. For instance, misinterpretations of cyber actions can lead to unintended escalations, as seen in cases where cyber operations have influenced domestic political dynamics and strategic postures (Reinhold & Reuter, 2023; Whyte, 2020). Additionally, the persistent engagement strategy, which involves continuous cyber interactions, could inadvertently lead to escalation if not carefully managed (Fischerkeller & Harknett, 2018). These perspectives suggest that while the risk of escalation may be downplayed, it is not entirely absent and requires careful consideration in cyber strategies and policies.

Lucas Kello, in his article *"The Meaning of the Cyber Revolution: Perils to Theory and Statecraft"* reaches a similar conclusion that the real scope of cyber capabilities is difficult to determine because this is a novel phenomenon that creates new opportunities and threats, and existing theories are unable to clarify it (Liff, 2012). Some scholars blame the scientific complexity of this domain for a slower theoretical response from I.R. scholars, while others dismiss the very notion of cyberwar on the premise that cyberweapons lack any intrinsic military utility and do not affect the nature and means of war. He writes

> "The range of conceivable cyber conflict is poorly understood by scholars and decisionmakers, and it is unclear how conventional security

> mechanisms, such as deterrence and collective defense, apply to this phenomenon. […] There is an evident need for scholars of international relations and security to contribute to the theoretical evaluation of the cyber revolution. Removed from the pressures of having to defeat the cyber threat, yet possessing concepts necessary to analyze it, academics are in a privileged position to resolve its strategic problems. Yet, there has been little systematic theoretical or empirical analysis of the cyber issue from the perspective of international security" (Kello, 2013).

The article concludes that the relevance of cyberspace for international relations will only grow and not diminish, and this is apparent from the current trajectory, where states are increasingly willing to conduct offensive cyber operations against their adversaries.

1.7.2 Research Gap

As already stated, a considerable gap in research exists regarding the two-way change in which cyberspace and world politics influence each other. Literature exists on cyberspace, but it is fragmented and comes from diverse fields such as information security, computer science, and electrical engineering. With the rise of disruptive technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), and Cloud Computing, world politics and the slow pace of social sciences' theorizing about their disruptive impact and adapting potential of international relations theory poses new challenges and opportunities for the field of international relations. In the literature review, Joseph Nye, Adam P. Liff and Kello identified a gap in international relations literature. Therefore, the scope for research in cyber international relations is immense, and its importance and relevance will further increase in the future.

1.7.3 Theoretical Framework

While some thinkers label the prevalence of cyberspace as another revolution in military affairs, others dismiss it as a buzzword. However, no one denies the centrality of this new domain in the contemporary world. None of these conditions existed in the other domains. This makes

cyberspace anomalous and explains why there is a visible thrust from theorists of all strands to comprehend the intricacies of this domain. Since the subject of this dissertation is this theoretical thrust in international relations, it does not employ any single theoretical perspective to proceed with the debate. However, the most conclusive explanation for the anomalous nature of cyberspace is the theory of cyber persistence.

Cyber persistence theory questions the established paradigm. It is a structural theory of cyber security that explains the underpinning logic of cyberspace conflict and competition. It is based on the premise that cyberspace is a distinct strategic environment and that all states are subject to it. This theory is applicable to all state and potentially non-state behaviors and argues that cyberspace is an arena of exploitation rather than coercion. Achieving strategic gains in this environment does not require the opponent to make concessions. Cyberspace is a manmade environment that can be reset and primed by states to their advantage without changing the decision calculus of the opposing side. Therefore, all states must anticipate the persistent resetting of the strategic environment and respond accordingly.

The theory of cyber persistence adopts a system-level analysis. It starts from the premise that cyberspace is a sociotechnical environment and that interconnectedness is its central feature. Interconnectedness means that states are in a structurally imposed condition of constant contact with all other actors in this global system. Constant contact is not a policy choice; it is the core condition that logically follows from operating in an interconnected world. This approach differs from a unit-level analysis of state behavior that assumes contact may also be imminent, potential, or episodic, but not constant. In cyber persistence theory, the interconnectedness of cyberspace carves out a distinct strategic environment that is defined by the prospect that at every minute of every day, some actor somewhere has both the capacity and will to exploit some vulnerability that allows access to one's national sources of power directly or indirectly.

This theory argues that the dominant form of state behavior in cyberspace will be exploitation short of armed-attack equivalence, not coercion or brute force. This primarily takes the form of cyber faits accomplis— a limited unilateral gain at a target's expense, where that gain is retained when the target is unaware of the loss or is unable or unwilling to respond. China's illicit cyber-enabled acquisition of IP and North Korea's exploitation of international financial systems to circumvent international sanctions are examples. A less prevalent type of exploitative action is direct cyber engagement, where a state directly engages with another actor for control over key cyberspace terrain. Examples include the US grappling with Trick Bot and ISIS network administrators and the November 2014 competition between the United States and Russia's APT29 for control over the Department of State and White House IT systems.

The principles of cyber persistence theory provide a more robust explanation for the behavior witnessed in the early twenty-first century. The abundance of open-source evidence available to researchers and policymakers aligns more clearly and comprehensively with cyber persistence theory than with the expectations and assumptions of coercion theories. Cyber persistence theory presents a stark contrast to the explanations, predictions, and prescriptions of deterrence theorists, who rely on a coercion frame to explain cyberspace behavior and its dynamics. Focusing on unilateral behavior rather than mutually dependent behavior yields greater explanatory power. Competitive interaction, rather than escalation, is the dominant dynamic in this space below armed attack equivalence. Cyber Persistence theory argues that lessons of nuclear war are irrelevant in the cyber domain which is why Libicki's cyber deterrence argument proposed in his work 'Cyberspace in Peace and War'.

Cyber persistence theory argues that while conventional warfare is a domain of confrontation, conduct of hostilities, and winning wars, nuclear warfare is the domain of coercion due to the absence of war because negative-sum outcomes rule out the possibility of war. However, cyberspace is predominantly a domain of exploitation where asymmetry in resources does not hinder any offensive

move, even by weaker states or actors. Another defining feature of cyberspace is the inevitability of connection and interactions, which cannot be muted but at the expense of loss to the economy. Interacting in cyberspace is imperative for states; they cannot mute these interactions. This theory proposes a foundational shift in theorizing the strategic arena of cyberspace. It discards the traditional theoretical paradigms that still carry a strong tint of the Cold War era strategic paradigms of deterrence and war. This theory treats cyberspace as a distinct strategic domain marked by episodes of conflict and perpetual competition.

- **Perpetual Strategic Competition**

This dynamic resembles the state of anarchy in world politics as argued by the realist thinkers. However, there is an important difference that this perpetual competition is mostly low intensity unlike active hostilities in the physical domain. This perpetual contest between actors in cyberspace remains mostly in the arena of exploitation unlike the physical domain where competition is more intense and states attempt to outdo each other through coercive means or by deterrence.

- **Domain of Exploitation**

Cyber persistence theory argues that cyberspace is inherently a domain of exploitation where states actively seek to exploit the technological vulnerabilities of adversaries and in pursuit of their strategic objectives, they make sure not to provoke adversaries into an actual war.

- **No Isolated Victory or Defeat in Cyberspace**

In cyberspace security is not attained through success in isolated conflicts or the deterrence of aggression; rather, it is accomplished through the continuous shaping of the cyber environment to advantage one's strategic position.

- **An Interconnected Domain**

The interconnected nature of cyberspace necessitates coordinated efforts across governmental and international domains, as no single entity possesses the capacity to govern

it independently.

- **A Strategic Domain Short of War**

In the realm of cyberspace, numerous operations do not escalate to the level of armed conflict, yet they exert considerable strategic influence. CPT argues that contemporary statecraft frequently involves "fait accompli" exploitations—actions that decisively influence outcomes without surpassing thresholds that would provoke conventional military responses.

- **Strategic Competition in a Gray Area**

Cyberspace represents a complex domain characterized by continuous international competition, thereby transforming the traditional war/peace dichotomy into a dynamic landscape of perpetual positioning and strategic maneuvering.

- **Irrelevant Nuclear Analogies**

The analogy to nuclear deterrence is inadequate in the context of cyberspace, where attribution is challenging and operational costs are minimal. Instead, security is achieved through active, persistent defense and offense, rather than passive deterrence. The offense-defense balance is dynamic, with emphasis placed on initiative and adaptability over static defense or threats of retaliation.

- **Different Bargaining Mechanisms**

Contrary to formal treaties, Cyber Persistence Theory (CPT) suggests that cyber stability is predicated on implicit negotiation and mutual signaling. States discern boundaries and acceptable conduct through repeated interactions, occasionally "accepting" adversarial activities provided they do not escalate to intolerable levels. This "normalization" of intrusion and exploitation establishes a stabilizing framework for international cyber relations, even as it facilitates ongoing low-level competition.

- **A Domain for All Actors**

Cyberspace encompasses both state and non-state actors, including entities such as private corporations, hacktivists, and criminal organizations. These actors play significant roles, thereby complicating global politics and blurring the traditional boundaries of power and sovereignty.

The below form shows how cyber persistence theory as a framework identifies the shortcoming of traditional theories and offers a new and compelling framework to analyze the disruptive impact of cyberspace on world politics.

Traditional Paradigms	Cyber Persistence Theory
Episodic conflicts or crises	Continuous strategic competition
Coercion and deterrence focus	Exploitation and initiative focus
War/peace binary	Gray zone, persistent positioning
State-centric	Involvement of multiple actor types

1.8 Methodology

This study is qualitative in nature, involving the use of analytical and descriptive methods. The approach used is that of social scientists, who generalize theories and extend their use to anomalous cases to test the explanatory power of these theories. Primary and secondary data, including official documents, speech transcripts, scholarly journals, monographs, and books of leading scholars on the topic, will be used to assess the proposed hypothesis. Although primary sources provide unadulterated accounts, they are subject to availability; therefore, research articles from reputed journals and prominent authors and theorists in the field will be used.

1.8.1 Research Design

Research design is a strategic framework for action that acts as a bridge between research questions and research implementation. The research design is the general structure or main design of any research. This research will be descriptive and analytical, drawing insights from scholarly journals, paper publications, policy documents, and case studies.

1.8.2 Operational Definitions

- **Cyberspace**

  The U.S. Department of Defense defines cyberspace as

  > "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers."

- **Cyberspace Attack**

The U.S. National Institute of Standards and Technology (NIST) defines cyberspace attack as

> "Cyberspace actions that create various direct denial effects (i.e. degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains."

1.8.3 Procedure (Data Collection)

Data will be collected from diverse and diametrically opposed sources to triangulate the research problem and assess the likely answers. Views on cyberspace's relevance to world politics are fragmented and scattered, with some researchers forecasting a cyberwar in the future while others dismiss it as a collective hallucination. There are plausible reasons on both ends, but contemporary developments conform to and substantiate the former view. Cyber-skeptics argue that the virtual domain of cyberspace is not a standalone thing but relies on physical infrastructure that resembles any other physical target in counterforce or

countervalue strikes. One can predict the trajectory of cyberspace from the forecast of the McKinsey Global Institute in 2018, which predicted that Artificial Intelligence (AI) has the potential to deliver an additional global economic activity of approximately $13 trillion by 2030 (Bughin et al., 2018). This huge potential for economic activity makes it difficult for states to downplay cyberspace's importance.

1.8.4 Data Analysis

Analytical and descriptive tools will be employed in this study to identify new patterns or incoherence in the established understanding, capitalizing on the existing literature, including case studies that offer detailed accounts of major cyber incidents worldwide. These incidents include cyber espionage, network breaches, data theft, ransomware attacks, attacks on critical infrastructure, and distributed denial-of-service (DDoS) attacks. Since the subject of this study cuts across various disciplines, frameworks, and reports, established protocols in information security, such as the CIA triad, will also be used.

Various academic experts in internation relations were reached to ascertain how academics and experts in the discipline see the developments in cyberspace and their implications for the established conceptions and major theories of international relations. These interviews helped add nuance to the study because they explained both the local and global dynamics since most of the scholars and practitioners have extensive interaction with academia and industry. The interviewees explicitly assented to include their views on this academic study without any need for anonymity. For the respondents from academia the responses are mostly theoretical in nature, but the practitioners' view tilted more towards the actual use of new technologies and the how the governments can regulate to mitigate their negative use.

1.9 Organization of the Study

This research comprises six chapters, each building on the previous chapter and furthering the research systematically.

Chapter One (Evolution of Cyberspace)

This chapter tracks the evolution of cyberspace from a purely military project to the commercialization and boom of the worldwide web, which today makes it an irreducible part of modern life that enables countless experiences.

Chapter Two (Cyberspace: New Threat Vectors)

This chapter extensively discusses how new technologies create new threat vectors, and essentially every new technology comes with a tradeoff of convenience and vulnerability. Paradoxically, developed societies are more vulnerable because of their higher levels of automation than developing countries.

Chapter Three (Cyberspace and Realism)

This chapter discusses how the emergence of cyberspace as a fifth domain challenged the enduring mainstays of realist theories and, by changing the conditions underpinning centuries of theorizing, forced theorists to come up with new interpretations for novel questions.

Chapter Four (Cyberspace and Liberalism)

This chapter discusses how cyberspace has furthered the liberalist worldview through its enabling nature and how liberal theory argues for keeping this new domain functional and not compromising its openness through interstate competition.

Chapter Five (Cyberspace and Constructivism)

This chapter discusses how new norms and rules can be proposed and how the rise of parallel realities impacts state interactions. It extensively debates norm construction and contestation

in the context of cyberspace.

Chapter Six (Overarching Cyber-Responsive Policies)

This chapter discusses the overarching nature of policies that are cyber-responsive because cyberspace itself by its very nature is enveloping. Therefore, any approach involving cyberspace will be inherently overarching.

Chapter Seven (Pakistan's Realization Episodes and Response)

This chapter discusses Pakistan's realization episodes (cyber wakeup calls), the shortcomings of Pakistan's cyber defense, and how it responded to these problems.

Conclusion

This chapter concludes the study by summarizing the answers to different anomalies in the form of research questions.

CHAPTER 2

2.. Evolution of Cyberspace

Cyberspace has forever transformed how individuals, entities, and states relate to one another, and its dynamics have altered global politics in ways that were previously unthinkable. Its ubiquity, speed, and instantaneous flow have taken over every aspect of life, and the field of international relations is no exception. Cyberspace is a virtual environment of interconnected digital networks (the Internet, telecommunication networks, and computer systems). Cyberspace moves beyond traditional physical boundaries through real-time communication and information sharing.

2.1 Etymology of Cyberspace

The word cyberspace is derived from cybernetics which has its roots in the ancient Greek word "kybernētēs" meaning a steersman, pilot, or rudder (Pym, 2021). In particular, the phrase first surfaced in the late 1960s artwork Atelier Cyberspace, which was jointly produced by Danish artists Susanne Ussing and Carsten Hoffman. In this piece, the term "cyberspace" refers to a collection of pictures and installations dubbed as "sensory spaces," which means an open physical area capable of sensing and adapting to human behavior as well as that of other things in that space. In the 1980s, American science fiction author William Gibson published several cyberpunk books, such as Neuromancer and Burning Chrome (Gibson, 2003). In its original definition, the term "cyberspace" refers to the digital realm produced by computers. It was specifically defined as "a graphic representation of data abstracted from the banks of every computer in the human system" and "a consensual hallucination experienced daily by billions of legitimate operators." (Gibson, 1984)

2.2 Varying Definitions of Cyberspace

The term "cyberspace" refers to the digital realm created by interconnected networks, including the Internet, telecommunication systems, and computer infrastructure. This virtual environment serves as a platform for generating, sharing, storing, and processing information and facilitates interactions between individuals, organizations, and nations. Unlike the physical realm, cyberspace is not confined by geographical limitations, enabling instant global communication and data transmission. Cyberspace is a multifaceted concept that encompasses the virtual environment of computer networks where data is stored, shared, and communicated. This includes the infrastructure, user interactions, and informational and social dynamics enabled by these technologies.

- **William Gibson's Definition**

The term "cyberspace" was first coined by William Gibson in his 1982 short story "Burning Chrome" and popularized in his 1984 novel, *Neuromancer*. Gibson envisioned cyberspace as a virtual reality data space, a computer-generated landscape where data could be navigated and manipulated as though it were a physical environment.

> "Cyberspace, a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters, and constellations of data. Like city lights, receding..." (Gibson, 1984).

Academics and scholars have further refined the concept of cyberspace to encompass the technological, social, and economic dimensions of virtual environments. For instance, Nye defines cyberspace as "the environment in which communication over computer networks occurs. It is a domain characterized by the use of electronics and the electromagnetic spectrum

to store, modify, and exchange data via networked systems and associated physical infrastructures" (J. S. Nye, 2017). In the context of law and policy, cyberspace is often defined with an emphasis on its implications for governance, security, and legal frameworks.

- **Clarke and Knake's Definition**:

Richard A. Clarke and Robert K. Knake describe cyberspace as

> "The virtual world that is a global common where people communicate, interact, and transact business through the use of computers and other networked devices. It is not a physical space, but a domain created by the interconnectedness of information technology" (Clarke & Knake, 2010).

In military and strategic contexts, cyberspace is defined in terms of its role in national security and defense operations.

- **The U.S. Dept. of Defense (DoD) Definition**

The U.S. Department of Defense (DoD) defines cyberspace as

> "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (DoD, 2011).

The concept of cyberspace is multifaceted and dynamic, encompassing both the digital realms generated by interconnected computers and the tangible and social impacts they exert. It has varying definitions depending on the context— literary, academic, legal, or strategic— but consistently underscores the interconnected and digital nature of contemporary data and communication systems.

2.3 Birth of the Internet

In 1969, the first message was sent across the Advanced Research Projects Agency Network (ARPANET), and it was from this first step that the Internet, as we know it today, was

born (Roberts, 1988). Now billions of people use the Internet every day, and it is interwoven into the fabric of the society. It has created tremendous access to information and technology for many populations across the globe; therefore, if there is Internet connectivity, everything that exists on the Internet can be accessed. Real-time global communications, fund transfers, and logistics chains are entirely dependent on the Internet, and the idea of a modern and efficient world is unthinkable without it. Although the Internet has helped ensure a permissive environment for global development in every field, at the same time it has also created a series of dependencies that have made the world vulnerable to new types of disruptions and threats.

The Internet has also created new vulnerabilities in critical infrastructure systems worldwide. For instance, the energy sector has increasingly adopted smart grid technologies and faces prominent information security risks and cyber threats (Song, 2018). The integration of the Internet into the way of life gives many options to any military to weaponize it, ranging from critical infrastructure to psychological operations and propaganda warfare. With growing automation, vulnerabilities and threats also grow, as do ethical questions such as the use of automated lethal weapons in conflicts.

2.4 Popularization of the Idea

Cyberspace has become a common term in a wide range of books, artworks, movies and television shows. In the 1990s, it became popular as a synonym for the Internet and computer networks. Various artistic works, scientific literature, and official government sources have different conceptions of cyber space. Due to the varying interpretations and intentions, there is still no single definition. Cyberspace is typically employed as a metaphor in artistic works to denote an imaginary or virtual environment created by computers and associated hardware. Despite being a disembodied and virtual realm, people can engage in all physical activities, including playing, buying, studying, and working in cyberspace, without being constrained by time or location. This ability to instantaneously connect and communicate

has challenged the fundamental mainstays of international relations by rendering temporal and spatial dynamics irrelevant to some extent.

Cyberspace is inherently disruptive because of the five factors that define its characteristics. These include temporality, virtuality, permeation, fluidity, participation, attribution, and accountability. Temporality means that information flow in cyberspace is instantaneous, and virtuality means that geographical borders are nonexistent (Choucri & Clark, 2018, p. 13). In the film The Matrix, cyberspace is depicted as an imagined place that resembles the real world but is run by artificial intelligence (AI) systems and computers. With hardware, humans can establish connections and exist in cyberspace. They play different roles in both the real world and cyberspace and meet their various needs by switching between these two spaces. Conversely, scientific literature and official governmental sources have emphasized the makeup and functionality of cyberspace. The term "cyberspace" is generally utilized as a generic and enveloping term for computer and communication technologies, which is conceptualized as a digital world with which people interact.

2.5 Cybersecurity: From a Movie Script to Policy

The idea that advances in information and communications technologies have serious implications for national security first came into consideration before the spread of the Internet as we know it today and the U.S. Department of Defense (DoD) ARPANET was only 15 years old at that time. Ronald Reagan was the first American president who sensed the evolution of computer systems and their growing impact on national security. Interestingly, this realization came after watching a movie in June 1983. In this movie (WarGames) a young hacker breaches the nuclear response system of the North American Aerospace Defense Command (NORAD), and his actions push the United States and the Soviet Union to the brink of a nuclear war (Kapell & Elliott, 2013, p. 284). The scenario in the movie was discussed with the security staff, and the only question at hand was the possibility of such breaches. Most of the national security

officials were skeptical because a few months ago, the president had asked scientists to materialize his Star Wars vision by making laser weapons that could shoot the incoming Soviet nuclear ballistic missiles in the case of a war. However, despite the prevailing skepticism, the Chairman of the Joint Chiefs, General John Vessey, assured that he would investigate it further.

After investigating Gen. Vessey reached a starkly different conclusion: the likelihood and potential impact of such breaches were far greater than initially expected. This triggered the entire national security apparatus in a new direction, and consequently, the National Security Division Directive (NSDD-145) was signed in September 1984 as the 'National Policy on Telecommunications and Automated Information Systems Security' (Kaplan, 2016, p. 3). Reagan's question, in essence, was what later developed into a specialized field of cybersecurity. The problem of security is rooted in the pathology of cyberspace because network information systems were not envisaged and designed with the intention of being secure but efficient, and there is a trade-off between usability and security. A completely secure system is a dysfunctional one, and every usable and functional system has its own shortcomings in terms of security (Cranor & Garfinkel, 2005, p. 18).

2.6 Economic Impact of Cyberspace

The economic impact of cyberspace is significant and multifaceted, affecting various aspects of the global economy and business practices. Cyberspace and e-commerce have become integral parts of the international economic landscape, requiring new governance and regulatory approaches (Kobrin, 2001). The digital economy, which utilizes digital technologies and electronic communication, has emerged as a primary driver of economic growth and development in many advanced countries (Xia et al., 2024). It has led to improved user experience, faster processing, and easier access to services and products, resulting in increased efficiency and productivity across various sectors. Although cyberspace offers numerous economic opportunities, it also presents challenges. Cyber fraud in online financial transactions

poses a significant threat to economic stability and requires specific regulatory measures (Fletcher, 2007).

Additionally, the digital economy's impact extends beyond traditional economic metrics, influencing social and cultural fields, work arrangements, and global connectivity. The economic impact of cyberspace is profound and far-reaching. It has transformed business models, created new industries, and significantly influenced economic performance and sustainability in countries worldwide (Bocean & Vărzaru, 2023). However, it also necessitates careful consideration of regulatory frameworks, security measures, and potential negative consequences to ensure that its benefits are maximized while mitigating risks.

2.7 Strategic Importance and Militarization of Cyberspace

Cyberspace has become a critical domain for states, with significant strategic importance in modern international relations and security (Deibert et al., 2012; Stevens, 2012). It plays a crucial role in national security, economic development, and political influence, making it a key arena for state competition and conflicts. States recognize cyberspace as vital for protecting national interests, conducting information operations, and achieving their military objectives. The ability to control physical infrastructure, deny information, and leverage cyber capabilities has become strategically important in conflicts (Deibert et al., 2012). Additionally, cyberspace offers unique opportunities for states to project power, conduct covert operations and influence global norms (Barrinha & Turner, 2024; Stevens, 2012).

The strategic importance of cyberspace has led to paradoxical outcomes. While states seek to enhance their cyber capabilities for national security, these actions often negatively impact global cybersecurity. The militarization of cyberspace and the focus on state-centric security approaches can overshadow individual citizens' security needs, creating a multi-dimensional security dilemma (Dunn Cavelty, 2014). Cyberspace has emerged as a critical

strategic domain for states, influencing national security, economic prosperity and international relations. Its importance is evident in the development of cyber deterrence strategies, norm-setting efforts, and ongoing competition between major powers such as the US and China (Stevens, 2012; Xuetong, 2020). As the digital age progresses, the strategic significance of cyberspace is likely to increase, shaping the future of international politics and global governance.

States have increasingly militarized cyberspace through various means and strategies. The development of offensive cyber capabilities and the integration of cyber operations into national security strategies have become central to modern statecraft (Jensen et al., 2024). States engage in cyber operations to pursue perceived strategic utility, although the success rate of these operations in achieving political or strategic objectives remains relatively low, estimated at less than 5% (Gomez & Villar, 2018). The militarization of cyberspace has led to a complex security dilemma that extends beyond traditional state interactions. This has resulted in a focus on national security that often overlooks the security needs of individual citizens.

The use of cyberspace as a tool for national security, both for warfare and mass surveillance, has had detrimental effects on global cybersecurity (Dunn Cavelty, 2014). In response to the militarization of cyberspace, there has been a growing discourse on international cyber norms. Some states, particularly small nations like the Netherlands and Estonia, have emerged as norm entrepreneurs, attempting to shape responsible state behavior in cyberspace (Adamson, 2019). However, the multiplication of norm entrepreneurs, including non-state actors such as technology firms, has led to uncoordinated and sometimes conflicting norms (Katagiri, 2021). Katagiri also contends that many norms of cyberspace behavior remain contested, despite some being accepted. The norm discourse in diplomatic venues has become

highly undemocratic, dominated by a small mix of great powers and active middle powers (Katagiri, 2021).

While states continue to militarize cyberspace, the effectiveness and consequences of these actions are uncertain. The complex interplay between state and non-state actors, coupled with the challenges of establishing coherent international norms, highlights the need for a more comprehensive and inclusive approach to cybersecurity that considers both national security interests and individual rights. War is an irreducible part of the human experience, but the methods and conduct of war have persistently changed over time. Technology defines the future of warfare by changing how decisions are made and providing previously unreachable capabilities. Lessons from the past inform the future, as every technological leap redraws the battle lines we once knew. Until now, all the revolutions in military affairs have occurred in the physical realm, but now the battleground has shifted to the virtual domain of cyberspace, along with kinetic operations in the physical domain (Mbanaso & Dandaura, 2015, pp. 17–24).

The amount of interconnected technology has fundamentally transformed the operational environment, familiar domains have grown increasingly complex, and the race to dominate the ultimate high ground has begun. After machines and algorithms dominated warfare, the speed of warfare accelerated considerably across the entire spectrum of capabilities, ranging from intelligence collection and target acquisition to mission execution in challenging physical environments. Today, our lives rely heavily on technological systems, and we are entangled in the tentacles of the Internet; thus, our data is prone to intrusion. Similarly, conflicts now occur in the virtual domain at the push of a button, bringing disorder without a single soldier setting foot on the ground.

For instance, two days before Christmas in 2015, lights went out in Ukraine after hackers infiltrated three electricity distribution companies. The intrusion was performed with

remarkable ease by simply attaching malware-infected code to Word documents and PowerPoint presentations sent to company executives. The malware called Black Energy was later attributed to a Russian cyber gang called Sandworm, which infiltrated the electrical company's computer systems and flipped the power grid circuit breakers. The intruders seized control of the electrical supply for almost a quarter of a million people. In the next phase, company call centers were inundated with a barrage of automated telephone calls, and multi-wave attacks were underway.

This chaos and confusion soon led to public outrage as complaints from frustrated customers went unheard and medical centers were overwhelmed. Ukraine was pushed into darkness without any intruder setting foot in the country (Baezner, 2018, p. 10). When services were restored in Ukraine, a new realization dawned that a highly coordinated cyber-attack had taken place. A group of hackers, with the help of malicious code, directly targeted and compromised a nation's power grid. This incident eliminated the clear division between the physical and cyber domains and demonstrated how actions taken in the cyber realm can affect the physical domain in a devastating way (Greenberg, 2019).

2.8 Temporality, Cyberspace, and International Relations

The intersection of temporality, cyberspace, and international relations highlights how time and digital technology influence global politics. This dynamic interplay challenges traditional notions of state sovereignty and reshapes diplomatic practices in many ways. The emergence of cyberspace as a distinct domain has fundamentally challenged the spatial and temporal dynamics of international relations (IR) theories. Traditional IR theories, particularly realism, are predicated on the notions of territoriality and the physical presence of state actors.

However, the characteristics of cyberspace—its borderless nature and the speed of interactions— necessitate a reevaluation of these established concepts. First, cyberspace operates on a transnational level, allowing interactions that transcend physical borders.

Cyberattacks occur continuously and globally, highlighting the need for international collaboration to effectively combat these threats (Back et al., 2018). This 24/7 operational nature of cyberspace challenges the realist focus on state-centric interactions, which are often bound by geographical constraints and time. The fluidity of cyberspace means that actions taken by one state can have immediate repercussions across the globe, complicating the traditional understanding of power dynamics and their influence on international relations.

Moreover, the temporal dynamics of cyberspace introduce a rapidity that is often at odds with the slower pace of traditional diplomatic processes. Manjikian notes that the Internet has transformed the battlefield into a virtual space where decisions and actions can be executed almost instantaneously, thus altering the strategic calculations of states (Manjikian, 2010). This speed can lead to escalations that outpace diplomatic responses, challenging the realist assumption that states can manage conflicts through calculated power plays and negotiation. The implications of these spatial and temporal shifts extend to the concept of sovereignty itself. Cavelty and Wenger argue that the intelligence community's role in cyberspace has evolved, as it has become a key player in shaping norms and responses to cyber threats (Cavelty & Wenger, 2022).

This shift indicates a fragmentation of authority, where state sovereignty is increasingly challenged by non-state actors and transnational networks operating in the digital realm. The traditional realist view, which emphasizes the state as the primary actor in international relations, is undermined by the emergence of these new dynamics. Additionally, the complexity of cyberspace necessitates a nuanced understanding of international law and norms. The obligation of due diligence in cyberspace highlights the challenges of establishing clear legal frameworks that can adapt to the rapidly changing nature of cyber interactions. This legal ambiguity complicates the realist perspective, which relies on established norms and rules that

govern state behavior. Furthermore, the interconnectedness of cyberspace with physical and social dimensions complicates the spatial theories that are traditionally employed in IR.

Kademi and Koltuksuz (2021) argue that cyberspace exists as a hybrid entity intertwined with physical infrastructure and social interactions, thereby challenging binary distinctions between different domains. This interconnectedness requires a reevaluation of how states engage with one another because actions in cyberspace can have profound implications for physical security and political stability. The rise of cyberspace as a distinct domain has significantly challenged the spatial and temporal dynamics of international relations theories. The transnational nature of cyber interactions, immediacy of actions, fragmentation of authority, and complexities of legal frameworks all necessitate a reevaluation of traditional IR concepts. As states navigate this new landscape, the need for adaptive strategies and collaborative approaches becomes increasingly evident, marking a departure from state-centric models that have historically dominated the field.

Understanding these temporal aspects is crucial for navigating the complexities of global politics in the digital era. Choucri and Goldsmith (2012) discuss how cyberspace disrupts traditional international relations theories that are rooted in the 19th and 20th centuries. The fluidity and anonymity of cyberspace challenge state-centric models and introduce new patterns of cyber-based conflict and cooperation (Choucri & Goldsmith, 2012). Drezner (2020) explores how assumptions about time affect the conceptualization of power in international relations theory. This study emphasizes the importance of understanding the temporal scope and feedback effects in the exercise and accumulation of power (Drezner, 2020).

Choucri and Clark proposed the integration of cyberspace into international relations, creating a socio-technical system called Cyber-IR. This framework addresses how digital interactions influence traditional IR activities such as trade, diplomacy, and security (Choucri

& Clark, 2012). Choucri also investigated the implications of cyberspace for international relations theory, policy, and practice. This study highlights how cyberspace challenges concepts such as national security, diplomacy, and borders, necessitating new analytical frameworks (Choucri, 2012).

Solomon examines the role of temporality in shaping subjectivity in world politics, drawing on psychoanalytic theory. This study discusses how time and desire influence political identities and behaviors, with implications for understanding international conflicts (Solomon, 2014). Holden explores the concept of timescape to analyze the European Union's fragmented power and long-term strategic goals. This study emphasizes how different temporal frameworks influence the EU's foreign policy and structural relationships (Holden, 2016). Hom discusses the "temporal turn" in critical international relations, highlighting the political importance of time. This study critiques linear and timeless visions of politics, advocating for a more nuanced understanding of temporal dynamics in global affairs (Hom, 2018). He also provides a comprehensive account of how temporal assumptions shape the study of international politics. The book argues for a reimagined approach to time in IR, emphasizing the importance of narrative timing techniques in understanding political events (Hom, 2020).

The intersection of temporality, cyberspace, and international relations introduces new complexities and opportunities in global politics. By integrating digital technologies and understanding temporal dynamics, policymakers and scholars can better navigate the evolving landscape of international relations in the digital era. The concept of temporality in cyberspace has significantly impacted International Relations (IR) theory, challenging traditional notions of time and space in global politics. Cyber communities and online social relations have evolved to a point where they necessitate new theoretical frameworks to understand their implications for IR (Fernback, 2007).

The emergence of cyberspace as a domain of conflict has led to a reconsideration of traditional IR concepts, such as deterrence and coercion. The unique characteristics of cyberspace, including its non-physical nature and the speed at which events unfold, limit the applicability of conventional deterrence theory (Taddeo, 2018). Similarly, the dynamics of coercion in cyberspace differ from those in traditional domains, requiring a reevaluation of warfighting strategies and their effectiveness in the digital realm (Borghard & Lonergan, 2017). Temporality in cyberspace has prompted IR scholars to reconsider fundamental concepts and theories. The need for new approaches that account for the fluidity and contingency of international events in the digital age has become evident (McIntosh, 2015). As cyberspace continues to shape global politics, IR theory must adapt to better model and predict international political practices in this dynamic and interconnected domain.

2.9 Spatiality in Cyberspace and International Relations

The concept of spatiality in cyberspace and its implications for international relations involves understanding how digital spaces influence and reshape political, economic, and social interactions on a global scale. This involves examining how cyberspace is mapped, governed, and used as a new dimension of international politics. Cyberspace introduces a new realm of spatiality that transcends traditional geographic boundaries. This has profound implications for international relations, as it alters how states interact, exercise their power, and engage in diplomacy.

Kitchin emphasizes that spatiality is central to the understanding of cyberspace. The study introduces cyberspace to geographers and suggests an agenda for future research that integrates cyberspace into geographical studies (Kitchin, 1998). Crampton uses concepts from Michel Foucault to map cyberspace, arguing that it has a rich geography of political practices and power relations. The book highlights how maps shape political thinking about cyberspace and includes case studies on crime mapping and geo-surveillance (Crampton, 2003). Gao et al.

(2019) explored the theoretical foundations of cyberspace geography, extending geographic research to virtual spaces. They discuss the need for innovative methods to map and understand cyberspace, emphasizing its importance for national security and cybersecurity (C. Gao et al., 2019).

2.10 Ubiquity in Cyberspace

The ubiquity of cyberspace presents significant challenges to the traditional theories of international relations. The complexity and rapid evolution of cyberspace make it difficult to apply conventional IR theory. Cyberspace introduces new dimensions to international conflicts and governance that traditional IR theories struggle to account for. Deibert et al. (2012) discuss the emergence of "cyber-privateering" and the "unavoidable internationalization of cyber conflicts," which challenge traditional state-centric models of international relations. The paper also introduces the concept of "cyclones in cyberspace," referring to the tendency to magnify unanticipated outcomes in cyber conflicts (Deibert et al., 2012).

The governance of cyberspace presents unique challenges that require novel approaches to address them. Kobrin argues that effective governance of cyberspace will require significant international cooperation and public-private sector collaboration, which may not align neatly with existing IR theories (Kobrin, 2001). Similarly, Weiss and Jankauskas highlight how states navigate between functional and national security imperatives in designing cybersecurity governance arrangements, often employing a mix of delegation and orchestration depending on the nature of the cybersecurity problem (Weiss & Jankauskas, 2019). The ubiquity of cyberspace necessitates the reevaluation and adaptation of traditional IR theories. As cyberspace continues to blur the lines between the physical, digital, and biological spheres (Carr & Lesniewska, 2020), IR scholars and policymakers must develop more flexible and comprehensive frameworks to understand and navigate this complex domain.

2.11 Anonymity in Cyberspace (Attribution Problem)

The Tallinn Manual provides the rules of how nation states should operate when it comes to cyber warfare operations. In 2007, the Estonian city of Tallinn became an unlikely cyber warfare hotspot. Tallinn is the capital of Estonia and one of the first environments where a significant Russian cyber warfare attack occurred. The Estonian authorities relocated a bronze statue of a World War II Russian soldier and remains from several Soviet war graves from Central Tallinn to the outskirts of the city. For the Estonian people, the war memorial represented Russian occupation, but for the Estonians of Russian descent, it represented liberation from Nazi forces. Moving the statue to a lesser-known location was symbolic for both groups, and its relocation sparked ethnic outrage. Fueled by Russian media, it triggered protests and riots between Estonians and Russian descent Estonian population, which then culminated in a cyber-attack emanating from an enemy state (Brüggemann & Kasekamp, 2008).

This cyber-attack disabled Estonia's highly connected digital infrastructure, including government websites, banking, and the media industry was hit hard. Detecting an attack in cyberspace is not the difficult part, but attributing responsibility for that attack to a particular actor and then figuring out the actor's intent is extraordinarily difficult. As access to cyber capabilities grow, this problem will worsen. Estonia was quick to pin the blame on Russia, and the foreign ministry produced a document linking Russian government internet addresses with the attack, but Russia has repeatedly denied involvement.

This cyberattack signaled a new form of warfare where states can bank on deniability and use non-state actors for such operations. Non-state actors can strike unnoticed without the need to use military equipment. As the burgeoning threat of cyber warfare grew, NATO quickly stepped in to independently assess and report on the Estonian cyber-attack. The waves of cyber-attacks that hit Estonia's websites are a security issue that concerns NATO; therefore,

cyberspace must be protected just as land, air, and sea. Barely a year later, in 2008, the Republic of Georgia, a pro-Western neighbor to Russia, fell victim to a series of cyber-attacks. It disabled government websites and crippled banks, communications, and transport companies. This cyber-attack created an information vacuum, allowing Russia to control the war narrative and paving the pathway for their invading forces.

By 2009, NATO, along with academics and international lawyers, had composed the Tallinn Manual, an academic study on how international law applies to cyber conflicts and cyber warfare (Jensen, 2016). NATO founded a cyber warfare center of excellence in Estonia, tasked with figuring out ways to counter hybrid warfare in cyberspace. Now, an attack on a state entity that involves or could involve loss of life, serious injury, or damage to a major state asset could potentially be considered an act of war. Cyberattacks can originate from an enemy state or a lone rogue actor. Evaluating the impact of an attack is one thing but determining who is behind the attack and why they attacked is entirely different. Once attribution and intent are established, the state subject to the cyber-attack can launch a proportional response in return.

Retaliation against the wrong target can be calamitous and an incredibly difficult technical problem because it is difficult to locate the actual origin of a particular attack. Even in well-defined and well-studied attacks, attribution is often not stated explicitly because cyber-attacks leave no spent munitions or military equipment. Non-state actors can deliver devastating blows to the economies of the most powerful countries in the world. Self-recruited ad hoc networks that are not tied to any state are essentially free-floating and willing to do their own thing in the service of a particular ideology. There is no equivalent of DNA in cyberspace that can identify a piece of information and establish any link to a particular state or individual. The attribution dilemma complicates the cyber warfare landscape and nullifies traditional ideas

of deterrence strategies, but states still navigate the digital minefield of cyberspace and enact their strategies to overcome any opposition (J. R. Lindsay, 2015).

In 2018, in response to the need for states to attribute cyber-attacks, the U.S and its allies launched persistent engagement and the cyber deterrence initiative, and under both those policies, the U.S. and its allies have agreed to first attribute attacks to the countries undertaking them and warn them at the same time that continued attacks will be followed by retaliation either in or outside cyberspace (Gold, 2020; Healey, 2019). The U.S. law of war manual (2015) tried to legitimize a kinetic response to cyberattack if the kinetic response is proportional and necessary (DoD, 2015, p. 1000). A recent example suggests that the opposite is also true, responding to a kinetic high-power attack with a cyber-attack. In June 2019, in the Strait of Hormuz off the coast of Iran, an American Global Hawk drone was shot down by Iran. Since Iran targeted something without a person in it, a proportionate U.S. response followed this kinetic attack in the form of a cyberattack (Hatzman et al., 2019). The U.S. responded by taking out missile launches and targeting the databases of some Iranian government agencies. Iran claimed that the drone violated its airspace, which the U.S. denied, saying that the drone was in international airspace, and the U.S. had the right to respond. This is an example of proportionality in the context of cyber-attacks.

The restraint on the part of the United States seems to have been part of an overall strategy to de-escalate things in the Strait of Hormuz, so as to use operations that fall short of conventional definitions of armed attack, blur the lines between wartime and peacetime, and take full advantage of the attribution dilemma. Such operations are conducted in the gray zone, not fully covert or clandestine, but certainly not overt, and more on the borderline of detectability in that liminal maneuver space. The gray zone, a non-geographic borderless realm outside of any real jurisdiction, is highly exploitable by adversaries, where the very definition

of confrontation can be contested. There are many definitions of the gray zone, and the rise of influence operations, political warfare, and information warfare in this gray zone is obvious. States operating in the gray zone take advantage of legal uncertainty because it allows them to conduct effective operations until the costs of this approach outweigh its benefits. It is not just legal uncertainties but also the exploitation of the difficult ethical and political choices surrounding the escalation of a crisis into a full-blown war.

Some of the examples that we talked about before are Russian interference in the 2016 American presidential elections and Stuxnet. Under existing definitions, they fall short of the use of force or an armed attack, but they highlight that there is enough room in terms of preventing a state from conducting its internal affairs, which amounts to a breach of sovereignty. Cyber warfare can balance the scales of traditional military power, placing power back into the hands of weaker states. It has incentivized countries that were once considered not particularly cyber literate to rush toward enhancing their cyber capabilities. Many countries that are not particularly significant military threats are quickly becoming cyber superpowers. Extensive resources are not required to generate significant capabilities in the cyber realm. North Korea is a great example of a country that has put a lot of effort into cyber warfare (M. Kim, 2022). China has very capable cyber troops that caught up in the early 21st century in response to lessons learned from watching the U.S. in the period since the Cold War.

Today, the boundary between peacetime and wartime is blurred. New cyber and information warfare capabilities have opened a new space for political conflict between countries such as China and the U.S. and Russia and the U.S. Cyber capabilities have opened a new arena of conflict below the level of armed conflict. Revelations that have come out in September 2019 about a cyber-attack on Australia by China and Russian interference in the U.S. presidential elections in 2016. The contestation on the idea of international law is that

relations between states will be stable and predictable. Certain states will eventually reach a threshold where operating in the gray zone becomes too costly, and then a collective recognition that operations that technically fall short of the use of force or armed attack still have tremendous disruptive potential and probably need to be regulated as some kind of breach of sovereignty or interference in the state's affairs.

We are at the dawn of the cyber age, and there has been an increased focus on the capability and feasibility of use and this notion about how these devices and interconnectivity can be very helpful. The digital and physical domains are integrated, overlapped, and intermeshed, and separating the two is almost impossible. Cyber warfare will shape future warfare and the future of humanity. The future of warfare is multi-wave, multi-vector attacks against civil, military, and community targets on a scale not imagined before.

2.12 Defenders' Dilemma in a Pro-Offense Domain

We have so far focused only on the development of new technologies without giving much thought to security, and since the beginning, the design of the Internet has been based on openness and connectivity, which have obvious benefits (M. Libicki, 2011). We have developed many new technologies with barely any security or privacy, and patching the existing vulnerabilities in these systems is a colossal task. New technologies often emerge with a focus on innovation and functionality, sometimes at the expense of robust security. This trend is evident across various sectors, including finance, manufacturing, and information technology. In the financial industry, digital technologies have expanded the reach of financial services and driven innovation, but they have also introduced new network security management challenges (Q. Li, 2022).

Today, to understand what cyber warfare looks like from offensive and defensive aspects, we must first consider the pervasive computerized systems deployed in each country's

armed forces and civil sectors. Cyber warfare has become an integral part of modern military operations, encompassing both offensive and defensive aspects that target pervasive computerized systems in the armed forces and civil sectors. The offensive nature of cyber weapons has gained prominence, as demonstrated by the Stuxnet attack on Iranian enrichment facilities in 2010 (Shaheen, 2014, pp. 77–93). This incident highlighted the potential for cyber weapons to cause physical damage and sparked debates about cyber security. From an offensive perspective, cyber operations have evolved from signals intelligence and electronic warfare, capitalizing on the vulnerabilities created by the increasing reliance on interconnected military and civilian networks (D. Moore, 2022). The low cost and rapid effect of cyberwar encourage its use not only in armed conflicts but also below the standard threshold of war (Rudesill, 2021). Machine Learning has emerged as a potential solution for enhancing offensive cyber operations, enabling large-scale attacks, and supporting asymmetric operations (Nica & Tănase, 2020).

On the defensive front, Computer Network Defense (CND) plays a crucial role in protecting information assets. The CIA triad (confidentiality, integrity, and availability) and AAA (authentication, authorization, and auditing) are key principles for defending against cyberattacks (Andress & Winterfeld, 2014). However, defensive information warfare (DIW) has not advanced significantly beyond the information assurance model, falling short of meeting the need for a robust defense of critical command-and-control networks against sophisticated adversaries (French, 2004).

Heavy reliance on automation creates vulnerabilities, and civil infrastructure is likely to be targeted as a military system because the war effort depends on society as a whole and not only on the military. Another serious shortcoming is the weak human link in the entire cybersecurity effort; the most secure systems are also vulnerable if a workforce is not trained

in safe cyber practices and a robust information security audit and compliance system is not in place.

Therefore, cyberspace is an arena in which offense is easier than defense. (Nye, 2017 defence) Cyber defense is a costly and perpetual struggle, but intruders just need one weak link in the entire system. In many cases, this weak link is human because system operators and employees get trapped through social engineering and allow unauthorized access (Metwally & Mohammed, 2022). The effort required to secure a computer system is exponentially higher than that required to penetrate it. The resources and effort required to penetrate a computer system are linear because an intruder requires only a single vulnerability. Cyber warfare is disruptive and heralds a new era of military operations, reshaping the combat zone into a multi-platform digital battle space where data is the loaded gun.

The potential for cyber-attacks to impact the physical world was realized as early as 2010 when the Natanz nuclear facility in Iran was attacked by the malicious malware computer program Stuxnet. This exploited Iran's nuclear enrichment facility and worked through the facility's industrial control system. The Siemens Control Systems made the gas centrifuges speed out of control, and subsequently one in five centrifuges was removed from the facility where it was deployed (Baezner & Robin, 2017). The Stuxnet malware also secretly recorded daily operations within the facility and played them in a loop to plant operators to convince them that everything was normal. In fact, the centrifuges were blown up between 2009 and 2010, and around 1000 centrifuges in the Iranian facility were destroyed, causing a serious setback to the Iranian nuclear project (J. S. Nye, 2017b, pp. 44–71).

Losing 1000 centrifuges for a country that was already under nuclear embargo meant that its resources were greatly stretched. The success of Stuxnet at the Natanz nuclear facility signaled a paradigm shift in the ways of war, something that traditional war and conventional

military operations never saw coming and had not only become a reality but yielded surprising results (Kerr et al., 2010a, p. 8). The notion of cyber-attacks and cyber warfare has evolved significantly over the last few decades (Greenberg, 2019).

CHAPTER-3

3. Cyberspace: New Threat Vectors

The rapid pace of technological advancement continues to expand the capabilities and applications of cyberspace. Innovations in Artificial Intelligence (AI), big data, cloud computing, and the Internet of Things (IoT) are transforming all sectors and introducing new challenges and opportunities. Cutting-edge innovations, such as quantum computing and 5G technology, are poised to transform the digital landscape, offering improvements in speed, security, and interconnectivity within cyberspace. Technological advancements in cyberspace have profoundly affected world politics, reshaping how states interact, how power is exercised, and how international relations are conducted.

The evolution of sophisticated cyber capabilities has altered the landscape of warfare and national defense. Critical infrastructure, governmental systems, and private sector networks are vulnerable to cyberattacks, which pose substantial risks to a nation's security. Traditional military capabilities have been augmented by a new dimension: the capacity of nations to execute offensive cyber operations (OCOs). Clarke and Knake discuss how cyber warfare can disrupt national security and international stability, highlighting incidents such as the Stuxnet attack on Iran’s nuclear facilities (Clarke & Knake, 2010).

In 2010, the identification of Stuxnet, an exceptionally complex computer virus, represented a crucial turning point in cyber warfare. Engineered to undermine Iran's nuclear enrichment program, Stuxnet has proven consequential for global diplomacy, defense strategies, and the evolution of digital conflicts. The Stuxnet incident revealed how cyber weapons could inflict harm on essential infrastructure, upending the conventional notions of military capabilities and warfare. This event ushered in a new age in which pieces of code could accomplish strategic goals without resorting to traditional armed forces (Collins & McCombie,

2012). The use of Stuxnet also sparked global competition in cyber warfare, compelling countries to strengthen and expand their offensive and defensive capabilities in the cyber realm (Denning, 2012). States now consider cyber-attacks as a strategic tool that can be used to achieve specific geopolitical goals with reduced risk and cost compared to traditional military operations.

Stuxnet showed that cyber operations could delay or disrupt adversaries' critical projects without direct military confrontation and hostilities (Farwell & Rohozinski, 2011). The successful use of Stuxnet influenced military doctrines worldwide and pushed states to integrate cyber operations into broader military strategies and planning. This shift underscores the importance of cyber capabilities in national defense strategies (J. R. Lindsay, 2013). The incident also sparked discussions about the legal implications of cyber warfare in the context of international law. These debates center on the legitimacy of using force in cyberspace and the application of principles such as distinction and proportionality when conducting cyber-attacks (Haataja & Akhtar-Khavari, 2018). This event underscored the necessity for well-defined legal guidelines to regulate government actions in the digital realm and to tackle the issues raised by cyberattacks targeting essential infrastructure (Richardson, 2011).

Stuxnet also increased geopolitical tensions, particularly among Iran, Israel, and the United States. It demonstrates how cyber operations can be used as a tool of statecraft, impacting international diplomacy and relations (Yannakogeorgos & Tikk, 2016). In response to the threat posed by cyber-weapons, many countries have developed or enhanced their national cybersecurity policies, established cyber commands, and increased their investments in cyber defense capabilities (Butrimas, 2014). Stuxnet challenged the existing assumptions about the protection of critical infrastructure, revealing vulnerabilities in industrial control systems that were previously considered secure due to their isolation from the Internet, which

in technical cybersecurity terms is called an air gap (Karnouskos, 2011). This incident spurred major innovations in cybersecurity methods and technologies, resulting in enhanced protection against complex digital threats (Clark et al., 2013).

Stuxnet has profoundly impacted world politics by introducing cyber weapons as viable tools for achieving strategic objectives, influencing military doctrines, raising legal and ethical questions, and altering the geopolitical landscape. This incident underscores the importance of developing robust cybersecurity frameworks and international norms to address the challenges posed by cyber warfare. Stuxnet specifically targeted Iran's nuclear enrichment facilities, sabotaging centrifuges by altering their operational speeds and providing false feedback to operators, thereby delaying detection (Kerr et al., 2010b).

This attack revealed several key aspects of modern cyber warfare. First, Stuxnet highlighted the increasing sophistication and complexity of cyber weapons. It exploited multiple zero-day vulnerabilities and used advanced methods to infiltrate and propagate within highly secure environments (Lindsay, 2013). The worm's ability to operate covertly for an extended period before being detected underscores the challenges of defending against such sophisticated threats. Second, it demonstrates the strategic use of cyber weapons as tools for achieving geopolitical objectives without direct military confrontation. The attack on Iran's nuclear facilities delayed uranium enrichment and potentially altered geopolitical dynamics in the region without the immediate risks associated with conventional military actions (Lindsay, 2013).

Furthermore, the event highlighted the weaknesses in critical infrastructure systems, many of which were originally designed without considering cybersecurity. This incident highlighted the necessity for enhanced security protocols in Industrial Control Systems (ICS)

and Supervisory Control and Data Acquisition (SCADA) systems, both of which are essential for managing critical infrastructure operations (Abu-Nimeh et al., 2013).

Finally, Stuxnet highlighted the moral and juridical intricacies of cyber conflicts. The clandestine nature of the assault, its consequences on a country's vital infrastructure, and the participation of government entities prompted discussions about the standards and regulations governing state conduct in the digital realm (Baylon, 2017). Overall, Stuxnet's impact on cyber warfare is profound, as it has reshaped the understanding of cyber capabilities, highlighted the vulnerabilities of critical infrastructure, and sparked debates on the ethical, legal, and strategic dimensions of offensive cyber operations.

3.1 Information Warfare and Influence Operations

The digital realm has emerged as a crucial arena for information conflicts, where various entities, including governments and non-governmental groups, conduct campaigns to influence public sentiment, distort information, and disrupt other nations' political systems. The exploitation of digital platforms, including social media, for influence campaigns has been extensively documented. A notable instance is Russian meddling in the 2016 United States presidential election, which involved the widespread utilization of social media channels to disseminate false information and create societal divisions (Bennett & Livingston, 2018).

Advancements in digital surveillance technologies have enabled states to monitor and control their populations more effectively. The consequences for personal privacy, individual freedom, and fundamental human rights are substantial. Zuboff explores how digital surveillance by state and corporate actors threatens individual privacy and democratic governance. She contends that the widespread use of surveillance technologies in countries such as China illustrates the potential for state control and repression (Zuboff, 2019). However, the adoption of digital technologies in governance has transformed state operations, enhancing

efficiency, transparency, and public engagement. E-government initiatives streamline administrative processes and improve service delivery. West delves into the benefits of e-government, including increased transparency and citizen participation. Digital governance initiatives in countries such as Estonia demonstrate the potential of technology to enhance democratic processes and government efficiency (West, 2004).

The worldwide reach of the Internet necessitates collaboration among nations and the creation of guidelines to regulate how countries conduct themselves in the digital realm. It is essential to work towards developing cybersecurity standards and treaties to ensure stability and reduce the risk of conflicts in cyberspace. According to Nye, establishing international standards for cyberspace is crucial for managing conflicts and fostering stability. International bodies, such as the United Nations, are essential for promoting discussions and collaboration on cybersecurity matters (J. S. Nye, 2017).

Technological advancements in cyberspace drive economic growth and shift the balance of power. States that lead in technological innovation gain significant advantages in terms of global competitiveness and economic influence. Technological advancements in cyberspace have far-reaching implications for global politics. They influence national security, governance, international norms, and economic power. Policymakers and researchers must comprehend these effects to grapple with the intricacies of the digital era.

3.2 Security Concerns in Cyberspace

Cyberspace presents numerous security concerns that affect individuals, organizations, and nation states. The spectrum of issues encompasses digital offenses, cyber-based extremism, clandestine information gathering, and the defense of essential national infrastructure. The increasing prevalence of digital crimes, unauthorized system access, and cyber-based terrorism presents substantial risks to people, corporations, and national defense. Malicious online

activities targeting essential infrastructure, monetary institutions, and governmental data systems can have dire and far-reaching consequences. These attacks can disrupt essential services, cause financial losses, and compromise sensitive data, thereby posing significant threats to national security and economic stability.

The impacts of such attacks can be particularly devastating when they coincide with other crises, such as extreme weather events. For instance, a compound cyber-physical threat scenario involving a cyber-attack during a heatwave could lead to a 12% unserved electric load in Long Island, affecting nearly 198,000 customers and potentially decreasing state and local government enterprise activity by 37% (Avraam et al., 2023). Ensuring cybersecurity involves a complex interplay of technical safeguards, legal frameworks and international cooperation. States, organizations, and individuals must work together to protect against cyber threats and enhance their resilience.

3.2.1 Cybercrime

Cybercrime encompasses a wide range of illegal activities conducted over the Internet, including identity theft, financial fraud, and malware distribution. The past decade has witnessed significant growth in financial cybercrime, particularly credit card fraud and identity theft, which have become increasingly globalized in a digital ecosystem (Kraemer-Mbula et al., 2013). Cybercrime has become a significant threat to individuals, organizations, and societies, with a substantial impact on countries' GDP (Djenna et al., 2023). The COVID-19 pandemic expanded the cybercrime threat landscape, leading to increased opportunities for cybercrime and fraud as people spent more time online (Kemp et al., 2021).

To combat this growing issue, various detection and prevention techniques have been developed, including collaborative deep learning approaches for the early identification of botnet attacks (Djenna et al., 2023). However, the complex nature of cybercrime necessitates

ongoing research and the development of effective countermeasures to address this evolving threat. Brenner also points out the staggering costs of cybercrime, “Cybercrime has become a significant threat to financial systems worldwide, with annual losses estimated in the billions of dollars” (Brenner, 2010 p.39).

3.2.2 Cyberterrorism

Cyberterrorism refers to the use of cyberspace to conduct terrorist activities, including attacks on critical infrastructure, dissemination of propaganda, and coordination of such attacks. Lewis discusses the potential for cyber terrorists to target critical infrastructure such as power grids, water supply systems, and communication networks. The vulnerability of critical infrastructure to cyberattacks poses a significant national security threat (Lewis, 2002 p.27). Cyberterrorism has the potential to cause lethal consequences similar to those of conventional terrorism, especially when aimed at critical infrastructure (Backhaus et al., 2020). Cyberterrorists exploit vulnerabilities in computer networks to gain access to sensitive information, disrupt essential services, and cause widespread damage (Embar-Seddon, 2002).

The scope of cyberterrorism includes data theft, data manipulation, and disruption of essential services, with potential impacts on power grids, hospitals, and transportation systems (Iftikhar, 2024). Public perception plays a significant role in classifying cyberattacks as acts of terrorism. Research shows that the public refrains from labeling attacks by unknown actors or hackers as cyberterrorism and tends to classify attacks that disseminate sensitive data as terrorism to a greater extent than physically explosive attacks (Shandler et al., 2023). This finding contradicts the common assumption that physical attacks are perceived as more severe. Additionally, while cyberterrorism is often dramatized in popular media, there is a legitimate danger, and a clear understanding of the threat must begin with a precise definition (Embar-Seddon, 2002).

Cyberterrorism poses a significant threat to society, with the potential to cause extensive damage to critical infrastructure, economic losses, and even loss of life. The interconnectedness of digital systems and decreasing entry barriers for malicious actors have made cyberterrorism a growing concern (Iftikhar, 2024).To counter this threat, effective intrusion detection methods, robust cybersecurity regulations, and resilient cyber-physical systems are essential (Hansen et al., 2007). As the fields of cyber conflict and international security evolve, it is crucial to develop a conceptual baseline and standardized approaches to address the challenges posed by cyber terrorism (Shandler et al., 2023; Srinivas et al., 2019).

3.2.3 Cyberespionage

Cyber espionage involves unauthorized access to sensitive information by state or non-state actors, often for political or economic gain. This poses significant risks to national security and corporate competitiveness. Clarke and Knake (2010) highlight the growing threat of state-sponsored cyber espionage, in which nations exploit cyber capabilities to gather intelligence on rivals. Cyber espionage allows states to access critical information without physical intrusion, making it a preferred method of intelligence gathering (Clarke & Knake, 2010 p102).

Cyber espionage is a major concern for national security, as it can compromise critical infrastructure and sensitive information. These attacks can directly impact human safety because they can disrupt and manipulate equipment widely used across industrial processes, such as water treatment facilities, gas plants, and power plants. (Al-Hawawreh & Moustafa, 2024). It can target dual-use command, control, communication, and intelligence assets, potentially leading to inadvertent nuclear escalation between nations (Acton, 2018). This dynamic alone explains the volatility of South Asia, where three nuclear powers, China, India, and Pakistan, have a history of wars and hostilities. This form of entanglement between nuclear and non-nuclear capabilities creates a dangerous situation in which misinterpreted warnings or damage-limitation windows could escalate conflicts.

The threat of cyber espionage extends beyond direct attacks on state assets. It can also impact the private sector through industrial espionage, affecting national wealth generation and the overall digital economy (Parn and Edwards, 2019). This blurs the line between state and non-state actors in cybersecurity, making it challenging to effectively attribute and respond to threats. Cyber espionage represents a complex and evolving threat to states, requiring comprehensive cybersecurity policies and international cooperation (A. Mishra et al., 2022).The interconnected nature of modern digital infrastructure means that cyber espionage can have far-reaching consequences, from compromising national security to disrupting economic stability. States must adapt their security strategies to address these multifaceted challenges in a rapidly changing cyber landscape (Guitton & Fréchette, 2023).

3.2.4 Critical Infrastructure Protection

Protecting critical infrastructure from cyber threats is a paramount concern. This includes sectors such as energy, transportation, finance, and healthcare, where disruptions can have catastrophic effects. Critical infrastructure systems are highly interconnected and complex, rendering them vulnerable to cascading failures across domains (Linkov et al., 2022). For instance, a cyberattack on an electrical power network could disrupt food supply chains, affecting food security and community resilience (Nozhati et al., 2019). Similarly, smart home infrastructure vulnerabilities can be exploited to launch community-level cyberattacks, potentially causing large-area power system blackouts through cascading effects (Y. Liu et al., 2016).

However, the effectiveness of current cybersecurity approaches varies by sector. Factors such as the nature of the cyber threat to firms' operations and regulatory pressure on firms play significant roles in determining policy success (Atkins & Lawson, 2021a). Additionally, the complexity of critical infrastructure dependence analysis necessitates the partitioning of complicated dependencies into cyber and cyber-physical functional

dependencies to support cascade modeling and vulnerability severity assessment (Y. Jiang et al., 2023).

The evolution of smart cities and the Industrial Internet of Things (IIoT) has brought significant advancements in critical infrastructure management but has also introduced complex security challenges. The IIoT, a rapidly evolving technology, is becoming a core component of smart cities, offering numerous opportunities for developing industrial applications such as smart grids, smart manufacturers, and smart transportation systems (Abosata et al., 2021). However, the increased connectivity and intelligence of these systems also provide a rich attack surface for adversaries, making them vulnerable to various security threats (N. Mishra et al., 2024). Although IIoT provides substantial benefits, its wider implementation poses greater security risks than its advantages (Abosata et al., 2021).

This contradiction highlights the need for robust security measures in smart-city infrastructures. For instance, the industrial control systems (ICS) that form the backbone of smart cities are hackable and difficult to secure from cyberattacks, leaving future smart cities in a state of perpetual uncertainty. Moreover, the highly technical nature of the tools and techniques required to assess these risks complicates the situation, especially for local governments that have largely been absent from conversations about the cybersecurity of critical infrastructure (Falco et al., 2018). As smart cities and (Industrial Internet of Things) IIoT continue to evolve, it is crucial to prioritize the development and implementation of robust security measures to protect critical infrastructure from potential cyber threats.

The increasing usage of the Internet has led to a rise in cyber threats, affecting not only individual users and corporations but also national security. This has prompted nations to develop comprehensive cybersecurity policies to adopt a proactive approach against various types of cyber threats. Governments and international bodies are increasingly focusing on

developing policies and regulations to enhance cybersecurity and protect against cyberthreats. These policies aim to establish frameworks for cooperation, responses, and resilience. A study of seven nations identified 14 common cybersecurity attributes, including telecommunications, network security, cloud computing, online banking, e-commerce, and privacy. The focus on specific cybersecurity attributes varies by country. For instance, the USA scored highest in online banking policy, while Canada excelled in e-commerce and spam policies (A. Mishra et al., 2022).

This variation in focus highlights the need for a more coordinated approach to cybersecurity governance across nations. While governments are making efforts to enhance cybersecurity through policies and regulations, challenges remain. The fast-changing geography of the Internet demands a transnationally coherent and coordinated governance approach (Calderaro & Craig, 2020). Moreover, the study suggests that a country's science and technical knowledge is the most robust explanation for its cyber capacity level, emphasizing the need for policymakers to support countries in the Global South by strengthening education and technical skills beyond national security paradigms (Calderaro & Craig, 2020).

As cybersecurity continues to evolve, it is crucial for governments and international bodies to adapt their policies and regulations to effectively address emerging threats. Nye also highlighted the importance of international cooperation in addressing cybersecurity threats. He contends that effective cybersecurity requires collaborative efforts across borders, involving states, international organizations, and private entities (J. S. Nye, 2017 p.68).

3.2.5 Data Privacy

Data privacy concerns in cyberspace have become increasingly prominent because of the vast amounts of personal information collected and processed by digital firms. These concerns have led to various regulatory and technological responses aimed at protecting

consumer information. Governments worldwide have implemented data localization measures to address privacy, national security, and cyberterrorism concerns (Potluri et al., 2020).These measures range from allowing the free flow of data to imposing stringent restrictions on data storage within territorial jurisdictions. While such restrictions aim to protect personal data, they can have significant economic consequences, potentially limiting consumer choices and affecting the quality and price of services (Potluri et al., 2020).

Some economists and privacy advocates have proposed granting individuals' property rights to their personal data as a means of promoting information privacy. However, this approach may not be entirely effective because of the free alienability of property rights, which could potentially undermine privacy goals. Instead, adapting concepts from trade secrecy law and imposing minimum standards of commercial morality on firms that process personal data might be more beneficial (Samuelson, 2000). Addressing data privacy concerns requires a multifaceted approach. Enhancing individuals' mobile information protection behaviors (Belanger & Crossler, 2019) and improving online privacy literacy (Prince et al., 2023) are crucial steps in safeguarding privacy in cyberspace. Balancing the need for data protection with the benefits of digital services remains a complex challenge that requires ongoing research and policy development.

Zuboff highlights the risks associated with the collection and misuse of personal data by corporations and governments. She contends that "The pervasive collection of personal data creates vulnerabilities that can be exploited by malicious actors, compromising individual privacy and security" (Zuboff, 2019, p. 123). Zuboff's concept of "surveillance capitalism" highlights the risks associated with corporate and governmental collection and misuse of personal data. This model is characterized by a logic of accumulation based on networked captures of life, enabling complex processes of extraction, commodification, and control. The

key concern is that data representations open up opportunities for enhanced market control of life through algorithmic monitoring, prediction, and modification of human behavior. While Zuboff focuses on corporate data extraction, some researchers have proposed personal data markets as a solution.

However, this approach is critiqued on two grounds: it fails economically to address exploitation, and it ideologically reduces the critique of surveillance capitalism to consumer exploitation, concealing the broader aim of data capitalists to create worlds that generate audiences (Charitsis et al. 2018). The risks of data collection and misuse extend beyond privacy concerns to include broader social and political implications. The concept of "data pollution" offers a novel perspective, arguing that the central problem in the digital economy is how information provided by individuals affects others and undermines public goods and interests (Ben-Shahar, 2019). This framework suggests the need for new regulatory approaches, akin to environmental law, to address the external effects of data use and misuse in an increasingly digitalized world. Cyberspace introduces a range of security concerns that necessitate robust and adaptive measures to protect individuals, organizations, and nations. Addressing these challenges necessitates a multifaceted approach that combines innovative technologies, regulatory frameworks, and global collaboration.

3.3 Structure of Cyberspace

The physical infrastructure of cyberspace includes hardware and physical devices that support digital communication and data exchange. This infrastructure forms the backbone of cyberspace and is essential for its functioning, encompassing a wide range of hardware and devices that enable digital communication and data exchange in cyber-physical systems (CPS). They include sensors, actuators, communication networks, and computing devices that form the backbone of modern CPS architectures (Mois et al., 2016). In smart grids, for instance, the physical infrastructure comprises power system components integrated with Internet-of-Things

(IoT)-based digital communication networks. This integration allows real-time monitoring, control, and data exchange, thereby enhancing grid stability, sustainability, and reliability (Habib et al., 2023).

Similarly, in manufacturing environments, sensor-packed systems and equipment provide event and status information, forming the physical layer of cyber-physical production systems (CPPS) (Babiceanu & Seker, 2016). Recent advancements have led to the development of wirelessly powered and battery-free wireless sensors for CPS applications in harsh environments. These sensors, powered by radiofrequency sources, can collect and transmit data without the need for batteries, thereby demonstrating the evolving nature of physical infrastructure in cyberspace (Loubet et al., 2019).

Moreover, the potential use of satellite Internet constellations, such as Starlink, to enhance communication in cyber-physical power systems demonstrates the expanding scope of physical infrastructure in cyberspace (Duan & Dinavahi, 2021). The physical infrastructure of cyberspace is a complex and evolving ecosystem that includes diverse hardware and devices. From sensors and actuators to communication networks and computing systems, this infrastructure forms the foundation for digital communication and data exchange in modern cyber-physical systems across various domains, including smart grids, manufacturing, and structural health monitoring.

3.3.1 Software and Applications

Software and applications play crucial roles in cyberspace infrastructure, forming the backbone of digital interactions and services across various domains. The exponential growth of the Internet has led to a significant increase in cyber-attack incidents, with malware being the primary weapon of choice. This highlights the importance of robust software applications in maintaining cybersecurity. The development of innovative and effective malware defense

mechanisms is considered an urgent requirement in the cybersecurity community, emphasizing the critical role of secure software in protecting cyberspace infrastructure (Jang-Jaccard and Nepal, 2014).

Although software and applications are essential for cyberspace functionality, they can also be potential vulnerabilities. For instance, the additive manufacturing process chain heavily relies on cloud-based resources and software programs connected to the Internet, making cybersecurity a major concern (F. Chen et al., 2017). This dual nature of software, as both a critical component and a potential weakness, underscores its significance in the cyberspace ecosystem. Software and applications are integral to cyberspace infrastructure, enabling various services and functionalities. From mobile social networking platforms process vast amounts of data (Y. Zhang et al., 2018) to healthcare operational information systems requiring robust cybersecurity measures (Coutinho et al., 2023), software forms the foundation of our digital world. As cyberspace continues to evolve, developing secure and efficient software remains paramount to ensuring the integrity and functionality of the global network computing infrastructure.

3.4 Cyber Threats and Vulnerabilities

Cyberspace is rife with threats and vulnerabilities that can compromise the security and integrity of information systems. These threats range from cyberattacks conducted by state and non-state actors to inherent vulnerabilities in software and hardware systems.

3.4.1 Malware

Malware, or malicious software, is designed to infiltrate and damage computer systems without the user's consent. Malware remains a significant threat to cybersecurity, exploiting vulnerabilities in hardware, software, and network layers to carry out malicious activities in cyberspace (Jang-Jaccard & Nepal, 2014). The impact of malware on cybersecurity is multifaceted and far-reaching, affecting organizations, critical infrastructure, and individual

users. In the healthcare sector, for instance, the increasing use of smart medical equipment and mobile devices has made organizations more susceptible to ransomware and other types of malware (Abraham et al., 2019). This vulnerability is exacerbated by the complexity of operations and the presence of numerous legacy and incompatible systems, making it challenging to implement effective cyber security measures.

The development of malware and cybersecurity measures has evolved into an arms race. While machine learning algorithms have proven effective in detecting threats, particularly in PDF files, adversarial attacks have emerged to challenge these systems (Maiorca et al., 2020). This ongoing battle highlights the need for continuous innovation in malware defense mechanisms and the importance of robust and adaptive cybersecurity solutions. Malware significantly impacts cybersecurity by exploiting vulnerabilities, challenging detection systems, and threatening critical infrastructure security. To address these challenges, organizations must adopt a proactive approach to cybersecurity risk management, including regular employee training (He et al., 2019), the development of innovative defense mechanisms (Jang-Jaccard & Nepal, 2014), and the implementation of comprehensive cybersecurity solutions that can detect and respond to attacks in real time.

Ransomware is a type of malware that encrypts a victim's files and demands payment for the decryption key. Ransomware has emerged as a major global cybersecurity threat, causing significant disruptions and financial losses across various sectors, particularly in healthcare. In 2017, a piece of ransomware took the world by storm and demonstrated the true havoc that a cyberattack could wreak on society. Ukraine was again the target of a cyber-attack, and a ransomware worm named Not Petya spread across 10 percent of all computers in Ukraine. Transportation hubs, banks, government agencies, media outlets, and utility companies were all paralyzed. Not Petya then crossed borders, affecting Russia, the U.S., and France, shutting

down oil companies, hospitals, pharmaceutical, and food production companies. In Copenhagen, it pushed the world's largest shipping firm, Moller-Maersk, offline. The assessment of the loss was $ 10 billion (Greenberg, 2018). These cyber-attacks exploit the connectivity of our modern lives, which can shut down our ports and airports, expose corporate and military secrets, and bring society to its knees. Malicious malware continues to reinvent itself, as do cyberattacks, which is why every cyber-attack is different.

The WannaCry attack in 2017 affected over 150 countries, crippling parts of the UK's National Health Service and highlighting the vulnerability of healthcare systems to cyber-attacks (G. Martin et al., 2017). This incident exposed the poor state of cybersecurity in healthcare and emphasized the need to recognize it as a fundamental issue of patient safety. Although ransomware attacks have become increasingly sophisticated, they often still rely on human factors for initial intrusion. Many attacks are initiated through phishing emails, demonstrating the complex interplay between technical vulnerabilities and social engineering tactics (Y. Connolly & Wall, 2019). This complexity necessitates a multilayered approach to cybersecurity, combining technical measures with human-focused strategies, such as training and awareness programs.

In response to this growing threat, researchers and cybersecurity experts have developed new approaches to detect, classify, and mitigate ransomware attacks. These include the use of machine learning techniques, network function virtualization, and software-defined networking (Fernández Maimó et al. 2019). Moreover, frameworks such as the Ransomware Risk Management Model (R2M2) have been proposed to help organizations assess and mitigate ransomware risks (Mukhopadhyay & Jain, 2024). As ransomware continues to evolve, ongoing research and development of robust cybersecurity measures are crucial to protect critical infrastructure and sensitive data worldwide.

3.4.2 Phishing and Social Engineering

Phishing involves tricking individuals into revealing sensitive information, such as passwords and credit card numbers, by masquerading as trustworthy entities in electronic communications. Attackers often use emails that appear to be from legitimate sources to lure victims into providing confidential information. These attacks can lead to significant financial losses and data breaches. Phishing is a significant global cybersecurity threat that affects individuals, organizations, and entire industries. Studies have shown that phishing attacks are common in everyday life and pose a major risk to cybersecurity worldwide. However, curated training in cybersecurity reduces the likelihood of employees opening phishing emails by approximately 70%, which shows the centrality of the human element in cybersecurity (Daengsi et al., 2022).

The impact of phishing on cybersecurity is substantial and extensive. In healthcare, for instance, almost 1 in 7 simulated phishing emails were clicked on by employees, representing a major cybersecurity risk for hospitals (Gordon et al., 2019). The COVID-19 pandemic transformed the cybercrime threat landscape, with phishing being a key component of cybercriminal activities that significantly impacted the GDP of targeted countries (Djenna et al., 2023). The effectiveness of phishing attacks can vary based on factors such as age, gender, and the content of the email. For example, older women showed the highest susceptibility to phishing, and the relative effectiveness of attacks differed by weapons of influence and life domains with age group variability (T. Lin et al., 2019). Interestingly, in the Thai cybersecurity ecosystem, female employees were found to have a higher level of cybersecurity awareness than their male coworkers (Daengsi et al., 2021).

Various approaches have been developed and tested to combat the global threat of phishing. These include employee education and awareness programs, simulated phishing campaigns, and advanced-detection frameworks. For instance, a study involving over 10,000

employees found that both information provision and simulated experience substantially reduced the proportion of employees who fell for phishing attacks (Baillon et al., 2019). Phishing remains a critical global cybersecurity challenge that affects various sectors and demographics differently. Ongoing research and development of multifaceted approaches, including technical solutions, employee training, and legal frameworks, are essential to mitigate the risks posed by phishing attacks and enhance overall cybersecurity worldwide.

3.4.3 Distributed Denial of Service (DDoS) Attacks

DDoS attacks involve overwhelming a network, service, or website with a flood of Internet traffic, rendering it unavailable to users. These attacks can disrupt services and cause significant economic harm. DDoS attacks have become a significant global cybersecurity threat, causing substantial financial losses and service disruptions in various sectors. These attacks exploit thousands of compromised machines to overwhelm data services and online platforms, resulting in system failure and downtime (Talpur et al., 2024). The impact is particularly severe in the industry 4.0 era, where business continuity is crucial, leading to billions of dollars in financial losses and irreparable reputational damage.

The COVID-19 pandemic has exacerbated this situation by exposing vulnerabilities in traditional perimeter-based security measures. Attackers have diversified their targets, focusing on health services, e-commerce, and education services (De Neira et al., 2023). Moreover, the integration of IoT devices into critical infrastructure, such as Energy Hubs, has introduced new vulnerabilities to DDoS attacks, highlighting the need for advanced detection and prevention methods (Sakr et al., 2024). The global impact of DDoS attacks necessitates the development of sophisticated defense strategies to mitigate their effects. Recent research has focused on leveraging artificial intelligence and machine learning techniques to enhance the detection and prevention capabilities (Cil et al., 2021).

Additionally, cooperative defense systems, such as the Blockchain Signaling System (BloSS), offer promising solutions by combining detection and mitigation capabilities across distributed networks (Rodrigues et al., 2020). These advancements are crucial for improving business sustainability and protecting critical infrastructure in an increasingly interconnected and digital landscape.

3.4.4 Advanced Persistent Threats (APTs)

Advanced Persistent Threats (APTs) are prolonged and targeted cyberattacks in which an intruder gains access to a network and remains undetected for an extended period. These attacks are often conducted by state-sponsored groups. APTs significantly impact cybersecurity by presenting sophisticated, stealthy, and long-term challenges to organizations and critical infrastructure systems. APTs employ complex tactics to infiltrate systems, often remaining undetected for extended periods and causing substantial damage. These attacks are highly tailored and targeted and mostly evade defenses. These threats are designed to steal intellectual property, compromise sensitive data, and potentially sabotage critical systems, making them a major concern for cybersecurity professionals (Friedberg et al., 2015).

APTs differ from traditional malware in terms of their techniques and tactics. A study involving over 16,000 malware samples revealed that APT-linked malware could be statistically differentiated from regular malware (González-Manzano et al., 2023). This suggests that APTs require specialized detection and mitigation strategies that are distinct from those used for conventional cyber threats. APTs pose a significant challenge to cybersecurity because of their persistence, sophistication, and ability to evade traditional security measures.

To combat these threats effectively, organizations need to adopt proactive, dynamic defense strategies that can adapt to the evolving nature of APTs (L. Huang & Zhu, 2020). This may include leveraging advanced technologies, such as machine learning for anomaly

detection (Berrada et al., 2020), and implementing security-aware defense mechanisms (Y. Li et al., 2019), and utilizing knowledge graph-based approaches for threat intelligence and attribution (Ren et al., 2022).

3.4.5 Zero-Day Vulnerabilities

Zero-day vulnerabilities are flaws in software that are unknown to vendors. Because they are undisclosed, these vulnerabilities can be exploited by attackers before developers have a chance to issue patches. Zero-day exploits are highly sought after in the cybercriminal underworld because of their potential to bypass traditional security measures. Zero-day vulnerabilities significantly impact cybersecurity by presenting unique challenges and risks to organizations and individuals. These unknown software flaws provide attackers with powerful means to carry out cyber intrusions, often leaving systems defenseless against exploitation (Leal & Musgrave, 2023).

The unpredictable nature of zero-day vulnerabilities makes them particularly difficult to measure and address. Traditional security metrics struggle to account for these unknown threats because a seemingly secure configuration may still be susceptible to zero-day attacks. To address this issue, the concept of "k-zero day safety" has been proposed, which quantifies the number of unknown vulnerabilities required to compromise network assets, providing a more robust security metric (L. Wang et al., 2014).

The rapid evolution of cyber threats has led to increased collective action among security researchers to reduce the time required to characterize and address emerging threats. Platforms such as the Malware Information Sharing Platform (MISP) enable collaborative efforts to quickly complete threat descriptions, potentially mitigating the impact of zero-day vulnerabilities (Gillard et al., 2023). Moreover, the development of proactive cyber threat

intelligence (CTI) using data from the Dark Web can help organizations prioritize vulnerabilities and manage risks associated with zero-day exploits (Samtani et al., 2022).

Zero-day vulnerabilities pose significant challenges to cybersecurity, requiring innovative approaches for their detection, measurement, and mitigation. The development of new security metrics, collaborative platforms, and proactive threat intelligence strategies is crucial for addressing the risks associated with these unknown vulnerabilities. Organizations must remain vigilant and adapt their security practices to effectively combat the ever-evolving zero-day threat landscape.

3.4.6 Insider Threats

Insider threats pose a significant and growing challenge to cybersecurity in various organizations. These threats, originating from individuals with privileged access to an organization's assets, can cause serious direct (financial) and indirect (reputational) consequences (Moneva & Leukfeldt, 2023).The impact of insider threats on cybersecurity is multifaceted and can be considerable, even if the probability of information leakage is small (Z. Liu & Wang, 2021). Insider threats are particularly dangerous because insiders often have more knowledge about the target system than external attackers, making them more effective at defeating security controls primarily designed to defend against external attacks (D. Liu et al., 2008).

This unique position allows insiders to compromise the proper functioning of systems and potentially cause severe damage. For instance, in power systems, insider threats can lead to load redistribution attacks, increasing the attacker's payoff and potentially causing significant harm to the grid (Liu & Wang, 2020). Although insider threats are a major concern, they have received less attention than outsider attacks in cybersecurity research (Alslaiman et

al., 2022). This discrepancy highlights the need for more focused efforts to address insider threats.

Additionally, it's worth noting that insider threats are not always malicious; they can also be negligent but still pose significant risks to an organization's cybersecurity (Moneva & Leukfeldt, 2023). Insider threats represent a complex and persistent challenge in cybersecurity. A multifaceted approach to mitigation is required, including technical measures, employee training, and fostering a culture of cybersecurity awareness (Le et al., 2024). As the cybersecurity landscape continues to evolve, addressing insider threats remains a critical aspect of maintaining robust information security practices.

3.4.7 Vulnerabilities in IoT Devices

The proliferation of Internet of Things (IoT) devices has introduced numerous vulnerabilities that significantly impact the security landscape of interconnected systems. With an estimated 14.4 billion active endpoints in 2022 and a projected 30 billion connected devices by 2027 (Canavese et al., 2024), the rapid expansion of the IoT has created a vast attack surface for cybercriminals to exploit. These devices often suffer from intrinsic security vulnerabilities, limited computing power, and a lack of timely security updates, making them attractive targets for malicious actors to exploit. Although IoT technology promises significant societal benefits, it has also become a double-edged sword. The extensive scale of IoT networks has introduced security challenges, including vulnerabilities, cyberattacks, and a lack of standardized protocols (Merlino & Allegra, 2024).

The proliferation of IoT devices has created a complex security landscape, with vulnerabilities ranging from device-level weaknesses to broader infrastructure concerns. The rapid adoption of IoT systems without thorough consideration of risks and vulnerabilities has the potential to cause catastrophic damage to the privacy, safety, and security of individuals

and corporations (X. Liu et al., 2019). To address these challenges, a multifaceted approach involving improved security measures, regulatory frameworks, and ongoing research into emerging threats is essential for creating a more resilient IoT ecosystem.

3.5 Resilience and Defense in Cyberspace

Resilience and defense in cyberspace are critical for safeguarding digital infrastructure and ensuring the continuity of services amid various cyber threats. Effective strategies encompass a blend of technological measures, policy frameworks and organizational practices.

3.5.1 Cyber Resilience

Cyber resilience refers to an organization's ability to prepare for, respond to, and recover from cyberattacks. It emphasizes not only defense against cyber threats but also the capacity to maintain operational continuity under adverse conditions. Cyber resilience offers a comprehensive approach to improving cybersecurity by enhancing an organization's capacity to withstand, recover from, and adapt to cyber threats (Dupont, 2019). Unlike traditional cybersecurity measures that focus primarily on prevention and protection, cyber resilience acknowledges the inevitability of cyberattacks and emphasizes the ability to maintain operations under challenging circumstances.

The concept of cyber resilience encompasses several key dimensions, including being dynamic, networked, practiced, adaptive, and contested (Dupont, 2019). It involves implementing a framework that includes a knowledge base of potential threats, detection models, and visualization dashboards to monitor and respond to cyber risks effectively (Saeed et al., 2023). This approach enables organizations to prepare for adverse events and continue operating even when they are faced with sophisticated attacks.

Cyber resilience is particularly crucial for small and medium-sized enterprises (SMEs), which often have limited resources but represent a significant target for cybercriminals (Carias

et al., 2020). The implementation of cyber-resilience practices can help SMEs anticipate, detect, withstand, recover from, and evolve after cyber incidents, providing a more holistic approach to cybersecurity. Cyber resilience complements traditional cybersecurity measures by focusing on an organization's ability to maintain functionality and adapt to evolving threats. This emphasizes the importance of preparedness, response capabilities, and continuous improvement in the face of cyber risks. By adopting a cyber-resilience approach, organizations can enhance their overall security posture and better protect their critical assets and operations in an increasingly complex threat landscape (Dupont, 2019; Zhao et al., 2024).

3.5.2 Defense Mechanisms

Effective cyber defense mechanisms include a range of technologies and practices designed to protect information systems from unauthorized access, use, disclosure, disruption, modification, and destruction.

Intrusion Detection and Prevention Systems (IDPS)

Intrusion detection and prevention systems (IDPS) play a crucial role in improving cybersecurity by detecting and preventing unauthorized activities on digital networks. These systems enable organizations to protect their networks and data from complex security threats. An IDPS utilizes various machine learning techniques to recognize network attacks and defend against cyber security threats. By developing efficient intrusion detection systems, organizations can identify anomalies in computer servers and improve overall cybersecurity (Omer et al., 2023).

These systems can detect both known and novel intrusions through misuse, anomaly, and hybrid detection approaches, enhancing the overall security posture (Jiong Zhang et al., 2008). An IDPS provides multiple layers of defense, giving defenders precious time before unrecoverable consequences occur in physical systems. By utilizing network traffic data, host

system data, and measured process parameters, these systems offer a comprehensive approach to cyber-attack detection (F. Zhang et al., 2019).

Additionally, IDPS can be integrated with other security measures, such as firewalls and data diodes, to create a defense-in-depth strategy. The effectiveness of IDPS is further enhanced by leveraging advanced technologies such as Big Data analytics, data fusion, and Security Information and Event Management (SIEM) systems. These approaches enable the correlation of security events from heterogeneous sources, providing a more holistic view and greater situational awareness of cyber threats (Zuech et al., 2015).

IDPS significantly improves cybersecurity by providing real-time monitoring, early detection of threats, and automated response capabilities. By incorporating advanced technologies and machine learning techniques, these systems offer a robust defense against evolving cyber threats, enabling organizations to maintain a strong security posture in an increasingly interconnected digital landscape.

Firewalls and Antivirus Software

Firewalls and antivirus software play crucial roles in improving cybersecurity by providing essential layers of protection against various cyber threats. Firewalls act as the first line of defense, monitoring and controlling incoming and outgoing network traffic based on pre-determined security rules. They help prevent unauthorized access and protect against network-based attacks, such as Distributed Denial of Service (DDoS) (Salah et al., 2012). In contrast, antivirus software focuses on detecting, preventing, and removing malicious software from computer systems (Cain et al., 2018).

In the interview Dr. Baqir Malik asserted that firewalls in the digital world are a lose equivalent of borders in the physical world. Although these cannot entirely stop the flow of data but slow down the transmission speed and deny access for some time. Although these

traditional cybersecurity approaches are widely used, they may not be sufficient to address the evolving and sophisticated cyber threats in today's interconnected world. For instance, in industrial control systems and smart grids, relying solely on firewalls and antivirus tools may not ensure security across all dimensions of the information assurance model (Saleem et al., 2020).

Additionally, the effectiveness of these tools can be limited by user behavior, as end users' cyber hygiene often plays a significant role in cybersecurity breaches (Cain et al., 2018). Although firewalls and antivirus software are essential components of a cybersecurity strategy, a more comprehensive approach is necessary. This may include implementing diverse security mechanisms, adopting advanced technologies such as reinforcement learning (Oh et al., 2023), and addressing economic challenges such as misaligned incentives and information asymmetries (T. Moore, 2010). Furthermore, improving users' cyber hygiene knowledge and practices and implementing multilayered defense strategies can significantly enhance the overall cybersecurity posture.

3.6 Incident Response and Recovery

An Incident response refers to the approach taken by an organization to manage and mitigate the effects of cyberattacks. Recovery focuses on restoring systems and data to their normal operations. Incident response and recovery play crucial roles in improving cybersecurity by enabling organizations to effectively manage and mitigate the impact of cyber threats. These processes help organizations detect, analyze, and contain security incidents, restore normal operations, and learn from the experience to enhance future preparedness. Effective incident response strategies are critical for successful recovery when organizations encounter cybersecurity incidents. Organizations must develop 'agility' in their incident response processes to respond swiftly and efficiently to sophisticated and potent cyber threats (Naseer et al., 2021).

Downtime due to cyberattacks costs organizations a lot in terms of their reputation, loss of business, and in cases where consumers' or clients' data is exposed, lawsuits always follow. Therefore, an agile incident response regime and plans for disaster recovery are necessary to ensure business continuity and reduce downtime. The implementation of dynamic models, such as the Cyber Resilience Recovery Model (CRRM), can help combat zero-day outbreaks and minimize disruptions to business operations (Tran et al., 2016).

Despite the push for appropriate legislation and guidance, operators of Industrial Control Systems (ICS) and Critical National Infrastructure (CNI) still face multiple challenges in their cyber incident response and recovery capabilities (Staves et al., 2022). This highlights the need for continuous improvement and adaptation of incident-response strategies across various sectors. Incident response and recovery contribute to improved cybersecurity by enabling organizations to develop dynamic capabilities, leverage real-time analytics and implement robust frameworks. These approaches help organizations to detect cybersecurity incidents quickly, respond proactively, and adapt to evolving threats. By investing in in-house cybersecurity human resources, enhancing employee training, and developing agile response strategies, organizations can significantly improve their overall cybersecurity posture and resilience to potential attacks (Buil-Gil et al., 2021).

3.7 Cybersecurity Frameworks and Standards

Adopting cybersecurity frameworks and standards helps organizations implement best practices and improve their defense and resilience. These frameworks provide structured approaches for organizations to assess and enhance their cyber security posture. For instance, the National Institute of Standards and Technology (NIST) Cybersecurity Framework offers guidelines, best practices, and standards for managing cybersecurity risks. It helps organizations identify, protect, detect, respond, and recover from cyber threats, thereby providing a comprehensive approach to cybersecurity (Armenia et al., 2021).

Similarly, the Industrial Automation and Control Systems (IACS) framework and NIST framework for AIS cybersecurity in the shipping industry offer a structure for constructive decision-making and high-level cybersecurity (Soner et al., 2024). These frameworks often address multiple dimensions of cybersecurity, extending beyond traditional methods. For example, the multidimensional holistic framework proposed by (Saleem et al., 2020) incorporates advanced technologies, intelligent algorithms, and continuous assessments to address gaps in traditional cybersecurity approaches. This layered defense model can be integrated into utility networks to evaluate the security and resilience of microgrid control systems.

Although frameworks provide valuable guidance, they may have limitations. (Armenia et al., 2021) noted that self-assessment frameworks, such as NIST can produce a static view of an organization's cyber posture and may not capture the dynamics of organizational changes and cyberattacks. To address this issue, a robust cybersecurity audit and compliance system is necessary. Cybersecurity frameworks and standards serve as essential tools for organizations to implement best practices and improve their defense and resilience. They provide structured approaches, address multiple dimensions of cybersecurity, and offer guidance for decision making. However, organizations should also consider dynamic assessment methods to complement these frameworks and ensure a more comprehensive and adaptive approach to cyber security.

CHAPTER-4

4. Cyberspace and Realism

In international relations, realism is a prominent theoretical framework that emphasizes the chaotic nature of global interactions, in which nations primarily pursue power and security. Realism provides a framework for understanding international relations by focusing on the role of the state, the importance of power, and the impact of anarchy. Its emphasis on security, national interest, and inherent conflict in the international system continues to influence the study and practice of international politics. Some important mainstays of the realist theory are as follows

4.1 State-Centrism

Realism views states as the primary actors in international relations. States are sovereign entities with ultimate authority within their territories and act independently to pursue their national interests (Donnelly, 2000). The realist paradigm emphasizes the primacy of the sovereign state system and its autonomy from domestic political, social, and moral considerations, focusing on the vertical division of the world into sovereign states rather than the horizontal forces that transcend state boundaries (Neumann & Welsh, 1991).

Neoclassical realism, a prominent variant of realist theory, argues that a state's relative material power is the primary driver of its foreign policy and ambition. However, it also recognizes that systemic pressures are translated through intervening unit-level variables such as decision-makers' perceptions and state structure, highlighting the importance of both international and domestic contexts in foreign policy formulation (Rose, 1998).

Some scholars have attempted to bridge the gap between domestic and international politics within a realist framework. They propose models that relate state officials' goals in one arena to the strategies available in the other, acknowledging the interdependence between the

domestic and international spheres while maintaining the state as the central actor (Mastanduno et al., 1989). This approach demonstrates the evolving nature of realist theory while preserving its state-centric focus.

However, realist theory's state-centrism is evident in its emphasis on sovereign states as the primary actors in international relations, its focus on material power and state interests, and its analysis of how states navigate both domestic and international pressures. While some variations of realism incorporate additional factors, the state remains the fundamental unit of analysis for understanding world politics from a realist perspective.

4.2 Anarchy

Realists believe that the international system is characterized by anarchy, meaning that there is no overarching authority above the states. This absence of a central authority leads to a self-help system in which states must rely on their resources to ensure their survival. They argue that the international system lacks a central authority to enforce rules and maintain order, leading to a state of anarchy (Kono, 2007). This absence of hierarchy means that states must rely on self-help strategies to ensure their survival and security. The anarchic nature of the system is seen as a fundamental, invariant structural feature that shapes state behavior (Goldgeier & McFaul, 1992).

Realists base their understanding of anarchy on Hobbesian assumptions about human nature, viewing individuals and states as naturally self-interested and potentially aggressive entities. This perspective justifies the state’s internal monopoly on violence and the external competitive state-centric system. However, some scholars challenge this view, pointing to examples of cooperation and non-violent political action in the global civil society (Turner, 1998).

While realism emphasizes anarchy, other approaches offer alternative perspectives on the same. Institutionalists argue that international institutions can mitigate the effects of anarchy by facilitating cooperation and raising reputational costs for non-compliance (Kono, 2007). Constructivists focus on how shared rules and norms in international society can condition state behavior beyond what material power structures would predict (Copeland, 2003). These competing views highlight the ongoing debate on the nature and consequences of anarchy in the international system.

4.3 Power and Security

Realists argue that states' primary goal is to ensure their security through the accumulation of power. Power is typically understood in terms of military capability, economic strength, and political influence. They argue that states prioritize their security and survival in an anarchic international system by accumulating power through military capabilities, economic strength and political influence (Montgomery, 2006; Ross, 2006). This view assumes that states operate in an environment of uncertainty about others' motives and intentions, leading them to focus on self-help strategies (Parent & Rosato, 2015).

However, there are some interesting nuances and contradictions within realist theories. While offensive realists maintain that states cannot overcome this uncertainty, defensive realists argue that states can reveal their benign intentions through military reassurance, although this often increases their vulnerability (Montgomery, 2006). Additionally, some realists emphasize that states may define their interests more broadly than immediate security concerns, pursuing major-power foreign policies driven by potential power, international threats, or expanding economic interests (Fordham 2011).

While realists generally agree on the importance of power accumulation for state security, there are ongoing debates regarding the specific mechanisms and motivations behind

state behavior. Recent scholarship has attempted to integrate various aspects of realist thinking by combining structural variables with security dilemma considerations (Christensen, 1997). This evolving understanding of realism highlights the complexity of state motivations and behaviors in the international system, moving beyond simplistic notions of power accumulation to consider factors such as targeted balancing in shaping state strategies for survival and security (Lobell, 2018).

4.4 National Interest

The realist paradigm places a strong emphasis on national interest as the primary driver of state behavior in the international system. States act in pursuit of their national interests, which are often defined in terms of security and survival. This focus on national interest leads states to prioritize their own needs over those of other states or international institutions (Donnelly, 2000a). This strong emphasis on national interests stems from the core assumptions of realism regarding the nature of international politics.

Realists argue that states pursue their vital interests in a dangerous world that constrains their behavior, and the pursuit of national interest through Realpolitik is considered central to realist theory, with states either engaging in such behavior or being highly incentivized to do so by the structure of the international system (Rathbun, 2018). This perspective views power politics as the primary dynamic in international relations theory. The focus on national interest and power politics remains a defining feature of realism, even as the theory continues to evolve and faces challenges from alternative approaches in international relations.

4.5 Balance of Power

Realists believe that international stability is maintained through the balance of power. When power is distributed relatively equally among states, the risk of major conflict is reduced. States continuously adjust their alliances and military capabilities to maintain this balance

(Guzzini, 2004). Classical and neorealists argue that the distribution of power in the international system, particularly among great powers, is crucial for stability (Nexon, 2009; Zagare, 1996). They contend that states seek to balance potential hegemons to prevent any single state from becoming too powerful. However, there are disagreements among realists about how this balancing occurs and whether it always leads to stability. Some argue that secondary states may choose to accommodate rather than balance against rising powers, depending on local variations in their capabilities (Ross, 2006).

There is a debate between realists and institutionalists regarding whether international institutions can independently affect state behavior and promote peace. Realists maintain that institutions merely reflect the balance of power and state interests, while institutionalists argue that institutions can cause peace by convincing states to reject power-maximizing behavior (Mearsheimer, 1995). Additionally, some scholars challenge the notion that balance of power equilibria represent the "normal condition" or "natural tendency" of international relations (Nexon, 2009).

Realists generally agree on the importance of power distribution for international stability but disagree on the specific mechanisms of balancing, the role of institutions, and whether the balance of power theory adequately explains historical patterns of international relations. Some scholars suggest that a more nuanced approach to power-political competition may be necessary, treating "balancing" and "balance of power" as objects of inquiry rather than solely as realist theoretical constructs (Nexon, 2009; B. C. Schmidt, 2005).

4.6 Rational Actor Model

Realism assumes that states are rational actors that make decisions based on a calculated assessment of their interests and the potential costs and benefits of different courses of action (Smith, 2018). While realism posits that states behave rationally to maximize their self-interest

and power, some scholars argue that this view oversimplifies the complex decision-making processes within states. There are contradictions and nuances in the conceptualization and application of rationality in realist theory. Schmidt and Wight highlight the confusion arising from failing to distinguish between rationalism as an epistemological position and rationality as an ontological assumption about state behavior (B. C. Schmidt & Wight, 2023). Moreover, Mowle contends that systemic and situational factors, rather than purely rational calculations, often influence how states represent and respond to international conflicts (Mowle, 2003).

While realism assumes state rationality, decision-making is more complex. As (Nilsson & Dalkmann, 2001) argue, strategic decision-making processes are often characterized by bounded rationality rather than perfect rationality. Similarly, (Cabantous et al., 2010) reveal the intricate socio-technical infrastructure and practices underlying rational decision-making in organizations. These findings suggest that the realist assumption of state rationality may be an oversimplification, and a more nuanced understanding of decision-making processes in international relations is required.

4.7 Survival

According to realist thought, the primary concern of states is survival. Because the international system is anarchic and competitive, states must prioritize their security and survival above all else (Wohlforth, 2011). Realism in international relations theory posits that states' primary concern is survival in an anarchic and competitive international system. This view is rooted in the assumption that the absence of a central authority to enforce rules and maintain order leads states to prioritize security and power.

According to realists, the anarchic nature of the international system compels states to adopt self-help strategies for survival. This often manifests in balancing behaviors, such as

arms races and alliance formations, as states seek to maintain or enhance their relative power positions (Goldgeier & McFaul, 1992; Waltz, 2000).

However, some scholars argue that this perspective is overly simplistic. For instance, (Oelsner, 2007) suggests that some regions have overcome the security dilemma and constructed peaceful relationships based on mutual trust, resembling friendship at the interstate level. Although the realist paradigm remains influential, alternative perspectives challenge its core assumptions. For example, (Kono, 2007) argues that international institutions can promote cooperation by facilitating reciprocal strategies and raising the reputational costs of non-compliance, even within an anarchic system.

Additionally, (J. M. Hobson & Sharman, 2005) contends that hierarchical sub-systems have been common since 1648, suggesting that the international system is characterized by both anarchic and hierarchical relations. These perspectives indicate that while survival remains a crucial concern for states, the means and strategies for achieving it may be more diverse and complex than traditional realist theories suggest.

4.8 Relative Gains

Realists emphasize relative over absolute gains. In interactions with other states, what matters most is not just the benefits a state receives but how those benefits compare with what others receive. This focus on relative gains often leads to zero-sum thinking in international relations (Mowle, 2003b). They argue that states prioritize relative gains over absolute gains in international cooperation, emphasizing concerns about how well they perform compared to other states rather than their individual progress (Snidal, 1991). This perspective suggests that states are primarily focused on maintaining or improving their position relative to others, which can inhibit cooperation even when all parties would benefit in absolute terms.

However, several studies have challenged this view. (Snidal, 1991) demonstrates that as the number of states involved increases, relative gains become increasingly irrelevant to cooperation prospects. (Berejekian, 1997) introduced prospect theory, suggesting that states pursue absolute gains when in a gains frame and relative gains when in a losses frame, offering a more nuanced understanding of state behavior. (Snidal, 1991) further complicates the picture by showing that while relative gains do impede cooperation in two-actor scenarios, their significance diminishes with more competitors in the race.

While realists emphasize the importance of relative gains in international relations, empirical and theoretical studies suggest a more complex reality. The impact of relative gain concerns varies depending on factors such as the number of actors involved, the specific context of the interaction, and states' perceptions of their position (Berejekian, 1997; Powell, 1991; Snidal, 1991). This nuanced understanding challenges the strict realist perspective and calls for a more contextual approach to analyzing state behavior in international cooperation research.

4.9 Conflict and Competition

Realism posits that conflict and competition are inherent in international relations. The pursuit of power and security in an anarchic system inevitably leads to rivalries and conflicts among states (Donnelly, 2000b). This view stems from realism's core assumptions about state behavior and the anarchic nature of the international order (Legro & Moravcsik, 1999). Realists argue that states are primarily concerned with power and survival, which leads to an inherently competitive and conflictual environment (Cozette, 2004). However, this traditional realist perspective has faced challenges and criticisms.

Some scholars argue that realism can be seen as an ideology rather than a theory, manipulating intellectual history to maintain its dominance (Behr & Heath, 2009). Others have

proposed alternative frameworks, such as those based on Thomas Paine's international thought, which emphasizes democratic governance, trade, and human rights as factors promoting peace (Walker, 2000). While realism remains influential in international relations theory, its assumptions regarding inherent conflict and competition are increasingly scrutinized.

Recent research has explored the psychological micro-foundations of realist thinking (Kertzer & McGraw, 2012) and the conditions under which decision-makers adopt realist or liberal worldviews (Mowle, 2003a). These studies suggest that systemic and situational factors play a significant role in shaping state behavior, indicating that the realist perspective may not always accurately reflect the complexities of international relations.

4.10 Human Nature

Classical realism, particularly the work of Morgenthau, attributes the drive for power and competition to human nature, suggesting that the behavior of states reflects the selfish and power-seeking tendencies of individuals (Williams, 2004). Morgenthau's approach to international relations was heavily influenced by Max Weber's methodological writings (Turner & Mazur, 2009). He applied Weber's views to develop an ideal-typical model of the rational and responsible statesman, rather than simply attributing state behavior to selfish human tendencies. Moreover, Morgenthau's realism was not just an explanatory theory but also a critical project questioning the existing status quo (Cozette, 2008). This critical dimension is often overlooked in contemporary realism discussions. Interestingly, there are significant differences between Morgenthau and Weber's positions on political ethics.

While Morgenthau judged foreign policy in terms of its consequences for state power, Weber focused on its consequences for cultural values (Barkawi, 1998). This distinction highlights the complexity of Morgenthau's realist theory, which goes beyond simplistic notions of power-driven behavior. While classical realism considers power and competition as

important factors in international relations, Morgenthau's work is more sophisticated than often portrayed. His approach incorporates critical perspectives, ethical considerations, and a nuanced understanding of state behavior that cannot be reduced to mere reflections of individual selfishness. The mischaracterization of Morgenthau's views has led to ongoing debates about the nature of realism and its role in international relations theory (Behr & Heath, 2009; Williams, 2005).

4.11 New Realities of Cyberspace

The rise of cyberspace as a crucial arena for state engagement introduces novel complexities and prospects for realist interpretation. The advent of cyberspace as the fifth domain of warfare poses significant challenges to the realist theory of international relations (IR), which traditionally emphasizes state sovereignty, military power, and the anarchic nature of the international system.

Realism, with its focus on state-centric power dynamics and the pursuit of national interests, struggles to adequately account for the complexities introduced by cyberspace, where non-state actors, transnational networks, and the fluidity of information flow play pivotal roles. One of the primary challenges to realism is the diminished relevance of territoriality in cyberspace.

Choucri argues that the fluidity and anonymity inherent in cyberspace undermine traditional notions of borders and boundaries, which are central to realist thought (Choucri, 2012). In this digital realm, state actors often find their sovereignty challenged by non-state entities, such as hackers and cybercriminal organizations, which can operate across borders with relative impunity. This phenomenon complicates the realist perspective, which relies on the assumption that states are the primary actors in international relations and that their interactions are governed by power politics. Moreover, the nature of conflict in cyberspace

differs markedly from conventional warfare, which is a core concern of realist theory. Cyberattacks can be executed with minimal resources and can target critical infrastructure without the need for large military forces to be present. This shift is highlighted by Levy and Gafni, who discuss the challenges of assessing the impacts of cyberattacks, emphasizing that the traditional metrics of military power do not apply in the same way in cyberspace (Levy & Gafni, 2021).

The ability of smaller, less powerful actors to inflict significant damage through cyber means challenges the realist assumption that military power is the primary determinant of state power. Additionally, the role of international cooperation in addressing cybersecurity issues complicates the realist framework. Realism posits that states act primarily in their self-interest, often leading to competition and conflicts.

However, the transnational nature of cyber threats necessitates collaboration between states and non-state actors to develop effective responses. Deibert and Rohozinski note that while states may cooperate on certain cybersecurity policies, divergent national interests can lead to conflicting approaches, highlighting the limitations of a purely realist perspective (Deibert & Rohozinski, 2010). This need for cooperation suggests a more complex interplay of interests that realism does not fully address.

Furthermore, the emergence of public-private partnerships (PPPs) in cybersecurity illustrates a shift in the locus of authority and responsibility away from the state to the private sector. As organizations increasingly rely on private sector expertise to manage cyber threats, the traditional realist view of state sovereignty and control is challenged. Kour et al. emphasize the importance of involving multiple stakeholders in cybersecurity efforts, indicating that effective governance in this domain requires a collaborative approach that transcends state-centric models (Kour et al., 2019).

This trend reflects a broader shift towards recognizing the role of non-state actors in global governance, which realism tends to overlook. The rise of cyberspace as the fifth domain has significantly challenged realist theory by undermining traditional notions of state sovereignty, altering the nature of conflict, necessitating international cooperation, and highlighting the role of non-state actors in security issues. As the international landscape continues to evolve in response to cyber threats, reevaluating existing theoretical frameworks may be necessary to better understand the complexities of contemporary global security.

Realist perspectives on cyberspace emphasize the continuity of power politics, the importance of state sovereignty, and the strategic significance of cyber capabilities in the international arena. They view cyberspace as a new domain of competition and conflict, necessitating robust cyber defenses and strategic deterrence to protect national interests from adversaries. Cyberspace, as the fifth domain, has significantly challenged several key assumptions of realist theory in international relations, and its emergence has disrupted traditional notions of state sovereignty and territorial integrity, which are fundamental to the realist theory. In cyberspace, national borders become less relevant and states' ability to control their territory is diminished (Choucri & Goldsmith, 2012).

4.12 Realism in Cyberspace: Beyond Statism

This challenges the realist assumption that states are the primary actors in international relations and that their power is primarily derived from territorial control. Cyberspace has also altered the balance of power dynamics, which is a core concept of realism. Traditional metrics of state power, such as military and economic strength, are no longer sufficient to measure a state's capabilities in the digital age. As Albakjaji (2023) notes,

> "The concept of a strong state is no longer measured by its military and economic strength, but also by the level of its ability to both defend against cyber-attacks and control cyberspace."

This shift in power dynamics challenges the realist assumptions regarding the nature of state power and how it is exercised. Furthermore, cyberspace has introduced new forms of conflict and security challenges that do not align with realist conceptions of warfare. As Choucri and Goldsmith (2012) point out, "new patterns of cyber-based conflict have been exposed, from transnational crime and espionage to cyberwar that could disrupt military systems, shut down government servers, or damage critical infrastructure." These new forms of conflict blur the lines between war and peace and challenge realist assumptions about the nature of conflict and security.

While realism remains relevant in analyzing certain aspects of cyber international relations, the unique properties of cyberspace, such as its borderless nature, redistribution of power, and new forms of conflict, have been challenged and necessitated a reevaluation of traditional realist assumptions in international relations theory (Isnarti, 2016).

Choucri's work on the impact of cyberspace on realist theory of international relations (IR) provides a nuanced understanding of how the digital realm challenges traditional realist concepts. In her analysis, particularly in "International Relations in the Cyber Age" and "Cyberpolitics in International Relations," Choucri argues that the evolution of cyberspace fundamentally alters the dynamics of power, security, and state interactions, which are central to realist thought. One of the primary challenges cyberspace poses to realism is the transformation of its power dynamics. Choucri and Clark assert that cyberspace enables weaker actors to influence or threaten stronger states, consequently disrupting the traditional power hierarchy (Choucri & Clark, 2019).

This phenomenon challenges the realist assumption that power is concentrated predominantly in state actors with significant military capabilities. In cyberspace, non-state actors, including hackers and activist groups, can exert considerable influence, complicating

the realist focus on state-centric power structures. Furthermore, she emphasizes that the fluidity and anonymity of cyberspace challenge the realist conception of national security. In "Cyberpolitics in International Relations," she discusses how the digital realm introduces new security threats that are not easily categorized within the traditional frameworks of military power and territorial integrity (Choucri, 2012).

The emergence of cyber warfare, cyber espionage, and information warfare necessitates a reevaluation of security strategies, as states must now contend with threats that can originate from anywhere in the world, often from non-state actors. This shift undermines the realist notion that security can be effectively managed using conventional military means. Additionally, Choucri highlights the implications of cyberspace on state sovereignty and territoriality. The Internet's borderless nature challenges the realist emphasis on territorial integrity as a cornerstone of state power. In her view, the ability of cyber actors to operate across borders complicates the enforcement of national laws and the protection of state interests (Choucri, 2012).

4.13 Erosion of Sovereignty and Realist Response

This erosion of sovereignty is particularly relevant in the context of international cyber norms and governance, where states must navigate a complex landscape of competing interests and competing values. Moreover, Choucri's exploration of the intersection between cyberspace and international law reveals how traditional legal frameworks struggle to adapt to the realities of the digital age. The ambiguity surrounding accountability and attribution in cyberspace further complicates the realist focus on deterrence and retaliation, as states may find it challenging to respond effectively to cyber threats when the aggressor's identity is obscured (Choucri & Clark, 2019).

This uncertainty can lead to miscalculations and escalation, which are critical concerns for realists who prioritize stability and predictability in international relations. Her analysis illustrates that cyberspace significantly influences realist theory by reshaping power dynamics, complicating security concepts, challenging state sovereignty, and highlighting the limitations of traditional legal frameworks. As the digital landscape continues to evolve, the implications for realist thought are likely to deepen, necessitating a reevaluation of established theories to account for the complexities introduced by cyberspace.

Lucas Kello proposes treating cyberspace as a "structural modifier" in international relations, which has implications for realist theory (Foulon & Meibauer, 2024). This approach suggests that cyberspace influences state behavior within the existing international structure rather than completely revolutionizing it. For realist theory, which emphasizes the importance of state power and security in an anarchic international system, cyberspace alters the nature and number of interactions between states but does not fundamentally change the core principles of realism. Kello's view contrasts with some other perspectives that see cyberspace as a revolutionary force in international relations. By treating it as a structural modifier, he maintains that cyberspace operates within the confines and constraints of the existing structure, which aligns more closely with realist assumptions about the persistence of anarchy and state-centric power dynamics (Foulon & Meibauer, 2024).

Kello's approach suggests that while cyberspace impacts areas such as deterrence, foreign policy tool choice, and uncertainty - all key concepts in realist theory - it does not fundamentally overturn realist principles. Instead, it modifies how these principles operate within the existing international structure, requiring policymakers to consider cyberspace alongside other statecraft domains rather than in isolation (Foulon & Meibauer, 2024). However, he contends that the Clausewitzian framework is inadequate for understanding the

cyber threat, as it fails to capture the essence of the danger posed by virtual weapons and argues that cyber weapons are expanding the range of possible harms between war and peace, with significant consequences for national and international security (Lindsay & Kello, 2014).

Kello's views are contradicted by Erik Gartzke, who maintains that cyberwar has limited political utility and that the Internet is generally an inferior substitute for terrestrial force in performing coercion or conquest (Lindsay & Kello, 2014). This disagreement highlights the ongoing debate in the field of cybersecurity regarding the true impact and effectiveness of cyber weapons. While Kello emphasizes the transformative nature of cyber weapons and their potential to reshape security affairs, his argument has been criticized for its technological determinism and for overlooking relevant scholarship in the field (Lindsay & Kello, 2014). The debate surrounding the impact of virtual weapons on international security remains ongoing, with scholars presenting different views on their significance and effectiveness in modern warfare.

4.14 Cyberspace as a New Arena for Power Struggles

Realists view cyberspace as an extension of the traditional domains of conflict (land, sea, air, and space). Cyberspace provides states with new opportunities for power projection and influence, without physical confrontation. This includes cyber espionage, cyber warfare, and information operations aimed at undermining rival countries (Choucri & Clark, 2013). Cyberspace has emerged as a new arena for power struggles among nation-states, fundamentally altering the international relations landscape. It provides new opportunities for states to project their power and influence globally without the use of traditional military forces. States can engage in cyber espionage, cyber warfare, and information operations to undermine their rivals and achieve strategic objectives (Choucri, 2012).

Cyber operations allow states to covertly exert influence with plausible deniability. This can include hacking into critical infrastructure, stealing intellectual property, and manipulating information to sway public opinion or destabilize political systems. These activities are often less costly and risky than traditional military actions, making them attractive statecraft tools (Choucri & Clark, 2013). Cyberspace levels the playing field, allowing smaller or less powerful states and non-state actors to challenge more powerful ones. This asymmetry can destabilize traditional power hierarchies and introduce new dynamics into international relations. Smaller states can leverage cyber capabilities to punch above their weight, engaging in cyber-attacks that can cause significant damage to more powerful adversaries (Abbasi, 2020).

Cyberspace is increasingly being integrated with traditional military strategies. Cyber capabilities complement physical military actions by providing a force multiplier effect. For example, cyber-attacks can disrupt enemy communications, disable defense systems, and gather intelligence to support conventional military operations (Isnarti, 2016). Despite the competitive nature of cyberspace, there is growing recognition of the need for international cooperation to manage cyber threats. Efforts are underway to establish international norms and agreements that regulate state behavior in cyberspace to prevent escalation and promote stability (Stevens & Kavanagh, 2021).

Cyberspace has become a significant arena for power struggles among states, introducing new methods for projecting power and influencing international relations. The integration of cyber operations into state strategies, development of cyber deterrence, and establishment of international norms are all critical to navigating this new domain of conflict and cooperation. Despite the borderless nature of cyberspace, realists emphasize the importance of state sovereignty and the need for states to control and secure their

cyberinfrastructure. The protection of national cyber boundaries is crucial for maintaining sovereignty and preventing external interference (Choucri, 2012).

The concept of sovereignty and territorial integrity in cyberspace has become increasingly complex as states navigate the challenges of governing and securing their digital domains. Heinegg (2012) argues that the principle of territorial sovereignty applies to cyberspace, protecting the cyberinfrastructure within a state's territory. States are prohibited from interfering with the cyber infrastructure of another state if the conduct is attributable and inflicts severe damage to the integrity or functionality of the foreign cyber infrastructure. This framework aligns cyber operations with the traditional concepts of territorial sovereignty (Heinegg, 2012).

Mueller challenges the application of traditional sovereignty to cyberspace, arguing that the unique characteristics of cyberspace—where territoriality and authority are separated—render traditional sovereignty concepts inappropriate. He suggests an alternative governance model based on the global commons that may better address the challenges of cyberspace governance (Mueller, 2020).

Terenteva explored the possibility of applying the territorial principle of sovereignty to cyberspace. She argues that cyberspace should be included in the concept of "territory of the state" because of its role in social, economic, and political relations. This approach requires rethinking the spatial limits of state jurisdiction to include virtual spatial units that do not have a geographical extent (Terenteva, 2019). Schmitt and Vihul (2017) discuss the evolving interpretation of sovereignty in the context of cyber operations. They note that while international law applies in cyberspace, there is still a debate over when cyber operations constitute violations of sovereignty. The lack of consensus on applicable thresholds for such violations complicates the establishment of clear legal standards (M. Schmitt & Vihul, 2017).

Khanna examines the implications of state sovereignty and the right to self-defense in cyberspace. She addresses questions regarding the applicability of international law to cyberspace, the concept of territorial jurisdiction, and the conditions under which states can exercise the right to self-defense against cyber-attacks (Khanna, 2018).

Tsagourias discusses how states assert their sovereignty in cyberspace by creating national cyberspace zones. This process involves the application of territorial notions of international law to persons, activities, and objects operating in cyberspace, reflecting the continued relevance of borders in the legal regulation of cyberspace (Tsagourias, 2018). The principles of sovereignty and territorial integrity are being redefined in cyberspace. Traditional concepts are being adapted to address the unique characteristics of the digital realm, with ongoing debates on how best to govern and secure cyberspace while respecting state sovereignty.

4.15 Cyber Deterrence and Defense

Realist approaches to cyberspace involve developing robust cyber defenses and deterrence strategies. This includes the capability to respond to cyber-attacks with equivalent or greater force, thus discouraging adversaries from launching cyber operations. The focus is on building credible cyber deterrence to maintain strategic stability (Abbasi, 2020). Cyber deterrence and defense involve a combination of strategies, including deterrence by denial, punishment, and the establishment of international norms. The unique challenges of cyberspace, such as attribution and asymmetry, require tailored approaches to effectively deter and defend against cyberthreats.

States are developing cyber deterrence strategies to prevent adversaries from launching cyberattacks. This includes building robust cyber defenses, developing offensive cyber capabilities, and establishing norms and agreements to deter such malicious activities. The goal

is to create a credible threat of retaliation that discourages cyber aggression (Ferwerda et al., 2014). Cyber deterrence and defense have become critical components of national security strategies as states seek to protect their digital infrastructure and deter malicious cyber activity. Geers (2010) discusses the complexities of deterring cyber-attacks, highlighting two main strategies: deterrence by denial (making it difficult for attackers to succeed) and deterrence by punishment (retaliating against the attackers). He identifies key challenges, such as attribution and asymmetry, which complicate the implementation of effective deterrence strategies (Geers, 2010).

Nye (2017) argues that cyber deterrence should incorporate multiple mechanisms, including the threat of punishment, denial, entanglement, and norms. He emphasized that while attribution issues hinder punishment-based deterrence, defense by denial and normative taboos can still be effective in preventing cyberattacks (J. S. Nye, 2017a). Elliott (2011) explores the applicability of nuclear deterrence concepts to cyber deterrence. He suggests that a comprehensive defense (deterrence by denial) is the most effective way to protect critical infrastructure from cyberattacks, although this approach presents significant challenges (Elliott, 2011).

Braw and Brown (2020) proposed "personalized deterrence," which involves directly communicating with individual cyber attackers with the intent to hold them personally responsible. This strategy aims to address the difficulties in deterring state-sponsored cyber aggression (Braw & Brown, 2020). Harknett (2017) suggests that both scholars and policymakers should reassess the effectiveness of cyber deterrence. Harknett and Nye argue that traditional deterrence frameworks may not be entirely applicable to cyberspace and call for new approaches (Harknett & Nye, 2017). Cornish (2021) discussed the challenges of cyber warfare, such as zero-day vulnerabilities and non-attribution of attacks. He proposed a mix of

punitive, constructive, and protective deterrence to address these challenges (Cornish, 2021).

Simcox (2012) outlined various options for cyber deterrence, addressing both terrorist and nation-state threats. He emphasizes the need for tailored deterrence strategies that consider the unique aspects of the cyber domain (Simcox, 2012). Jardine (2020) highlights the trade-offs between different forms of cyber deterrence, such as denial, punishment, entanglement, and taboos. He argues that optimizing cyber deterrence requires an understanding of these trade-offs and their implications (Jardine, 2020). Chen (2017) proposes a new deterrence strategy involving prompt and direct cyber responses that are sudden, dynamic, stealthy, and random. This approach aims to mentally and virtually defeat adversaries and is a cyber version of shock and awe (J. Chen, 2017).

Lindsay (2015) discusses the role of attribution in cyber deterrence. He argues that while attribution is challenging, it can be more effective against high-value targets where defenders are willing to invest in attribution and retaliation (J. Lindsay, 2015). Ryan (2018) identifies five types of cyber deterrence: punishment, denial, association, norms and taboos, and entanglement. He argues that understanding these types and their interactions can enhance the effectiveness of cyber deterrence strategies (Ryan, 2018).

Cyber deterrence involves various strategies and mechanisms tailored to the unique challenges of cyberspace. Effective deterrence requires a combination of denial, punishment, engagement, and normative approaches to address the complexities of cyber threats and ensure national security. Senol (2022) highlighted the importance of proactive cyberspace defense strategies. He argues that both active and passive defense measures are necessary to address the increasing complexity and severity of cyberthreats. Proactive defense includes techniques and methods designed to anticipate and mitigate cyber-attacks before their occurrence (Senol, 2022).

Iasiello (2014) critiques the application of traditional deterrence principles to cyberspace on the premise that attribution challenges, rapid response requirements, and the ability to sustain deterrence make it difficult to apply Cold War-era deterrence strategies to the cyber domain (Iasiello, 2014). Borghard and Lonergan (2021) advocate a deterrence-by-denial approach, which focuses on counter-cyber operations rather than simply improving defenses. They argue that traditional deterrence frameworks must be adapted to address the unique challenges of cyberspace (Borghard & Lonergan, 2021).

4.16 Interstate Competition and Cyber Power

Realists argue that cyberspace has intensified interstate competition, with states vying for cyber superiority. This competition is reflected in investments in offensive and defensive cyber capabilities, as well as efforts to influence global cyber governance structures to favor national interests (Banta, 2020). Interstate competition and cyber power have become critical themes in contemporary international relations, reflecting cyberspace's increasing importance in global politics. The concept of cyber power extends beyond mere technical capabilities to include the overall resources and strategies that a nation can leverage to achieve political goals.

Klimburg highlights that cyber power involves not just government cyber warriors but also capabilities within the business and civil society sectors. Western democracies often depend on voluntary cooperation from these sectors, in contrast to the more coercive approaches seen in countries such as China and Russia (Klimburg, 2011). The increasing reliance on digital technology has intensified geopolitical competition. As highlighted by Zinovieva (2022), the fragmentation of the Internet and the geopolitical struggle for digital supremacy among great powers have led to cyber diplomacy becoming a critical tool for managing interstate conflicts and advancing national interests (Zinovieva, 2022).

Schmidt (2022) discusses how breakthroughs in AI are transforming cyber competition, enhancing national security threats, and altering power dynamics. AI technologies are augmenting cyber capabilities, making security relationships among rivals more unpredictable and conflicts more difficult to manage (E. Schmidt, 2022). Harknett and Smeets (2020) examined how strategic cyber operations are used to achieve long-term objectives without resorting to traditional armed conflict. These operations are part of broader cyber campaigns aimed at achieving strategic outcomes through continuous and persistent engagement in cyberspace (Harknett and Smeets, 2020).

Devanny and Dwyer (2023) explore the UK's shift from a focus on cyber security to embracing "cyber power" in its national strategy. This approach integrates domestic and international efforts to address vulnerabilities and leverage opportunities in cyberspace, reflecting a global outlook and the increasing importance of cyber capabilities in national policy (Devanny & Dwyer, 2023). The rise of cyberspace as a critical domain in international relations has intensified interstate competition and reshaped traditional power dynamics in the region. Nations are developing sophisticated cyber strategies to enhance their influence and protect their interests, highlighting the importance of cyber power in modern geopolitical competitions.

4.17 Institutional Responses and Cooperation

While realists typically emphasize conflict and competition, they also recognize the necessity of international cooperation in addressing common cyber threats. However, this cooperation is often driven by self-interest and the desire to maintain national security, rather than altruistic motives. Efforts to establish international norms and agreements are seen as necessary to manage the inherent risks of cyberspace (Ferwerda et al., 2014). Institutional responses and cooperation in cyberspace are critical for addressing the complex and evolving challenges of cybersecurity.

Ferwerda, Choucri, and Madnick (2014) emphasized the need for robust institutional frameworks to address cyber threats. They discuss the salience of cyberspace in daily life and the necessity of institutions to manage such security threats. They proposed mapping current institutions and highlighting emerging responses and challenges to create a comprehensive understanding of cybersecurity governance (Ferwerda et al., 2014). Rugge (2012) argues for enhanced cooperation between NATO and the EU to counter cyber threats. The asymmetric and borderless nature of cyber threats requires a cooperative governance system involving both public and private actors. This cooperation can enhance resilience, facilitate information sharing, and establish common security standards (Rugge, 2012).

Cho and Chung (2017) analyzed the interplay of conflict and cooperation among states in cyberspace. They highlight that while states like the U.S. and China are in intense competition for cyber dominance, there are also instances of temporary cooperation to address shared threats. However, such cooperation is often limited by national interests and sovereignty concerns (Cho & Chung, 2017). Qian and Zhang discuss the institutional dilemmas in global cyberspace governance. They proposed constructing a global cybersecurity cooperation system to collectively address security threats. This involves recognizing interdependence, bridging interests, and integrating different civilizations into cyberspace (Qian & Zhang, 2020).

Samuel (2011) explores the strategic fit for cybersecurity cooperation between India and the United States. Despite their shared democratic values and economic systems, cooperation has been limited. Samuel (2011) argues for leveraging complementarities in the services sector to enhance bilateral cybersecurity efforts. Kvasov (2021) examines the formation of cyberspace as a social institution. He analyzed the regulatory functions, roles, interactions, and public control mechanisms that contribute to the institutionalization of cyberspace (Kvasov, 2021).

Kasper and Krasznay (2019) draw parallels between environmental agreements and cybersecurity cooperation. They suggest that successful elements from environmental regimes, such as the Montreal Protocol, can inform the design of international cyber norms and cooperative mechanisms (Kasper & Krasznay, 2019). Institutional responses and cooperation are essential for addressing the cybersecurity challenges in an interconnected world. Effective governance requires collaboration between the public and private sectors, international cooperation, and the development of robust regulatory frameworks to ensure a secure and resilient cyberspace.

4.18 Impact on Traditional Concepts of Security

The rise of cyberspace challenges traditional realist security concepts based on territorial integrity and physical military capabilities. Realists now incorporate cyber capabilities into their analyses of state power and security, recognizing that cyber-attacks can disrupt critical infrastructure and undermine national security without physical invasion (Isnarti, 2016). The impact of cyberspace on traditional security concepts is profound, reshaping how nations perceive and address security threats.

Dobák (2021) discusses how cyberspace has significantly transformed national security. The integration of cyberspace into national security strategies requires continuous monitoring of technological developments and long-term strategic thinking to respond to cyber threats effectively. (Dobák, 2021) Wu, Li, and Ji (2018) highlight the unique characteristics of cyberspace, such as openness, heterogeneity, mobility, and dynamism, which necessitate new security approaches. Traditional static security methods are inadequate for addressing novel threats such as zero-day attacks and advanced persistent threats (APT), leading to the need for dynamic defense architectures and advanced security technologies (J. Wu et al., 2018).

Deibert and Rohozinski (2010) categorize cyber risks into two dimensions: risks to cyberspace (threats to the infrastructure) and risks through cyberspace (threats facilitated by cyber technologies but targeting other domains). The complex nature of these risks requires international cooperation for effective management, although political differences often hinder such efforts (Deibert & Rohozinski, 2010). Abbasi (2020) explored the role of international organizations in promoting cybersecurity cooperation. This study emphasizes the importance of multilateral approaches to cybersecurity, given the transnational nature of cyber threats. International organizations, such as the OECD, play a crucial role in facilitating cooperation and developing global cybersecurity standards (Abbasi, 2020).

Kozub and Mitręga (2021) argue that strategic thinking is essential for addressing the security challenges posed by cyberspace. They highlight the need for comprehensive cybersecurity strategies that integrate technological, political, and social dimensions to protect against cyber threats (Kozub & Mitręga, 2021). Taha (2023) discusses how cyberspace has become a critical domain for international power struggles, with major powers like the United States focusing on technological superiority to enhance their strategic capabilities. The integration of cyber strategies into national security policies reflects the growing importance of cyberspace in maintaining the global power balance (Taha, 2023). Choucri and Goldsmith (2012) examine how cyberspace challenges traditional international relations theories based on state-centric models and territorial sovereignty. Cyberspace introduces new forms of conflict and cooperation, necessitating a reevaluation of how states interact in the global arena (Choucri & Goldsmith, 2012a).

The impact of cyberspace on traditional security concepts is profound, requiring new approaches to national and international security. The unique characteristics of cyberspace, such as its borderless nature and rapid technological advancements, necessitate dynamic

defense strategies, international cooperation, and a reevaluation of traditional security frameworks to address the complex challenges posed by cyber threats.

3.19 Cyberspace and Realist Principles

In cyberspace, states seek to extend their control and influence, mirroring their behaviors in the physical world. The concept of "cyber sovereignty" has emerged, wherein states assert their right to regulate and control cyber activities within their borders. The extension of state sovereignty in cyberspace is a complex and evolving issue as states seek to assert control and jurisdiction over their digital domains.

Terentieva (2021) explores the special approach to establishing state sovereignty in cyberspace, considering both the technical and virtual components of network infrastructure. She emphasizes the need to construct boundaries in cyberspace, much like physical territorial boundaries, to maintain state sovereignty (Terentieva, 2021). Terenteva (2019) also discusses the possibility of applying the territorial principles of sovereignty and jurisdiction to cyberspace. She argues that cyberspace, as a sphere of social, economic, and political relations, should be included in the concept of "territory of the State," thereby extending traditional territorial jurisdiction to digital spaces (Terenteva, 2019).

Khanna (2018) examines the implications of state sovereignty and the right to self-defense in cyberspace, highlighting how international law applies to cyber operations. She addresses issues such as territorial jurisdiction, attribution, and the right of states to defend themselves against cyber-attacks (Khanna, 2018). Schmitt and Vihul (2017) discuss the evolving interpretation of sovereignty in cyberspace, noting that while international law applies, there is still debate over what constitutes a violation of sovereignty in a cyber context. They highlight the need for clearer legal standards to address these issues (M. Schmitt & Vihul, 2017).

Mueller (2020) argues against the application of traditional sovereignty concepts to cyberspace. He suggests that cyberspace governance should be based on the global commons model rather than territorial sovereignty, reflecting the unique characteristics of the digital domain (Mueller, 2020). Barcomb et al. (2012) propose a construct for establishing sovereignty in cyberspace by drawing parallels with space sovereignty. They discuss how nations can claim sovereignty over the physical and architectural aspects of cyberspace and manage information flows within these boundaries (Barcomb et al., 2012). Heinegg (2012) examined the principle of territorial sovereignty in cyberspace, emphasizing that states must not interfere with the cyberinfrastructure of other states. He also discusses the responsibility of states to prevent their territories from being used for cyber-attacks against other states (Heinegg, 2012).

The extension of state sovereignty in cyberspace involves adapting traditional concepts of territorial jurisdiction and sovereignty to the digital realm of cyberspace. This requires establishing clear legal standards and governance models that address the unique challenges posed by cyberspace while ensuring that states can protect their digital infrastructure and assert control over their cyber domains.

4.20 Anarchic Nature of Cyberspace

Cyberspace is inherently anarchic and lacks central governing authority. This parallels the realist view of the international system and emphasizes the need for states to develop their cyber capabilities to defend themselves against threats. The anarchic nature of cyberspace refers to the absence of a central authority governing this domain, leading to a self-help system in which various actors operate with significant freedom. Liu (2023) discussed the anarchic nature of cyberspace and its implications for national security. He highlighted the difficulty in controlling cyber-attacks targeting civilians and national facilities, emphasizing the need for proactive policies to detect and mitigate cyber threats. The invisibility and anonymity inherent in cyberspace contribute to its anarchic character (J. Liu, 2023).

Mainwaring (2020) challenges the libertarian narrative of cyberspace as a "Wild West" and argues that states have always exerted some control over it. Despite the perception of anarchy, the physical infrastructure of the Internet is located within specific jurisdictions, which allows states to exercise centralized control. This view contends that the anarchic nature of cyberspace has been exaggerated and deliberately promoted to distract from state influence (Mainwaring, 2020).

The extension of state sovereignty into cyberspace involves adapting traditional concepts of territorial jurisdiction to the digital realm of cyberspace. States seek to establish legal and regulatory frameworks to assert control over their digital domains, challenging the anarchic nature of cyberspace. This adaptation is necessary to protect national security and effectively manage cyber threats (Heinegg, 2012). Swann (2020) revisits the relationship between anarchism and cybernetics, focusing on how principles of self-organization and autonomy can inform anarchist social movement practices. This perspective highlights the potential for a non-hierarchical, decentralized organization within cyberspace, aligning with its anarchic nature (Swann, 2020).

Gelvin (2008) situates the concept of anarchy within the context of international relations, exploring how the absence of a central authority in cyberspace parallels the anarchic state of an international system. This perspective underscores the challenges of maintaining security and order in a domain where traditional mechanisms of control are less effective (Gelvin, 2008). The anarchic nature of cyberspace presents significant challenges to governance and security. While states attempt to extend their sovereignty and establish control, the decentralized and borderless characteristics of cyberspace complicate these attempts. Understanding the balance between anarchy and state control is crucial for developing effective cyber security policies and frameworks.

4.21 Cyber Power and National Security

The concept of power in cyberspace encompasses various dimensions, including the ability of state and non-state actors to exert influence, control, and project capabilities in the digital realm. The distribution of cyber capabilities among states affects the global power dynamics. States with advanced cyber capabilities can project power, influence other states, and achieve their strategic objectives without resorting to conventional military force. The rise of cyber capabilities has transformed the conceptualization of power in national security. States use cyberspace to achieve strategic objectives, often supplementing traditional military power with cyber operations. This includes both defensive measures and offensive strategies to disrupt adversaries' networks (Kramer et al., 2009).

Jordan (1999) explores the culture and politics of cyberspace, arguing that cyberpower involves not only technical capabilities but also the social and political dynamics that shape how these capabilities are used. He examined how cyberspace allows individuals and states to project power in new and complex ways (Jordan, 1999). Cyber power has great strategic importance as it is increasingly seen as an essential domain for achieving national objectives, supplementing the need for land, sea, air, and space power (Lonsdale & Kane, 2019).

Libicki (2007) discusses how cyberspace has become a medium for hostile actions such as hacking and cyber-attacks. These activities can disrupt information systems, steal data, and cause widespread damage, demonstrating the coercive potential of cyber power (M. C. Libicki, 2007). Venables et al. (2017) examine how cyberpower can be projected and measured. They argue that cyberspace provides a suitable medium for the projection of both soft and hard power, influencing the behavior of individuals and states through digital means (Venables et al., 2017). Stevens and Kavanagh (2021) provide a conceptual framework for understanding cyber power in international relations. They identify different forms of cyber power, such as

compulsory, institutional, structural, and productive power, and analyze how states leverage these forms to achieve their strategic objectives (Stevens & Kavanagh, 2021).

Brizhinev et al. (2018) model the dynamics of power transitions in cyberspace, comparing them to traditional domains of state interaction. They argue that cyberspace, owing to its unique characteristics, may be less conducive to the emergence of hegemonic powers than other domains (Brizhinev et al., 2018). The concept of power in cyberspace is multifaceted, involving both the projection of influence through digital means and the strategic use of cyber capabilities for the national security. Understanding cyber power requires consideration of its technical, social, and political dimensions, as well as the unique characteristics of the digital domain.

4.22 Cyber Warfare and National Security

One of the most significant implications of cyberspace for realism is its impact on national security and war. Realist scholars analyze how states use cyber capabilities to enhance security and engage in cyber warfare. The integration of cyber warfare into national security strategies reflects the growing importance of cyberspace in modern conflicts. Geers discusses the complexities of cyber-attack deterrence, highlighting two primary strategies: deterrence by denial (making it difficult for attackers to succeed) and deterrence by punishment (retaliating against attackers). He emphasizes the challenges of attribution and asymmetry in cyberspace, which complicate the effectiveness of these deterrence strategies (Geers, 2010).

Mukherjee outlines the broad implications of cyber warfare, including the potential damage to national infrastructure and information systems through cyber-attacks, such as computer viruses and denial-of-service (DOS) attacks. He also addresses the controversial nature of defining such operations as "war" and the challenges in responding to these threats (Mukherjee, 2019). Baram explores the impact of cyber warfare on Israel's national security,

emphasizing the need to revise traditional security concepts to ensure cyber superiority. He highlights the critical threats posed by cyber-attacks to vital infrastructure and the importance of integrating cyber defense capabilities into national defense strategies (Baram, 2017).

Jovanovski et al. provide a historical perspective on cyber warfare, tracing its evolution through three major periods: the technological advances of the 1980s, the post-Cold War era, and the period following the September 11 attacks. They emphasized the need for national policies and strategies to address the consequences of cyber warfare (Jovanovski et al., 2020). Wu and Huang discuss the threat cyber warfare poses to international security, highlighting issues such as the inefficiency of deterrence, limitations in legislation, and the potential for escalation. They emphasized the need for international cooperation and effective legal frameworks to manage these threats (Y. Wu & Huang, 2020).

Eun and Aßmann examined the implications of cyberwarfare for national security and traditional warfare. They argue that while cyber weapons do not make traditional war obsolete, they can amplify the effects of kinetic attacks and reshape the way wars are conducted. They stress the need to revamp policies and theoretical frameworks to address the new realities of cyber conflict (Eun & Aßmann, 2014).

Gondal explored the legal and ethical implications of cyber warfare, particularly during armed conflict. He highlights the challenges of applying international humanitarian law to cyber operations and the serious consequences of cyberattacks that extend beyond targeted computer systems (Gondal, 2017).

4.23 Cyber Warfare and National Strategies:

Cyber warfare represents a significant and evolving threat to national security, requiring comprehensive strategies that encompass deterrence, defense, and international cooperation. Integrating cyber capabilities into national defense frameworks is essential for addressing the

multifaceted challenges posed by cyber threats. Ahmed et al. (2022) discuss the importance of developing national strategies to secure cyberspace, particularly for naval operations. They highlight the need for advanced cyber capabilities to protect maritime assets and infrastructure from cyber-attacks and emphasize the integration of cyber defense into broader national security frameworks (Ahmed et al., 2022).

States develop offensive cyber capabilities to disrupt, degrade, or destroy adversary systems and defensive capabilities to protect their critical infrastructure and data. Offensive and defensive capabilities in cyberspace are critical components of national security and are integral to modern national security strategies. Although offensive capabilities offer strategic advantages, they also pose significant risks and complexities that must be carefully managed. In contrast, defensive strategies provide stability and resilience against cyber threats.

Smeets and Lin (2018) highlight that offensive cyber capabilities (OCC) can alter the strategic use of military power. While not particularly effective in deterring adversaries, OCC can be valuable for compellence and provide preemptive and preventive strike options for the United States. The reversibility of OCC effects can encourage compliance and de-escalate conflicts without public exposure (Smeets & Lin, 2018).

Herrick and Herr (2016) argue that the dominance of offensive operations in cyberspace is not axiomatic. Effective cyber operations require a nuanced interaction between offense and defense, considering the role of countermeasures and operational complexity involved (Herrick & Herr, 2016). Selján (2023) discusses the challenges of assessing and measuring offensive cyber capabilities. An accurate assessment is essential for understanding and developing national cyber capabilities to combat future cybersecurity challenges (Selján, 2023). Shaheen (2014) examined the offense-defense balance in cyber warfare, arguing that the offensive nature of cyber weapons can destabilize international security. The proliferation of offensive

cyber capabilities increases the likelihood of their use, raising concerns about global security (Shaheen, 2014).

Smeets discusses the benefits and risks of integrating intelligence and military capabilities to develop offensive cyber capacities. Enhanced interaction efficiency, better knowledge transfer, and reduced mission overlap are key benefits, but the risks include mission creep and intensified cyber security dilemmas (Smeets, 2018). Schneider (2016) explores the paradox of cyber-enabled warfare, in which an increased reliance on cyber capabilities enhances both offensive potential and vulnerability. This duality impacts deterrence and crisis stability, making cyber capabilities a double-edged sword (Schneider, 2016).

Campbell argues that defense has clear advantages in cyberspace. Drawing on the U.S. Army doctrine and Clausewitz's principles, he suggests that a defensive posture is more effective at both tactical and strategic levels . Huntley (2016) applies offense-defense theory to cyberspace, concluding that current factors favor offensive capabilities. However, strategic assessments must consider the interplay between cyber capabilities and other military means (W. L. Huntley, 2016).

4.24 State-Sponsored Cyber Attacks

State-sponsored cyber-attacks are a growing concern for national security and international stability. Examples of state-sponsored cyber-attacks include the Stuxnet virus (attributed to the U.S. and Israel) targeting Iran's nuclear program and Russia's cyber operations against Estonia, Georgia, and Ukraine. Vincent (2017) discusses how state-sponsored hacking has become a common part of the cybersecurity landscape, affecting not only governments but also businesses and NGOs. State-backed actors have increasingly targeted various organizations, leading to significant security challenges (Vincent, 2017).

Johnson (2014) examines how social networks play a role in state-sponsored cyber-attacks, such as motivating individuals to participate in Distributed Denial of Service (DDoS) attacks and facilitating spear phishing. The ubiquity of social networking infrastructures complicates the attribution and defense against these attacks (C. W. A. Johnson, 2014).

Martin (2020) explores how the Justice Against Sponsors of Terrorism Act (JASTA) can help U.S. victims of state-sponsored cyber-attacks overcome sovereign immunity and seek justice in U.S. courts. This framework aims to hold foreign states accountable for cyber-attacks that harm U.S. nationals (J. J. Martin, 2020). Blinderman and Din (2017) argue that the current U.S. legal framework does not effectively deter state-sponsored cybercrime. They suggest that U.S. law should apply extraterritorially and propose abrogating sovereign immunity for states engaged in cybercrime (Blinderman & Din, 2017).

Delerue (2019) addressed the difficulty of attributing cyber operations to state actors. Attribution involves technical, legal, and political dimensions, making it challenging to hold states accountable for cyber operations conducted by non-state actors under their direction or control (Delerue, 2019). Herrmann (2019) discusses state-sponsored cyber espionage, highlighting its lower risk compared to traditional espionage. Defensive measures against such well-funded attacks are costly and complex, underscoring the need for robust cyber defense strategies (Herrmann, 2019). Courtney (2017) explored the growing threat of state-sponsored cyber warfare, including cyber espionage and cyber-terrorism. The increasing reliance of national authorities on digital information and networks makes these attacks particularly damaging and disruptive (Courtney, 2017). Durojaye and Raji (2022) examine the impact of state-sponsored cyber-attacks on critical infrastructure. They highlight incidents such as the Russian cyber-attack on Ukraine's power grid in 2015, which caused significant disruptions

and demonstrated the vulnerability of critical infrastructure to cyber threats (Durojaye & Raji, 2022).

State-sponsored cyberattacks pose significant threats to national security, critical infrastructure, and global stability. Addressing these threats requires robust legal frameworks, effective attribution mechanisms, and comprehensive defense strategies to protect against the increasing sophistication and frequency of cyber-attacks by state actors. Just as nuclear deterrence shaped the Cold War, cyber deterrence has become a key component of national security strategies. States aim to deter cyber-attacks through retaliation or by demonstrating robust defensive capabilities. Cyber deterrence is a critical concept in national security that aims to prevent cyber-attacks through various strategies and mechanisms.

4.25 National Security in Cyber Age

- **Critical Infrastructure Protection**

  States prioritize the protection of critical infrastructure, such as power grids, financial systems, and communication networks, from cyber threats.

- **Cyber Espionage:**
- States conduct cyber espionage to gather intelligence on adversaries and influence their strategic decisions. High-profile cases include China's alleged cyber-espionage against the U.S. and other countries.

- **Cyber Alliances**
- Realist principles of alliance formation extend to cyberspace, with states cooperating to enhance their collective cyber defense. Examples include NATO's Cyber Defense Policy and the EU's cybersecurity initiatives.

Case Studies

- **Stuxnet:**

  Stuxnet was a sophisticated cyber weapon allegedly developed by the U.S. and Israel to target Iran's nuclear enrichment facilities. The attack demonstrated the potential of cyber

capabilities to achieve strategic objectives without direct military confrontation. It also highlights the vulnerabilities of critical infrastructure to cyber-attacks. Stuxnet reflects the realist principles of power projection and the use of covert operations to weaken adversaries. This underscores the importance of cyber capabilities in contemporary security strategies.

- **Russia's Cyber Operations**

  Russia has been implicated in several high-profile cyber operations, including attacks on Estonia (2007), Georgia (2008), and Ukraine (2015-2016). These operations involve disrupting communication networks, government services, and critical infrastructure. These attacks illustrate the use of cyber capabilities to achieve political and strategic objectives, such as undermining the stability of neighboring states and demonstrating power over them. Russia's cyber operations align with the realist principles of seeking power and influence in its near abroad. These attacks also emphasize the role of cyber capabilities in asymmetric warfare and statecraft.

4.26 Power Dynamics in Cyberspace

The distribution of cyber capabilities among states affects global power dynamics and has significant implications for international relations. The U.S. is a leading cyber power with advanced offensive and defensive capabilities. It invests heavily in cybersecurity and cyber warfare, viewing cyberspace as a critical domain for ensuring national security. China has also rapidly developed its cyber capabilities, focusing on cyber espionage, intellectual property theft, and cyber warfare. It seeks to challenge U.S. dominance in cyberspace and enhance its strategic position.

Similarly, Russia's cyber capabilities are integral to its hybrid warfare strategy, combining cyber operations with traditional military tactics to achieve geopolitical objectives. Cyberspace has become a key arena for strategic competition among major powers. The U.S.,

China, and Russia engage in ongoing cyber conflicts that influence global power dynamics. Cyber capabilities enable states to engage in asymmetric warfare, where weaker states or non-state actors can challenge stronger adversaries through cyber-attacks. States form cyber alliances to enhance their collective security, whereas cyber rivalries exacerbate tensions and contribute to the complexity of international relations.

The integration of cyberspace into realist theories of international relations highlights its profound impact on state behavior, power dynamics, and national security. By examining cyber warfare, national security strategies, and case studies, this chapter demonstrates how realism adapts to the challenges and opportunities presented by the digital world. The insights gained from this analysis underscore the need for a comprehensive understanding of cyberspace within a realist framework, setting the stage for further exploration of its implications for international relations.

4.27 Cyber-skeptics

Those who question the concept of cyberwar in the field of international relations contend that it is frequently exaggerated or misconstrued, mainly because of a lack of agreement on its definition and the true nature of cyber conflicts. This doubt stems from several key points that challenge the dominant narratives surrounding cyber warfare itself. A primary argument put forth by these skeptics is that numerous incidents branded as "cyberwar" are more accurately categorized as acts of espionage or sabotage rather than genuine acts of war. The term "cyberwar" might not accurately reflect the traditional definition of war, potentially leading to misconceptions. This viewpoint underscores the importance of developing a more precise framework to categorize different types of cyber conflicts, as many activities in the digital realm do not have the same impact as conventional warfare. (Ashraf, 2021).

Critics of the cyberwar concept also highlight the historical patterns of cyber conflicts as evidence against an imminent digital warfare scenario. According to Tikk and Kerttunen (2020), if cyberspace was truly dominated by offensive capabilities, we would expect to witness more frequent and intense cyber confrontations. However, empirical studies reveal a surprising trend of "cyber restraint," where nations exercise caution in their digital operations, contradicting the predictions of those who warn of impending cyber threats (Tikk & Kerttunen, 2020). The observed self-control in cyberspace challenges the assumption that digital environments lead to conflict escalation. This restraint indicates that cyber conflicts are more intricate and multifaceted than the simplistic war/peace dichotomy often used in discussions on cyberwarfare.

Furthermore, Lindsay & Kello (2014) emphasize the restricted political effectiveness of cyberwarfare, suggesting that the Clausewitzian framework, which stresses the importance of military force in achieving political goals, may not fully encompass the nature of cyber conflicts. They argue that cyber capabilities do not necessarily provide effective means of coercion or deterrence, thus questioning the strategic importance of cyber warfare as a diplomatic tool (Lindsay & Kello, 2014).

Furthermore, the participation of non-governmental entities in the digital realm challenges the traditional, state-focused perspective on conflict. The emergence of cyber terrorists and other non-state actors adds a level of intricacy that tests the conventional understanding of warfare, which typically centers on state actors. This added complexity raises concerns about responsibility and the ramifications for international law, further complicating discussions surrounding cyberwar (Sajid, 2024).

Moreover, skeptics of cyberwar argue that the concept is often mischaracterized, lacking a clear definition, and that the empirical evidence does not support the notion of frequent or severe cyber conflicts. They emphasize the need for a more nuanced understanding

of cyber interactions that considers the roles of non-state actors, the complexities of cyber operations, and the limitations of traditional military frameworks in the digital space.

4.28 Limitations of Realist Theory in Cyberspace

The limitations of realist theory in the context of cyberspace are significant and multifaceted, primarily because of the unique characteristics of the digital domain that challenge traditional realist assumptions about power, security, and state behavior. Several key aspects highlight these limitations. Realist theory traditionally emphasizes the state as the primary actor in international relations, focusing on military power and national interest.

However, cyberspace has enabled non-state actors, such as hackers, cybercriminals, and activist groups, to play pivotal roles in international security dynamics. Taddeo argues that the emergence of these non-state actors complicates the realist framework, which often overlooks their influence and the implications of their actions in the cyberspace. This shift necessitates a broader understanding of security that includes a diverse array of actors beyond the state (Taddeo, 2017).

Realism relies heavily on deterrence theory, which posits that the threat of retaliation can prevent aggression. However, Taddeo points out that the nature of cyber operations complicates traditional deterrence strategies. The anonymity and fluidity of cyberspace make it difficult to attribute attacks to specific actors, undermining deterrence. This lack of clarity can lead to miscalculations and escalations, which realist theory does not adequately address (Taddeo, 2017). The uncertainty surrounding cyber operations poses a significant challenge to realist assumptions regarding military power and strategic stability. Gomez and Whyte highlight that the inherent deficit of information about cyber operations creates gaps in understanding state behavior in cyberspace. This uncertainty complicates the realist focus on clear power dynamics and strategic signaling, as states may struggle to interpret the intentions behind cyber actions (Gomez & Whyte, 2021).

The borderless nature of cyberspace challenges the realist emphasis on territory and state sovereignty. Choucri notes that the fluidity and anonymity of cyberspace have disrupted traditional concepts of national security and diplomacy. In this context, the ability of cyber actors to operate across borders undermines the realist notion of state control over its territory and complicates the enforcement of national laws (Choucri, 2012).

Realist theory often simplifies conflicts into binary frameworks of war and peace; however, the nature of cyber conflicts is more complex. Watanabe argues that while cybersecurity can be likened to traditional deterrents, the dynamics of cyber interactions require a more nuanced approach that incorporates elements from other theories, such as constructivism. This complexity challenges the realist framework, which may not fully account for the multifaceted nature of cyber conflicts and the interplay of various actors and interests (Watanabe, 2020). The application of existing international law to cyberspace is fraught with such challenges.

Leng discusses how the unique nature of cyberattacks complicates the application of traditional legal frameworks, making it difficult to determine when a cyberattack constitutes the use of force. This ambiguity further complicates the realist focus on deterrence and retaliation, as states may find it challenging to respond effectively to cyber threats when the aggressor's identity is obscured (Leng, 2023). The limitations of realist theory in the context of cyberspace are evident in its inability to adequately address the complexities introduced by non-state actors, the challenges of deterrence, the erosion of sovereignty, and the ambiguous nature of cyber conflicts. As the digital landscape continues to evolve, these limitations necessitate a reevaluation of traditional theories in international relations to better understand the dynamics of cybersecurity and their implications for global security.

CHAPTER-5

5. Cyberspace and Liberalism

Liberalism in international relations emphasizes the importance of individual freedom, democracy, human rights, and the rule of law. It posits that international cooperation and institutions can lead to more peaceful and prosperous global interactions. The emergence of cyberspace as the fifth domain of warfare has significantly influenced the liberal theory of international relations (IR) by reshaping the dynamics of state interactions, security paradigms, and the roles of non-state actors. This transformation is characterized by a shift from traditional state-centric security concerns to a more complex interplay of actors, including international institutions, the private sector, and civil society, which are pivotal in addressing cybersecurity challenges.

Cyberspace is increasingly recognized as a strategic domain that challenges the foundational principles of sovereignty and territoriality underpinning traditional IR theories. Medeiros and Goldoni argue that the rise of human interaction in cyberspace necessitates a reevaluation of these principles, as the state monopoly on violence is contested in this new domain (Medeiros & Goldoni, 2020). This is echoed by Kututung, who posits that liberalism can foster a cooperative cyber order by framing cyberwarfare as a common challenge that requires collective action among state and non-state actors (Kututung, 2024). The liberal perspective emphasizes the importance of international institutions in facilitating cooperation and establishing norms for cybersecurity, which is crucial for mitigating the risks posed by cyber threats.

Moreover, the liberal theory's focus on interdependence and cooperation is further illustrated by the evolving nature of conflict in cyberspace. The competition between major powers, such as the United States and China, highlights the dual nature of cyber interactions,

in which conflict can coexist with opportunities for collaboration (Cho & Jongpil, 2017). This complexity necessitates a nuanced understanding of how states can navigate the cybersecurity landscape by balancing competitive and cooperative strategies to enhance their security (Ardita, 2023). The role of international organizations, such as the United Nations, in promoting cybersecurity norms and practices is critical in this context, as they provide a platform for dialogue and cooperation among states (Cho & Jongpil, 2017).

The implications of cyberspace as the fifth domain extend beyond state interactions to encompass broader societal impacts, including the privatization of cybersecurity efforts. McCarthy discusses how public-private partnerships (PPPs) have emerged as a vital mechanism for addressing cybersecurity challenges, reflecting a shift in the locus of authority from the state to a more decentralized model involving various stakeholders (McCarthy, 2018). This trend aligns with the liberal emphasis on pluralism and the recognition of multiple actors in the international system, thereby reinforcing the relevance of liberal theory in understanding contemporary security dynamics.

The integration of cyberspace as the fifth domain into the liberal theory of international relations underscores a paradigm shift in the conceptualization and management of security. The interplay between state and non-state actors, the role of international institutions, and the emergence of new governance models illustrate the evolving landscape of global security in the digital age. Thus, liberalism offers a robust framework for analyzing these developments and fostering cooperation in addressing the multifaceted challenges posed by cyberspace.

5.1 Democratic Peace Theory

Democratic Peace Theory is a significant concept in international relations, positing that democracies are less likely to engage in armed conflict with one another. This theory has been influential in shaping foreign policy and promoting democratic governance as a means of

achieving global peace. This theory posits that democracies are less likely to go to war with one another because of their shared norms, political structures, and mutual economic interests. Doyle (1986) highlights that liberal states create a separate peace among themselves but may still engage in conflict with non-liberal states (Doyle, 1986).

Furtuna analyzed the theory of democratic peace, highlighting its popularity and influence in international relations. Democracies resolve contradictions peacefully, and a world with more democratic states would be more peaceful. This article also addresses the criticisms and challenges of the theory (Furtuna, 2021). Reiter tests the hypothesis that peace fosters democracy and examines whether war defeats increase the likelihood of democratization in authoritarian states. The study finds mixed results, suggesting that peace does not necessarily lead to democracy and that participation in international wars can hinder democratic transitions (Reiter, 2001). Russett & O'neal argue that democracy, economic interdependence, and international mediation collectively reduce the chances of war. Drawing on Kantian ideas, the authors suggest that these elements work together to promote peace (Russett & O'neal, 2000).

Gartzke debated whether democratic peace is due to shared democratic norms or a lack of motives for conflict. This study uses United Nations General Assembly roll-call votes to analyze preference similarity and its impact on peace between democracies (Gartzke, 2000). Layne critically questions the theoretical foundations of democratic peace theory, suggesting that it oversimplifies the complex relationship between democracy and peace. The study argues that the theory does not account for the behavior of democratic states towards non-democracies (Layne, 1994). Solingen explored democratic peace theory from the perspective of domestic political processes and international behavior. This suggests that domestic coalitions and internationalization impact the likelihood of war and peace (Solingen, 2001).

Hobson argues for a critical theory approach to democratic peace, addressing its ethical and practical consequences. This study highlights the need for diverse methodologies to understand the democratic peace theory (Hobson, 2011). Democratic Peace Theory remains a central and debated concept in international relations, highlighting the potential for democracies to maintain peace among themselves. While empirical evidence supports some aspects of the theory, ongoing research and critiques emphasize the need for a nuanced understanding of the relationship between democracy and peace.

In the context of cyberspace, this theory can be adapted to understand how democratic principles influence online interactions and conflict resolution. The digital realm offers a new dimension to democratic engagement, potentially fostering peace through enhanced communication and participation. However, the application of democratic peace theory to cyberspace is complex and multifaceted. The Internet provides a platform for democratic engagement, allowing citizens to participate more actively in political discourse and decision-making processes. This increased participation can lead to a more informed and engaged citizenry, which is the cornerstone of democratic peace theory. The Internet's role in facilitating electronic democracy is crucial, as it enhances citizens' ability to engage in politics, potentially reducing the likelihood of conflict (Fisher et al., 1996).

Cyberspace can serve as both a battlefield and a platform for peacebuilding. Cyber peacebuilding involves actions that delegitimize online violence and build societal capacity to manage peaceful online communication. This approach aligns with democratic peace theory by promoting nonviolent conflict resolution and reducing vulnerability to online violence triggers (Chenou & Bonilla-Aranzales, 2022).

Democratic peace theory suggests that democratic norms and structures, such as transparency, checks, and balances, contribute to peaceful interactions. In cyberspace, these

principles can be mirrored through open communication channels and collaborative platforms that encourage dialogue and understanding among users, potentially reducing the likelihood of cyber conflicts (Adiputera, 2017).

There are challenges in applying democratic peace theory to cyberspace because of methodological gaps. For instance, the theory often treats democracy as a dichotomous variable, which may not capture the nuances of online democratic engagement. Reconceptualizing democracy as a measurable variable could provide a more accurate understanding of its impact on cyber peace (Mouchantaf, 2013). The application of democratic peace theory in cyberspace must also consider real-world events that challenge its assumptions. For example, the belligerent behavior of democratic states during the 'War on Terror' highlights the limitations of the theory in explaining all forms of conflict, including those in cyberspace (C. Hobson, 2011).

Studies have indicated that democracies exhibit a pacifying effect in cyberspace, meaning that they are less likely to initiate state-sponsored cyberattacks against other democracies. This mirrors the traditional democratic peace theory, which posits that shared norms, mutual trust, and institutional checks discourage open conflict among democratic states (Browning, 2023). When cyber incidents occur between democracies, they are typically limited to espionage rather than more destructive forms of attack, such as data destruction or manipulation. Espionage is often handled privately rather than being publicly attributed, possibly to avoid escalation and to maintain diplomatic relations. This suggests that democracies prefer to resolve cyber disputes quietly, consistent with the theory's emphasis on negotiation and compromise (Hunter et al., 2022).

Democracies are less likely to publicly attribute cyberattacks to other democratic nations. This may be due to concerns over public perception, economic disruption, or the desire

to avoid framing another democracy as an aggressor. The lack of public attribution supports the idea that democratic states seek to manage cyber conflicts in ways that minimize public confrontation and escalation (Geiger, 2021). The same structural and normative factors that underpin democratic peace in physical conflicts—such as the need for public support, institutional checks, and shared values— seem to operate in cyberspace. Democratic institutions require time and consensus to engage in conflict, and shared norms encourage compromise and respect for agreements, thereby reducing the likelihood of offensive cyber operations (Browning, 2023).

Although democratic peace theory offers a framework for understanding potential peace-promoting mechanisms in cyberspace, it is essential to recognize the complexities and limitations of its applicability. The digital realm presents unique challenges and opportunities for fostering peace, requiring a nuanced approach that considers both the strengths and shortcomings of democratic principles in this context.

5.2 Interdependence and International Institutions

Liberalism emphasizes the role of international institutions and interdependence in promoting peace and cooperation. Institutions help manage international relations by providing frameworks for negotiation, reducing transaction costs, and fostering cooperation. Keohane (2012) discusses how institutional liberalism has contributed to increasing the legalization, moralism, and coherence of international regimes (Keohane, 2012).

Interdependence and the role of international institutions are crucial concepts in international relations, focusing on how states and other global actors interact, cooperate with, and resolve conflicts with each other. This perspective emphasizes that global peace and stability can be achieved through economic, political, and social interdependence, facilitated by international institutions.

Farrell and Newman discuss how transnational interactions shape domestic institutions and global politics in a world of economic interdependence. This study examines how interdependence alters domestic political institutions through diffusion, coordination, and extraterritorial application, and how it changes the national institutions mediating internal debates on globalization (Farrell & Newman, 2014). Sundelius examined the concept of interdependence and its implications for national foreign policymaking. This study highlights how interdependence impacts state objectives, domestic and foreign policy relations, and national strategies, especially for smaller European nations (Sundelius, 1980).

Holsti explored the increasing interdependence between industrial countries and the significant impact of events and technological innovations. This study discusses how interdependence shapes diplomacy and international relations (Holsti, 1978). Kroll provides a framework for understanding interdependence using game-theoretic analysis. This study distinguishes between dependence, interdependence, and independence, and explores how these concepts influence state interactions in international politics (Kroll, 1993).

Gartzke, Li, and Boehmer discuss how economic interdependence influences states' recourse to military violence. The study demonstrates that interdependence can deter minor conflicts and offers non-militarized avenues for signaling resolve (Gartzke et al., 2001). Morse explored the contradiction between interstate and intrastate politics in a world of increasing interdependence and concluded that modernization impacts governmental power and interstate interactions (Morse, 1969).

Interdependence and international institutions are integral to understanding contemporary international relations. These concepts highlight how interconnected economic, political, and social systems influence global stability and cooperation. Effective governance and conflict resolution in the modern world rely on recognizing and managing these

interdependencies. Liberal international relations theory focuses on the relationship between states and the domestic and transnational social contexts in which they are embedded. This interaction shapes state preferences and behavior in world politics. Moravcsik (1997) elaborates on how societal ideas, interests, and institutions influence state behavior by shaping state preferences (Moravcsik, 1997).

State-society relations in international relations focus on how domestic political structures, social contexts, and interactions between the state and society influence state behavior and international dynamics. This perspective is essential for understanding the complex interplay between internal and external factors in shaping international policy and action.

Halliday discusses the theoretical debates within international relations regarding the primacy of the state and its role as the primary actor in international politics. He examines how different paradigms, such as realism, transnationalism, and structuralism, challenge state dominance by highlighting the roles of non-state actors and global systems (Halliday, 1994). Kaiser examined state-society relations in an international context, using a case study of Ismaili healthcare initiatives in Tanzania to illustrate the relevance of multi-level analysis in studying civil society (Kaiser, 1995). Moravcsik reformulates liberal international relations theory by emphasizing that state-society relations fundamentally impact state behavior. He argues that societal ideas, interests, and institutions shape state preferences, which in turn influence international interactions (Moravcsik, 1997).

Putnam's two-level game theory explores how domestic politics and international relations are intertwined in the negotiation process. Leaders must navigate both domestic and international arenas to secure agreements, which impact their negotiating behavior and strategies (Putnam, 1988). Shapkina discusses the legal nature of state-society partnerships and

the influence of technological advancements on these relations. This study highlights the importance of effective legal frameworks in supporting positive interactions between the state and society (Shapkina, 2020).

Nye and Keohane discuss how transnational interactions influence state behavior and the global political landscape. They argue that non-state actors and transnational networks play crucial roles in shaping international relations (J. Nye & Keohane, 1971). State-society relations are a vital component of international relations and influence how states interact on the global stage. Understanding the interplay between domestic political structures, societal influences, and international dynamics is essential for comprehending state behavior and the complexities of global interactions.

Liberal interdependence in cyberspace refers to the interconnectedness and mutual reliance of states, institutions, and actors within the digital realm, guided by liberal principles such as cooperation, democracy, and freedom of the market. This concept is increasingly relevant as cyberspace becomes a critical domain for international relations, economic activities and governance. The transition from a liberal to a post-liberal order in cyberspace, the role of international cooperation, and the challenges of self-governance are key aspects of this issue.

The shift from a liberal international order to a post-liberal reality is evident in cyberspace, where power dynamics and norms are contested. This transition has led to the emergence of cyber diplomacy as a tool for navigating the new order and building bridges between differing political visions (Barrinha & Renard, 2020). Cyber diplomacy is seen as a response to evolving power structures and is crucial for shaping the future of cyberspace, highlighting the need for new practices and institutions that can accommodate diverse political and cultural perspectives (Barrinha & Renard, 2020).

Liberalism emphasizes international cooperation to address global challenges such as cybersecurity. The US–China cyber conflict exemplifies the need for sustained efforts and strong commitments to build a cooperative cyber order. International institutions, the private sector, and civil society play significant roles in fostering safe and equitable cyberspaces. These actors contribute to the development of cyber ethical norms and diplomatic mechanisms that can mitigate conflicts and enhance global cybersecurity (Naomi Kututung, 2024).

However, the notion of cyberspace self-governance, which suggests that the Internet can achieve liberal democratic ideals through bottom-up private ordering, faces significant challenges that must be addressed. Critics argue that unregulated cyberspace could undermine liberal democracy by enabling majority dominance, privacy invasion, and inequality. Selective state regulation is proposed as a necessary measure to protect liberal ideals and prevent the emergence of quasi-state institutions that may suffer from democratic deficits similar to those of nation-state democracies (N. W. Netanel, 2000).

Contrary to the belief that the Internet threatens state sovereignty, it can enhance national and global governance. The Internet facilitates access to government documents and decision-making processes, thereby strengthening the rule of law and international law through improved access to information. The Internet's role in bolstering global markets and economic interdependence aligns with liberal principles, suggesting that cyberspace can support rather than undermine state sovereignty (Maurer, 1998).

While liberal interdependence in cyberspace offers opportunities for cooperation and governance, it also presents challenges that require careful navigation by policymakers. The balance between self-governance and state regulation, the role of international institutions, and their impact on sovereignty are critical considerations. As cyberspace continues to evolve, the interplay between liberal ideals and practical governance shapes its future trajectory. The

ongoing discourse on these issues highlights the complexity of achieving a truly liberal and cooperative cyberspace, necessitating further research and policy development in this area.

5.3 Human Rights and Individual Freedoms

Liberalism places a strong emphasis on human rights and individual freedoms, arguing that international relations should protect and promote these values globally. Slaughter (2000) discusses how liberal theories of international law are based on the premise that the relationship between states and the domestic and transnational social context critically shapes state behavior (Slaughter, 2000). Human rights and individual freedom are fundamental principles of international relations, emphasizing the inherent dignity and equal rights of all individuals. These principles are enshrined in various international treaties and institutions, shaping global interactions and policies.

Forsythe discusses the evolution and status of human rights in international relations. He highlights how human rights have become central to liberal theories of a good society based on respect for individual equality and autonomy. The book examines the tension between state sovereignty and the universal application of human rights (Forsythe, 2012). Ohonbamu and Kutner discuss the challenges in protecting individual freedoms against state violations. They highlight the role of the United Nations in promoting human rights and the dilemma of enforcing these rights against sovereign states (Ohonbamu & Kutner, 1970).

Sarmiento explores the philosophical foundations of human rights, emphasizing their role in legitimizing state authority and their importance in international law to protect human rights. He discusses the impact of human rights on global civil society and state sovereignty (Sarmiento, 2001). Landman examines the intersection of human rights, comparative politics, and international relations. He highlights how human rights considerations shape domestic and international political behavior and the importance of human rights in political science

(Landman, 2005). Oikya addresses how human rights are incorporated into state diplomacy and international relations and delves into the development of international human rights regimes and their impact on state behavior and international enforcement mechanisms (Oikya, 2021).

Badar examines the legal principles governing the limitations on individual rights within international human rights instruments. This study highlights the conditions under which rights can be restricted and the importance of balancing individual freedoms with community needs (Badar, 2003). Howie discusses the protection of freedom of expression in international law, emphasizing its importance for individual development and a democratic society, and tracks the global trends of restricting free speech and the challenges in protecting this fundamental right (Howie, 2018).

Human rights and individual freedom are central to the liberal perspective of international relations. Despite its widespread recognition and incorporation into international law, practical enforcement remains a challenge. Balancing state sovereignty and the protection of individual rights continues to be a critical issue in global politics.

5.4 Economic Liberalism in International Relations

Economic liberalism advocates free trade, open markets, and economic interdependence as pathways to peace and stability. Liberal thinkers argue that economic integration reduces the likelihood of conflict by creating mutual dependency. Economic liberalism in international relations emphasizes the role of free markets, trade, and economic interdependence in promoting peace and prosperity. Liberal ideals state that economic openness and cooperation reduce the likelihood of conflict and foster stable, cooperative international relations.

The classical liberal theory of international relations presented by Haar (2009) emphasizes free trade and the balance of power as essential components of peace (Haar, 2009). Ebaye explains the historical separation of economics and politics in international relations, attributing it to liberalism. She argues that liberalism traditionally views economic activity as the domain of private enterprise, separate from government influence, which impacts international economic management and political interactions (Ebaye, 2018). Haar synthesizes classical liberal theories in international relations, highlighting their common ideas on trade, peace, international law, and balance of power. This comprehensive theory contrasts with contemporary liberal IR theory (Haar, 2009).

Buzan critiques the assumption that liberal economic structures promote international security, arguing that political and military factors are more influential. He suggests that both liberal and mercantilist structures have mixed impacts on the use of force, which are contingent on non-economic factors (Buzan, 1984). He posits that economic structures alone do not determine international security, and political and military factors play a crucial role in influencing state behavior.

Agharebparast and Zeinali discuss how international relations influenced by liberalism impact economic development. They argue that managed interdependence can lead to economic growth and stability (Agharebparast & Zeinali, 2016). Liberalism views international relations as key to economic development and argues that the effective management of interdependence promotes economic growth. Moravcsik reformulates liberal IR theory to emphasize the impact of state-society relations on state behavior. He argues that societal ideas, interests, and institutions shape state preferences, which drive international politics (Moravcsik, 1997). He argues that state behavior is influenced by domestic and transnational

societal contexts, and that liberal theory prioritizes state preferences over capabilities or institutions.

Doyle examines three traditions of liberalism (Schumpeter, Machiavelli, and Kant) and their impact on international politics. He finds that while liberal states are generally peaceful, they can also engage in conflict under certain conditions (Doyle, 1986). Liberal states are unique in their foreign policy behavior as they maintain peace among themselves but can be aggressive.

Simmons, Dobbin, and Garrett explored the diffusion of liberal policies across countries, proposing theories of coercion, competition, learning, and emulation to explain this phenomenon (Simmons et al., 2006). Liberal policies spread through various mechanisms across nations, and understanding these processes is crucial for analyzing global liberalism.

5.5 Cyberspace and Liberal Principles

- **Enhanced Cooperation**

  Cyberspace enables greater cooperation among states, international organizations, and non-state actors. Shared challenges, such as cybercrime and cybersecurity, necessitate collaborative effort.

- **Role of International Institutions**

  Institutions such as the United Nations, International Telecommunication Union, and regional organizations are pivotal in establishing norms, regulations, and frameworks for cyberspace governance.

- **Economic Integration**

  The digital economy and e-commerce promote economic interdependence, aligning with the liberal ideals of trade and economic cooperation.

5.6 Liberalist Perspectives on Cyberspace

Liberalism, a key theory in international relations, emphasizes the potential for cooperation, the role of international institutions, and the importance of economic interdependence in fostering global stability and peace. Cyberspace, with its inherent characteristics of connectivity and information sharing, aligns with many liberal principles and offers unique opportunities and challenges for international cooperation and global governance.

Liberalist perspectives of cyberspace emphasize the principles of individual freedom, democracy, and self-governance. These views often highlight the potential of cyberspace to enhance democratic participation, facilitate free speech and promote global cooperation. However, they also acknowledge challenges, such as the risk of digital divides, privacy issues, and the need for regulatory frameworks. Liberalism, as an ideological framework, prioritizes individual liberty, democratic governance, and the rule of law. In the context of cyberspace, liberalist perspectives focus on how digital technologies can support these values while also recognizing the challenges arising from the unregulated and borderless nature of the Internet.

Netanel critiques the notion that cyberspace should be self-governing, arguing that this approach might undermine liberal democratic ideals. He suggests that unregulated cyberspace could lead to majority tyranny, discrimination, privacy invasions, and inequalities and advocates for selective state regulation to protect liberal values (N. Netanel, 2000). The idea of cyberspace self-governance suggests that the Internet should be governed independently from nation-states. Proponents argue that this model better realizes liberal democratic ideals by promoting bottom-up private ordering and granting autonomy to cyberspace communities than the state-centric model. However, this concept faces significant criticism from liberal democratic theory.

Critics of this approach argue that cyberspace self-governance to achieve liberal democratic ideals is fundamentally flawed. Unregulated cyberspace can undermine liberal democracy by allowing majorities to oppress minorities, facilitating status discrimination, invading privacy, and exacerbating inequalities in accessing digital resources. Netanel argues that cyberspace self-governance would lead to several democratic deficits, mirroring those in nation-state representative democracies, but potentially worse due to the lack of oversight (N. Netanel, 2000). He contends that selective state regulation of cyberspace is necessary to protect and promote liberal democratic values. Without regulation, cyberspace communities might create quasi-state institutions to legislate and enforce norms, which could suffer from significant democratic deficits (N. Netanel, 2000).

Cyber-libertarians advocate minimal government intervention in cyberspace, promoting freedom and innovation. However, this approach can lead to regulatory gaps that exacerbate privacy, security, and inequality issues (Hart, 2001). Unregulated cyberspace may undermine liberal democratic ideals by failing to protect minorities and prevent discrimination. Effective governance requires balancing autonomy and regulation to uphold democratic principles (Simpson, 2012). Comparing cyberspace self-governance with traditional governance structures highlights the potential democratic deficits in both systems. Effective governance in cyberspace may require hybrid models that combine state regulation and community-based oversight (Ebaye, 2018).

Cyberspace self-governance poses significant challenges to liberal-democratic theory. Although it offers the potential for increased autonomy and innovation, it risks undermining key democratic principles. Selective state regulation combined with community oversight may offer a more balanced approach to governance in cyberspace. Han’s book contrasts Western liberal democratic models with China's one-party system, discussing online expression and

authoritarian resilience. This study critiques the effectiveness of liberal ideals in the Chinese context, highlighting the challenges of applying Western liberal principles universally (Han, 2018). The application of liberal democratic models to non-Western contexts is problematic. For instance, China's approach to cyberspace governance highlights the tension between liberal ideals and authoritarian practices.

5.7 China’s Approach to Cyberspace

"Contesting Cyberspace in China: Online Expression and Authoritarian Resilience" by Rongbin Han explores the dynamics of online expression in China and how the Chinese government maintains control over the internet. The book examines the balance between online freedom and authoritarian resilience, highlighting the complexities of Chinese Internet governance. The Chinese government has developed sophisticated mechanisms to control online expression while allowing sufficient space for public discourse to maintain its legitimacy. This balancing act helps the regime manage dissent and maintain stability. Han describes the use of censorship, surveillance, and propaganda to shape online discourse. The government's approach allows for some level of free expression, which serves as a safety valve to release social tensions (Han, 2018).

Han employs a "guerrilla ethnography" approach, gathering data from Chinese bulletin boards and university Internet forums. This method allows for an in-depth understanding of online interactions and government responses to digital dissent. He acknowledges the ethical concerns regarding his methodology but defends its effectiveness by citing similar research practices used by Harvard University scholars (Han, 2018). The book critiques the tendency of Western scholars to advocate a superior liberal democratic model when analyzing China's Internet governance. He argues that such perspectives can be myopic and fail to appreciate the achievements of China's one-party system. This analysis highlights the complexity of China's

approach to Internet governance and the limitations of applying Western liberal democratic ideals to the Chinese context (Han, 2018).

The Chinese government's control over cyberspace impacts various aspects of society, including freedom of expression, public opinion, and social stability. This account discusses how the government manages online content to prevent collective action and maintain control over public discourses. This approach helps the regime navigate the challenges posed by digital communication technologies (Han, 2018). Han's work is part of a broader examination of Internet governance in Asia, where various countries face similar challenges in balancing control and freedom.

The book "Access Contested" by Ronald J. Deibert et al. offered a comparative analysis of Internet censorship and surveillance across Asia, providing context for understanding China's approach within the region (Deibert et al., 2011). "Contesting Cyberspace in China" provides a comprehensive analysis of how the Chinese government manages online expression to maintain authoritarian resilience. The book highlights the complexities of Internet governance in China and critiques the application of Western liberal-democratic models to understand these dynamics.

5.8 Cyberspace across Cultures

Matusitz examines how cyberspace serves as a global village, facilitating interactions across diverse cultural backgrounds. This study emphasizes the creation of a second-order culture that differs from traditional physical interactions, highlighting both the unifying and divisive aspects of cyberspace (Matusitz, 2014). Cyberspace can both unite and divide based on cultural, ideological, and political differences. This facilitates the creation of new cultural norms that are distinct from those in physical spaces. His account offers an in-depth look at

how cyberspace serves as a global village, fostering interactions between users from diverse cultural backgrounds.

This updated examination explores the unifying and divisive potentials of cyberspace, emphasizing the creation of a new cultural order that is distinct from traditional face-to-face interactions. He contends that cyberspace functions as a global village, a domain where individuals from various cultural backgrounds can interact. This virtual space can unite and divide people based on ideological, political, historical, racial, or religious differences. Matusitz argues that cyberspace facilitates the creation of a second-order culture distinct from the synchronous exchange of symbols and sounds that occurs in physical space (Matusitz, 2014a).

The widespread use of digital devices and social media has made communication in digital spaces a crucial research area. Intercultural communication in cyberspace involves understanding how different cultural backgrounds influence online interactions. Xiao Ming's study emphasizes that intercultural communication in cyberspace creates a new area of exploration, highlighting the dynamic development of cyberculture in various social media platforms (Ming, 2022).

Electronic communication across cultures presents distinct challenges and opportunities. Cultural gaps can exist not only between individuals but also between individuals and dominant cybercultures. Chase et al. identified that cyberspace has its own culture, and miscommunication can arise due to the lack of non-verbal cues inherent in face-to-face interactions. This makes electronic communication a unique challenge in intercultural contexts (Chase et al., 2002).

Cyberspace allows for the creation of virtual communities in which traditional cultural boundaries can be maintained and transcended. McIlvenny explores how human

communication is envisaged in transcultural virtual communities and the role of graphical avatars in embodying virtual ethnicity, impacting identity, and community in cyberspace (McIlvenny, 1999). Authentic identity construction and community building are significant challenges in cyberspace. Individuals strive to create satisfactory or "authentic" identities in a largely text-based environment. Macfadyen importance (Macfadyen, 2006).

Developing intercultural communicative competence is essential for effective communication in cyberspace, particularly in educational contexts. (Orsini-Jones & Lee, 2018) discuss the role of cyber pragmatics in telecollaborative projects, emphasizing the importance of politeness and pragmatic rules in online communication. "Intercultural Perspectives on Cyberspace: An Updated Examination" highlights the complex interplay between cultural diversity and online interactions. Cyberspace creates new opportunities for intercultural communication while presenting unique challenges related to identity, community and miscommunication. Understanding these dynamics is crucial for fostering effective and meaningful interactions in the digital age (Matusitz, 2014b).

5.9 Cyberspace Governance

"The Governance of Cyberspace: Politics, Technology, and Global Restructuring" explores the multifaceted issues surrounding cyberspace governance, including surveillance, control, privacy, and the roles of various stakeholders. This volume discusses how cyberspace is governed and its implications for politics and global restructuring. Cyberspace is defined as a computer-generated public domain without territorial boundaries or physical attributes that is in constant use. The key question addressed is how this domain should be governed in the future. Loader identifies various perspectives on cyberspace governance, contrasting cyber-libertarians, who oppose government intervention, with more critical views that stress the dangers of digital realities created by computer technology (Loader, 2003).

Issues of surveillance, control, and privacy are central to the governance of cyberspace, influenced by state concerns regarding security, crime, and economic advantages. This volume explores these issues through debates on the desirability, form, and responsibility of agencies for Internet regulation, analyzing emerging discussions on surveillance, control, rights, and privacy (Loader, 2003).

5.9.1 Digital Divide

The digital divide and teledemocracy are critical topics that address inequalities in Internet access and the potential for digital technologies to enhance democratic participation. Carter discusses these themes in a case study on teledemocracy experiments in Manchester, England, illustrating the potential and challenges of using digital technologies for democratic engagement (Hart, 2001). States are increasingly asserting their interests in cyberspace governance, with non-democratic states becoming more influential in governance forums that were previously dominated by transnational networks of engineers.

Deibert and Crete-Nishihata discuss how Western liberal democracies are shifting from laissez-faire approaches to more state-directed control and regulation in cyberspace (Deibert & Crete-Nishihata, 2012). Effective cyberspace governance requires balancing state sovereignty with the fragmentation of cyberspace and debating multilateral governance and multi-stakeholders. Liaropoulos examines the power politics of cyberspace governance through cases like ITU, ICANN, IGF, and NETmundial, highlighting the complex interactions between states and the private sector (Liaropoulos, 2017).

There is a need to build confidence, capacity, and consensus among key stakeholders to ensure stability and predictability in international cyber relations. Jayawardane et al. discuss how freedom, openness, and security can be achieved in cyberspace through collaborative efforts and international cooperation (Jayawardane et al., 2016). Liberalist perspectives on

cyberspace highlight both the potential and challenges of leveraging digital technologies to promote democratic values and individual freedom. While cyberspace offers opportunities for enhanced participation and communication, it also necessitates regulatory frameworks to address issues of inequality, privacy and security.

5.9.2 International Cooperation in Cyberspace

Cyberspace, with its borderless nature, requires international cooperation to address common challenges and ensure a stable and secure digital environment for all. States have entered multilateral agreements to enhance cybersecurity. Examples include the Budapest Convention on Cybercrime and regional agreements, such as the ASEAN Cybersecurity Cooperation Strategy (Sari, 2024).

International cooperation involves sharing information on cyber threats, vulnerabilities, and the best practices. The European Union Agency for Cybersecurity (ENISA) plays a crucial role in facilitating cyber cooperation in the European Union. ENISA emerged as the EU's key agency for cybersecurity, working to acquire epistemic authority and carve out a specific role for itself in the complex landscape of cybersecurity governance (Dunn Cavelty & Smeets, 2023). The agency's mandate was significantly strengthened by the Cybersecurity Act, which established the EU Cybersecurity Certification Scheme to increase cybersecurity and build cyber resilience in the European Union’s Digital Single Market (Ananda et al., 2022).

ENISA's efforts to facilitate cooperation are evident in several initiatives. For instance, the agency is involved in developing the European cybersecurity certification framework by coordinating the establishment of specific cybersecurity certification schemes (Kohler, 2020). This framework aims to address the fragmentation of the EU’s cybersecurity landscape by creating cross-European interoperable solutions and EU mechanisms for certification. Additionally, ENISA supports the implementation of cybersecurity centers at the national level

and contributes to situational awareness models for decision makers (Leitner et al., 2017). ENISA's role in facilitating cyber cooperation is multifaceted and encompasses policy development, certification schemes, and support for national cybersecurity efforts.

However, it is important to note that ENISA's role is part of a larger whole and continues to evolve (Dunn Cavelty & Smeets, 2023). The agency's efforts contribute to the EU's broader strategy of increasing trust and security in ICT products, services, and processes while addressing the challenges of cross-border cybersecurity issues (Kohler, 2020).

5.9.2.1 Joint Cyber Exercises

`States participate in joint cyber exercises to improve coordination and response to cyber incidents. Examples include NATO's Cyber Coalition and the EU's Cyber Europe exercises. These exercises provide a realistic simulation environment for cyber defense teams to practice and improve their skills. In the 2022 NATO Cyber Coalition Exercise, teams were given objectives to accomplish while preventing others from doing the same, including monitoring a simulated power microgrid (Blakely et al., 2023). These exercises not only focus on technical performance but also incorporate behavioral-assessment techniques. The 2010 NATO-led cyber defense exercise utilized multiple methods to assess team effectiveness, including automated availability checks, exploratory sequential data analysis, and network intrusion detection system attack analysis (Granåsen & Andersson, 2016).

This multifaceted approach provides a comprehensive evaluation of cyber defense capabilities. These Cyber Coalition exercises contribute significantly to improving cyber incident response by providing realistic training environments, fostering collaboration among member states, and incorporating both technical and behavioral assessments. These exercises help NATO and its member states develop more effective cyber defense strategies, enhance their capabilities, and stay prepared for evolving cyber threats (Shea, 2017). The continuous

refinement of these exercises, based on lessons learned and emerging threats, ensures that NATO remains at the forefront of cyber defense.

5.9.2.2 Cyber Governance

Institutions such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Governance Forum (IGF) play critical roles in managing the technical infrastructure of the Internet and fostering multi-stakeholder dialogue. ICANN, established in 1998, serves as the overall technical manager and coordinator of the global domain name system (DNS), wielding significant authority in shaping Internet policy and institutional relationships. ICANN's policies drive the technical operations that form the Internet as we know it, making it a key player in Internet governance (Gunnarson, 2011). It implements governance mechanisms through the DNS, including authority, law, sanctions and jurisdictions (Klein, 2002).

The IGF, on the other hand, was established in 2006 as a non-binding multistakeholder forum to encourage deliberation on Internet governance issues (Nonnecke & Epstein, 2016). While it does not produce binding rules like ICANN, the IGF promotes discourse among various actors and potential solutions to Internet governance challenges (Pohle, 2019). Interestingly, despite their importance, both the ICANN and the IGF face criticism and challenges. The ICANN operates under U.S. jurisdiction, subjecting it to OFAC sanctions programs that can impede its global operations (Pérez Fernández, 2023). The IGF's role in mediating and coordinating international cooperation is contested, especially in light of the increasing digital sovereignty efforts of various countries (Pohle, 2019).

While the ICANN plays a more direct role in managing technical infrastructure through its authority over the DNS, the IGF contributes by facilitating discussions and consensus building among diverse stakeholders. Both organizations are crucial in addressing the complex,

transnational nature of Internet governance issues, although their effectiveness and reception vary across different regions and stakeholder groups (Levinson & Marzouki, 2015).

5.9.2.3 Norm Development

The UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security has proposed norms for cyber conduct. Since its inception in 2002, the GGE has worked to foster consensus on international cyber norms, with significant progress made in 2013 and 2015 (Raymond, 2019). The 2013 GGE report marked a breakthrough by reaching an agreement on the applicability of international law and existing norms to cyberspace, as well as proposing voluntary confidence-building measures to reduce risks and misperceptions (Kane, 2014).

Interestingly, GGE's progress has occurred despite deteriorating relations between major powers and increasing global contention over Internet governance issues. This success can be attributed to a conscious process of rule-making and interpretation structured by agreed-upon secondary rules, allowing consensus-building even when substantive preferences diverge (Raymond, 2019). However, the process has not been without challenges, as evidenced by the failure to reach a consensus in the 2017 GGE report (Gorwa & Peez, 2018). The UN GGE has been instrumental in shaping the normative environment for cyber risk management and contributing to the development of voluntary technical norms (Kulikova, 2021).

While progress has been made, ongoing efforts are required to address emerging challenges and effectively implement agreed-upon norms. The involvement of regional organizations and non-state actors in complementary initiatives may further enhance the global uptake of cyber norms and their practical implementation (Gorwa & Peez, 2018; Ott & Osula, 2019).

The United Nations Office on Drugs and Crime (UNODC) addresses cybercrime as part of its broader mandate to combat transnational, organized crime and terrorism. The UNODC recognizes cybercrime as a growing global threat that requires international cooperation and a coordinated response (Citaristi, 2022). The UNODC's approach to cybercrime involves research, technical assistance, and legal support. The office conducts research on cybercrime trends and their connections to other forms of crime, providing valuable insights for policymakers and law enforcement agencies (Citaristi, 2022). The UNODC also offers technical and legal assistance to member states to enhance their capabilities in investigating and preventing cybercrime.

Interestingly, the UNODC acknowledges the disproportionate impact of cybercrime on women and girls, especially in the least developed countries with rapidly increasing Internet usage but limited educational campaigns (Howell, 2016). The office emphasizes the need for contextually specific and strategically targeted regulatory frameworks to effectively address cybercrime (Howell, 2016). The UNODC's approach to cybercrime is multifaceted, involving research, capacity building, and international cooperation. The office recognizes the need for global regulations while acknowledging the challenges of developing such frameworks. The UNODC advocates collaborative efforts involving multiple stakeholders, from local police forces to transnational regulatory agencies, to effectively combat cybercrime (Howell, 2016).

5.10. Regional Organizations

5.10.1 European Union

The EU Network and Information Security (NIS) Directive and Cybersecurity Act work together to promote a unified approach to cybersecurity across the European Union. The NIS Directive, adopted in 2016, aims to establish a high common level of cybersecurity across EU Member States by requiring them to adopt national cybersecurity strategies and implement specific measures to protect critical infrastructure and digital service providers (Kulesza, 2021;

Wallis et al., 2021). It mandates information sharing on threats and best practices among operators and state agencies and introduces a standard of due diligence for critical infrastructure operators (Kulesza, 2021).

The Cybersecurity Act, proposed as a new regulation by the European Union Agency for Cybersecurity (ENISA), reinforces ENISA's role in implementing the NIS Directive (Markopoulou et al., 2019). This strengthens the coordination and cooperation between Member States in cybersecurity matters. The Act also complements the NIS Directive by establishing an EU-wide cybersecurity certification framework, further promoting a unified approach to cybersecurity standards across the EU (Markopoulou et al., 2019).

Interestingly, while the NIS Directive and Cybersecurity Act aim to unify cybersecurity approaches, their implementation has revealed several challenges. For instance, some Member States began adopting their own cybersecurity laws before the NIS Directive was fully implemented, potentially leading to inconsistencies in the application of EU data protection principles (Jasmontaite & Burloiu, 2017).

Additionally, the difficulty in implementing the original NIS Directive led to the development of the NIS2 Directive in 2022, which aims to address new threats and strengthen security requirements (Vandezande, 2023). The NIS Directive and Cybersecurity Act promotes a unified approach to cybersecurity in the EU by establishing common standards, encouraging information sharing, and strengthening ENISA’s role. However, challenges in implementation and the need for continuous adaptation to new threats highlight the ongoing nature of this process.

5.10.2 ASEAN Cybersecurity Cooperation

ASEAN has developed a regional cybersecurity strategy to enhance cooperation among member states and address cyber threats. The strategy includes initiatives for capacity building,

information sharing, and the development of regional norms for cybersecurity. ASEAN's approach reflects the liberalist ideals of regional cooperation, economic integration, and the establishment of common norms and standards.

ASEAN has recognized the growing importance of cybersecurity in the region and adopted a multifaceted approach to address cyber threats and promote digital resilience. The organization has experienced significant economic growth, with its GDP reaching over US$3.6 trillion by 2022, making it the fifth-largest economy globally (Sari, 2024). However, this digital transformation has also made ASEAN countries prime targets for cybercrimes, including online scams, data breaches, and cyberattacks.

Interestingly, ASEAN's approach to cybersecurity has evolved from its broader regional security cooperation strategies. Initially, the organization took a hesitant and incrementalist approach to formulating strategies for siloed regional issues, including transnational crime. However, there has been a significant shift towards the deliberate institutionalization of regional cooperation under the ASEAN Political-Security Community, created under the 2008 ASEAN Charter (Desierto, 2021). While ASEAN has made progress in addressing cybersecurity concerns, challenges remain in enhancing cooperation to combat cybercrime.

5.11 Case Study: Budapest Convention on Cybercrime

The Budapest Convention, adopted by the Council of Europe in 2001, was the first international treaty to address cybercrime. The convention provides a framework for harmonizing national cybercrime laws, facilitating international cooperation, and promoting information sharing among member states. The Budapest Convention exemplifies the liberal principles of international cooperation and institution building to address common challenges in cyberspace.

The Budapest Convention on Cybercrime, adopted by the Council of Europe in 2001, remains a significant landmark in multilateral governance of cybersecurity (Shires, 2023). It was designed to serve as a global framework to harmonize legislation, which is considered an important element in the fight against cybercrime (Gercke, 2011). The Convention has been diffused globally and serves as a benchmark or 'model law' for drafting national cybercrime legislation in many countries worldwide (Nguyen & Golman, 2020).

The Convention aims to address cybercrime challenges, but it does not specify the general provisions of substantive criminal law, such as the provisions on the minimum age of criminal responsibility (MACR) for cybercrime (Balajanov, 2018). This omission has led to discrepancies between national laws, potentially hindering international cooperation against cybercrime and creating safe havens for perpetrators below the MACRs. Additionally, the rapid growth in Internet use, particularly in Asia, has been accompanied by significant increases in cybercrime, amplifying the risks and challenges faced by law enforcement agencies (Broadhurst & Chang, 2012).

While the Budapest Convention has played a crucial role in establishing state-of-the-art, principle-based criminal law standards and important procedural rules (Wicki-Birchler, 2020), it faces ongoing challenges. These include concerns from non-EU countries regarding Article 32, which allows cross-border access to stored computer data under certain conditions (Matei, 2024). Addressing these concerns is crucial for ensuring that the Budapest Convention remains an effective tool for combating cybercrime in a fair, equitable, and respectful manner, especially in the face of evolving technologies and new forms of cybercrime (Marcella, 2021).

5.12 Policy Implications

Policymakers should support and strengthen international institutions that facilitate cooperation and governance in cyberspace. Continued efforts to develop and promote

international norms for responsible state behavior in cyberspace are essential to ensure global cybersecurity. Governments should engage with the private sector to leverage its expertise and resources to address cyber threats and promote cybersecurity. Policies that foster innovation and collaboration between the public and private sectors can enhance cyberspace resilience and security.

Providing technical assistance and capacity building to developing countries can help bridge the digital divide and enhance global cybersecurity. Collaborative efforts to build cybersecurity capabilities and share best practices can strengthen global resilience to cyber threats. The integration of cyberspace into liberalist theories of international relations highlights the importance of cooperation, international institutions, and economic interdependence in addressing the challenges and opportunities of the digital age. By examining the role of international organizations, regional cooperation, and the digital economy, this chapter demonstrates how liberalist principles can inform policies and practices for securing a secure and prosperous cyberspace. The insights gained from this analysis underscore the need for continued international collaboration and institution building to navigate the complexities of cyberspace in the 21st century.

CHAPTER-6

6. Cyberspace and Constructivism

Constructivism, a prominent theory in international relations, emphasizes the role of ideas, identities, norms, and social constructs in shaping international relations. Unlike realism and liberalism, which focus on material power and institutions, constructivism considers the social and ideational factors that influence state behavior and global interactions. This approach asserts that human interaction is primarily shaped by ideational factors, including widely shared or "intersubjective" beliefs, which construct the interests of purposive actors (Finnemore & Sikkink, 2001).

Unlike rationalist approaches that focus on material forces, constructivism argues that both ideational and material factors construct the world around us and the meanings we assign to it (Agius, 2022). This perspective has gained significant traction in the field, with some scholars suggesting that constructivism has replaced Marxism as the main paradigmatic rival of realism and liberalism (Dessler, 1999). Constructivism's emphasis on identity, norms, and culture provides alternative readings of security and international relations (Agius, 2022). It offers a distinct perspective that complements and challenges traditional theories of IR. By focusing on the social construction of security threats and the role of identity in international relations, constructivism has reshaped core debates in IR theory and offers a valuable framework for understanding complex international phenomena (Agius, 2022; Finnemore & Sikkink, 2001).

International relations are shaped by socially constructed realities, including norms, identities, and beliefs. This perspective, known as social constructivism, challenges the realist view of international relations by emphasizing the importance of shared ideas and social interactions in shaping state behavior (Agius, 2022; Bellamy, 2004). According to this

approach, the international system is not simply given but actively constructed through the interactions and shared understandings of its participants.

Social constructivism posits that norms, identities, and beliefs play crucial roles in determining state interests and actions. For instance, the identity of states can shape their national interests and influence their interactions with other actors in the international system (Agius, 2022). This is exemplified by the case of Central European states, whose interests are shaped by their membership in NATO rather than the other way around (Bellamy, 2004). Similarly, emotions can play a significant role in shaping national norms and identities, as seen in the case of Korean aid policy, where emotions such as national pride and a sense of global responsibility contribute to the construction of Korea's donor identity (Noh, 2023).

The social constructivist approach provides valuable insights into the complex dynamics of international relations. By focusing on the role of norms, identities, and beliefs, it offers a more nuanced understanding of state behavior and the formation of the international order. This perspective highlights the importance of cultural competence, sensitivity, and awareness of biases in policymaking to foster positive international relationships (B. E. Saaida, 2023). As the global landscape continues to evolve, understanding the socially constructed nature of international relations is increasingly crucial for effective diplomacy and policymaking.

6.1 Key Concepts in Constructivism

- **Social Constructs**

  International relations are shaped by socially constructed realities, including norms, identities, and beliefs.

- **Norms and Ethics**

  Norms govern state behavior and establish standards for appropriate conduct.

- **Identity**

  State identities, shaped by historical experiences and social interactions, influence foreign policies and international behaviors.

- **Inter-subjectivity**

  Shared understanding and collective meanings play a crucial role in shaping international outcomes.

6.1.1 Norms as Determinants of States' Conduct

Constructivists argue that norms play a crucial role in shaping state behavior and establishing standards for appropriate conduct in international relations. They emphasize how norms influence interactions between states and guide foreign policy decisions (Hirata, 2008; Percy, 2007). Norms are shared expectations or rules that define what is considered acceptable or appropriate behavior for states in the international system. Some scholars have expanded this perspective to include the concept of roles, in addition to norms and identity. Roles are viewed as sets of appropriate behaviors that emerge through interaction, providing states with a sense of structure and possible actions in international politics (McCourt, 2012).

This adds nuance to the constructivist understanding of how state behavior is constructed socially. Constructivists highlight the importance of norms in regulating state behavior and establishing standards of conduct. However, the field has evolved to consider various mechanisms through which norms influence state actions, including the interplay between international and domestic normative systems (Cortell & Davis, 2005), the role of argumentative persuasion and social learning (Checkel, 2001), and the impact of domestic politics and institutional contexts on norm compliance (Checkel, 1997). This multifaceted approach provides a more comprehensive understanding of how norms shape state behavior in the international arena.

6.1.2 Identity as a Determinant of State's Conduct

Identity plays a crucial role in shaping a state's foreign policy and international conduct. According to constructivist theory, a state's identity generates specific values and attitudes that determine its preferences for particular foreign policy options (Ashizawa, 2008). This causal mechanism demonstrates how identity functions as a source of a state's foreign policy decisions. The concept of state identity is particularly significant in determining a country's long-term foreign policy and overall positioning in the international system (Alaranta, 2023). For instance, the Kurdish identity has been identified as a determinant in almost all areas of Turkey's foreign policy, affecting its relations with neighbors, Western states, and institutions (Karakoç, 2010). Similarly, the formation of the US foreign policy identity in the 21st century has been influenced by power narratives and the redistribution of influence among various political forces (Tsyrfa, 2020).

Interestingly, there is a subtle analytical difference between national and state identity. While a change in national identity may not necessarily lead to significant changes in foreign policy, a transformation in state identity often results in a shift in a country's long-term foreign policy and its position in the international system (Alaranta, 2023). This highlights the complex nature of identity's influence on state conduct. Identity serves as a fundamental factor in shaping a state's behavior in the international arena. It informs and shapes foreign policy processes while being influenced by international structures (Vucetic, 2018). The impact of identity on state conduct is context-dependent and versatile, cautioning against overly deterministic approaches to its role in foreign policy and international relations (Ashizawa, 2008).

6.2 Constructivist Perspectives on Cyberspace

Cyberspace, with its dynamic and evolving nature, presents a unique arena for constructivist analyses. As a complex and evolving environment, it offers a rich landscape for

constructivist analyses of international relations. The dynamic nature of cyberspace, characterized by constant technological advancements and shifting social interactions, aligns well with constructivist perspectives that emphasize the role of ideas, norms, and social constructs in shaping reality (Ikwu, 2019; Venables, 2021).

The constructivist approach is particularly relevant for examining the multidimensional aspects of cyberspace. For instance, the 'Geo-Cyber' spatial correlation mapping framework proposed by (B. Jiang et al., 2024) demonstrates how geographic metaphors can be used to understand and represent the interplay between physical and virtual spaces. This aligns with constructivist ideas about the social construction of space and the importance of shared meanings in international relations.

Similarly, the study of cyber strategy and its implications for international security, as discussed in (W. Huntley & Shives, 2024), reveal the complexities of applying traditional theories to the cyber domain. This study highlights the need for a nuanced understanding of the offense-defense balance in cyberspace, which can be seen as a socially constructed concept influenced by various actors' perceptions and interpretations. This aligns with constructivist notions of how ideas and perceptions shape strategic realities.

Cyberspace provides a unique arena for constructivist analysis because of its fluid nature and the constant interplay between technological, social, and political factors. The evolving dynamics of cyberspace, as highlighted in (Ikwu, 2019; B. Jiang et al., 2024; Venables, 2021), offer fertile ground for examining how shared understandings, norms, and identities are constructed and reconstructed in this digital realm, making it an ideal subject for constructivist approaches in international relations theory.

6.2.1 Cyberspace and Constructivist Principles:

- **Norm Formation**
  Cyberspace is a critical domain for the formation and evolution of international norms, such as norms against cyber-attacks on civilian infrastructure.

- **Identity and Perception**

  State and non-state actors use cyberspace to shape identities and influence perceptions through information dissemination and cyber diplomacy.

- **Social Constructs in Cyberspace**

  The narratives and discourses surrounding cyberspace, including concepts such as cyber sovereignty and digital rights, reflect broader social constructs and power dynamics.

Cyberspace's influence on constructivist theory of international relations (IR) is profound, as it reshapes the understanding of identity, norms, and the social construction of reality within the international system. Constructivism posits that the international structure is not merely a product of material forces but is also shaped by social interactions, shared ideas and collective identities. The emergence of cyberspace has introduced new dimensions to these interactions, challenging traditional constructs and fostering the development of new norms and identities.

One of the key ways cyberspace influences constructivist theory is through the creation of new identities and communities that transcend national boundaries. Černý highlights that cyberspace serves as a space where individuals and groups can engage in social interactions that contribute to the formation of collective identity (Černý, 2021).

This phenomenon is particularly relevant in the context of global movements, where individuals can mobilize and organize across borders and challenge state-centric notions of identity and sovereignty. The ability of non-state actors to shape narratives and influence public opinion in cyberspace underscores the importance of social constructs in international relations. Moreover, cyberspace has become a platform for developing and contesting norms. Lantis and

Bloomberg (2018) discuss how cyberspace governance involves ongoing debates over norms and values, reflecting the dynamic nature of international relations.

The process of norm contestation in cyberspace illustrates how states and non-state actors negotiate and redefine acceptable behavior, which is a central tenet of constructivist theory. The emergence of norms around cybersecurity, privacy, and digital rights exemplifies how cyberspace is not only a battleground for power but also a space for the evolution of international norms. The concept of due diligence in cyberspace further illustrates the constructivist perspective on the evolving nature of state responsibility in the digital realm. The obligation of states to ensure cybersecurity and protect their citizens in cyberspace reflects a normative shift socially constructed through international dialogue and consensus.

This evolving understanding of state responsibilities highlights the role of social interactions in shaping international norms and practices, aligning with constructivist emphasis on the importance of ideas and identities in IR. Additionally, the interplay between state behavior and cyber capabilities demonstrates how constructivist theory can explain the motivations behind state action in cyberspace.

Manjikian notes that the colonization of the Internet by state actors reflects a blend of realpolitik and social constructs, where states seek to assert their influence while navigating the complexities of a digital landscape (Manjikian, 2010). This duality illustrates how states are not merely driven by material interests but are also influenced by the social meanings and identities constructed in relation to cyberspace. Furthermore, the emergence of cyber diplomacy as a distinct practice underscores the relevance of constructivism in understanding contemporary international relations.

Watanabe discusses how states are increasingly engaging in capacity building for cybersecurity, which involves not only technical measures but also the cultivation of diplomatic

relationships and norms (Watanabe, 2020). This shift towards cyber diplomacy reflects a broader understanding of security that encompasses social and political dimensions, aligning with the constructivist view that international relations are shaped by social interactions and shared understandings. Cyberspace significantly influences constructivist theory by reshaping identities, fostering norm development, and highlighting the social dimensions of state behavior in the digital realm.

The emergence of new forms of interaction and governance in cyberspace challenges traditional state-centric models and underscores the importance of social constructs in understanding contemporary international relations. As cyberspace continues to evolve, its implications for constructivist theory are likely to deepen, necessitating ongoing exploration of the interplay between technology, identity, and international norms.

6.2.2 Cyber Norms Development

Constructivist scholars focus on the development, contestation, and internalization of norms and ethical standards in cyberspace. These norms shape state behavior and establish expectations for responsible conduct in the digital realm.

- **UN Group of Governmental Experts (GGE)**

The UN GGE has proposed norms for responsible state behavior in cyberspace, including prohibitions on targeting critical infrastructure and encouraging international cooperation in incident response. The UN Group of Governmental Experts (GGE) has proposed norms for responsible state behavior in cyberspace, including prohibitions on targeting critical infrastructure. This effort reflects the growing recognition of the need for international cooperation to increase stability and security in cyberspace (Hitchens & Gallagher, 2019). The GGE's work has resulted in several key developments. In 2013, the group reached a consensus that existing international law applies to the military use of information and communication

technologies (ICTs). This was followed by the 2015 GGE report, which extended this consensus (Raymond, 2019). Notably, the GGE recommended eleven norms on responsible state behavior in cyberspace, including norm (f), which prohibits cyber operations that cause intentional damage or impairment to critical infrastructure (CI) (Adamson, 2019b; Haataja, 2022).

However, the implementation and interpretation of these norms face several challenges in practice. The concept of critical infrastructure is subjective, and there are uncertainties regarding how international law applies to state conduct in cyberspace (Haataja, 2022). Additionally, the failure of the 2017 GGE to build upon its previous work is seen by some as a breakdown of the institutionalized state-led cyber norms process (Gorwa & Peez, 2018). While the UN GGE has made significant progress in proposing norms for responsible state behavior in cyberspace, including protections for critical infrastructure, challenges remain in terms of their implementation and interpretation.

There is a need for states to develop more clarity about the relationship between international law and these norms, as well as how international law applies to cyber operations, particularly where critical infrastructure is targeted (Haataja, 2022). Future efforts may benefit from the increased involvement of regional organizations and interregional collaboration to enhance norm development and implementation (Ott & Osula, 2019).

- **Tallinn Manual**

The Tallinn Manual on International Law Applicable to Cyber Warfare provides guidelines on how existing international law applies to cyber operations, influencing the development of cyber norms. The Tallinn Manual provides guidelines on how existing international law applies to cyber operations and has significantly influenced the development of cyber norms. It offers a comprehensive restatement of international law

applicable in the cyber context, focusing on jus ad bellum and jus in bello (Beatty, 2020; M. N. Schmitt, 2016). The Manual attempts to clarify how existing international law applies to cyber operations, addressing issues such as the prohibition of the use of force and the right to self-defense in cyberspace (M. N. Schmitt, 2016; Tanodomdej, 2019).

While the Tallinn Manual claims to reflect lex lata (the law as it is) applicable to cyber operations, its drafting process and the composition of the experts involved have been questioned. Critics argue that the Manual is marked by NATO influence and overlooks the practice of other states engaged in cyber operations, potentially compromising its role in assisting the cognition of international law (Tanodomdej, 2019). Additionally, there appears to be limited support in actual state practice and opinio juris for certain key Rules in the Tallinn Manuals, with several states heavily engaged in cyber operations showing limited interest in promoting legal certainty regarding the regulation of cyberspace (Efrony & Shany, 2018).

The Tallinn Manual has made a significant contribution to the development of cyber norms by providing a framework for the application of existing international law to cyber operations. However, its influence is not without controversy, as evidenced by debates surrounding its drafting process and the limited state practice supporting some of its rules. As cyber technologies continue to evolve, the Manual's approach and its impact on the development of international cyber security law will likely remain subjects of ongoing discussion and refinement (M. N. Schmitt, 2022; Von Heinegg, 2013).

6.2.3 Contestation of Norms in Cyberspace

- **Diverging Interests**

States have different perspectives on cyber norms based on their strategic interests, leading to contestation and negotiation. For example, the concept of cyber sovereignty advocated by China and Russia contrasts with the open and free Internet championed by the United States and European countries. China and Russia have been actively contesting

international norms in cyberspace, particularly through their promotion of the concept of "cyber sovereignty." This approach emphasizes state control over the Internet and challenges the Western-led multistakeholder model of Internet governance (Lantis & Bloomberg, 2018). Both countries advocate greater government involvement in cyberspace management and push for a more state-centric approach to Internet governance (X. Gao, 2022; Khasanova & Tai, 2024).

Interestingly, while China and Russia are often perceived as sharing a similar model of authoritarian digital sovereignty, there are significant differences between their approaches. For instance, their data localization regimes differ in terms of institutional centralization, policy-making responsiveness, and economic drivers (Khasanova & Tai, 2024). Additionally, China's cyber norm-building efforts have evolved, with recent reforms suggesting the greater involvement of Chinese companies in Internet policies (Gao, 2022). The contestation of cyber norms by China and Russia has created a complex landscape of competing visions for governance in cyberspace. While both countries champion cyber sovereignty, their specific approaches and implementations vary significantly.

Moreover, the dichotomy between China's sovereignty-oriented approach and the more open approach of Western countries is becoming increasingly blurred, with some Western nations, particularly the EU, also emphasizing digital sovereignty in their policies (X. Gao, 2022). This evolving situation highlights the ongoing struggle to shape the future of global Internet governance and the potential for new norms to emerge in this critical domain.

- **Non-state Actors in Cyberspace**

Non-state actors, including tech companies, NGOs, and hacker communities, play a significant role in shaping and contesting cyber norms. Their influence highlights the multistakeholder nature of cyberspace governance. Cyberspace has empowered non-state actors, closing the capability gap between them and states in terms of their ability to impact

international peace and security. Some non-state actors now match or exceed the cyber capabilities of many states, making public international law increasingly relevant to their interactions (M. N. Schmitt & Watts, 2016). This shift has led to the multiplication of norm entrepreneurs in cyberspace, including major technology firms that leverage their digital products to reshape norms and become norm entrepreneurs in digital defense (Katagiri, 2021b).

The role of non-state actors in cyberspace is not limited to technology companies and benign actors. Violent non-state actors (VNSAs) have also adapted to the digital age, using cyberspace for propaganda and recruitment strategies, particularly targeting women (Karakuş & Ak, 2022). Additionally, cybercriminals and hacker groups have emerged as significant players, often collaborating with or being leveraged by nation-states for cyber warfare capabilities (Sigholm, 2013). The involvement of non-state actors in shaping cyberspace norms has created both opportunities and challenges.

While initiatives such as the Global Commission on the Stability of Cyberspace (GCSC) have made notable contributions to cybersecurity norm-making (Eggenschwiler, 2020a), the multiplication of norm entrepreneurs has also resulted in uncoordinated and sometimes conflicting interests (Katagiri, 2021b). This has made the process of establishing universally accepted norms in cyberspace more complex and contested, highlighting the need for more inclusive and coordinated efforts in cyberspace governance (Herbst & Jakobi, 2024; Novanto et al., 2021).

6.3 Ethics in Cyberspace

- **Digital Rights**

The ethical debate surrounding digital rights, such as privacy, freedom of expression, and access to information, is central to the governance of cyberspace. Organizations such as the Electronic Frontier Foundation advocate for the protection of digital rights in policymaking. Privacy concerns are paramount, with the need to protect personal data and digital identities

becoming increasingly critical as technology advances (Rascão, 2020; A. Sharma, 2023). The rapid evolution of digital platforms has raised crucial questions about safeguarding fundamental rights while balancing innovation and security needs (Allahrakha, 2023; A. Sharma, 2023).

Freedom of expression in cyberspace presents a unique set of challenges. While the Internet has expanded opportunities for communication, it has also introduced new regulatory hurdles, such as managing cybersecurity and digital data protection (Mammadrzali, 2020; Revizore & Šļakota, 2017). The tension between ensuring free speech and preventing the spread of inappropriate or misleading content remains a significant ethical dilemma (Sudi et al., 2024). This debate extends beyond personal data to infrastructure design, as exemplified by privacy issues in the Domain Name System (DNS). These less visible aspects of Internet architecture have profound implications for user privacy and highlight the complex interplay between technology and rights (Bradshaw & DeNardis, 2019).

Moreover, the metaverse introduces new ethical considerations regarding virtual property, identity, and socioeconomic impact, further complicating the governance landscape (Bhardwaj, 2024). Addressing these ethical challenges requires a multifaceted approach. This includes developing comprehensive legal frameworks, increasing user awareness, strengthening regulations, and creating technologies that support privacy and security of AI models. By prioritizing ethical considerations in digital journalism, social media, and emerging technologies, we can work towards cyberspace that upholds both individual rights and societal well-being.

- **Ethical Hacking**

The ethics of hacking and cyber operations, including the distinction between ethical hackers (who identify vulnerabilities to improve security) and malicious actors, are key areas of constructivist analysis. Constructivist analysis views ethical hacking in cyberspace as a socially constructed practice shaped by shared norms, values and identities within the

cybersecurity community. This perspective emphasizes the role of ethical hacking in shaping and reinforcing security practices. Ethical hacking is a proactive approach to cybersecurity that involves the authorized testing of information systems to identify vulnerabilities before malicious actors can exploit them (Dogra et al., 2024). From a constructivist standpoint, this practice reflects the shared understanding within the cybersecurity community that preemptive action is necessary to protect digital assets and maintain trust in online systems.

The constructivist lens highlights the evolving nature of ethical hacking and its impact on cybersecurity norms. As technology advances, the need for sophisticated ethical hacking techniques increases (Gupta, 2023). This ongoing evolution demonstrates how the practice is continuously reconstructed and redefined by the actors involved, reflecting changing perceptions of threats and security needs in cyberspace. The constructivist analysis of ethical hacking in cyberspace emphasizes its role in shaping the norms and practices of cybersecurity. It views ethical hacking not only as a technical practice but also as a socially constructed activity that reflects and reinforces shared understandings of security, trust, and responsibility in the digital realm. This perspective underscores the importance of ethical considerations and legal frameworks in guiding the practice of ethical hacking(Gupta, 2023; Hani et al., 2024), highlighting how these social constructs influence the development and application of cybersecurity measures.

6.4 Identity and Perception in Cyberspace

Cyberspace profoundly influences state identity and perceptions, affecting international relations and foreign policy.

6.4.1 Cyber Diplomacy

States use cyber diplomacy to protect their national identities and values. For example, Estonia, known for its digital innovation, promotes itself as a leader in e-governance and in cybersecurity. Cyber diplomacy has become a crucial tool for nations to safeguard their

interests in the digital world. For instance, the European Union employs a set of tools, including cooperation, diplomatic dialogue, and preventive measures, to address cyber threats (Dragomir, 2021). Similarly, Indonesia has adopted a multifaceted approach to cyber diplomacy, utilizing legal, cultural, technological, and diplomatic means to protect its interests against cyber threats (Iswardhana, 2021).

Although cyber diplomacy aims to promote peace and security, it can sometimes lead to tensions between nations. For example, China and the US are at odds over cybersecurity issues, highlighting the potential for conflict in cyberspace (Y. I. Maulana & Fajar, 2023). Additionally, there is a delicate balance between ensuring national security and protecting individual rights, as seen in Bangladesh's Cyber Security Act 2023, which has raised concerns about its impact on freedom of speech and privacy (Shamsad Binte Ehsan & Md. Najmus Saquib, 2024).

Cyber diplomacy plays a vital role in protecting national identity and values in the digital era. Nations are developing comprehensive strategies, such as the USA's National Infrastructure Protection Plan and the NIST Cybersecurity Framework (Abimbola Oluwatoyin Adegbite et al., 2023), to safeguard their interests. However, the evolving nature of cyber threats and the need for international cooperation present ongoing challenges. As cyber issues continue to gain prominence in diplomacy and international relations, nations must navigate the complex landscape of cybersecurity while striving to maintain their sovereignty and promote their values in cyberspace (Fang, 2018; Kello, 2024).

6.4.2 Public Diplomacy

Social media and digital platforms enable states to engage in public diplomacy and shape international perceptions and narratives. The use of Twitter and other platforms by state leaders exemplifies this trend. Digital platforms and social media have revolutionized public

diplomacy, offering new avenues for states to shape international perceptions and narratives. These tools enable governments to directly engage with foreign publics, influence global opinion, and manage their national image on a scale that was previously unattainable (R. Wang & Xu, 2023; Yarchi, 2024). The rise of digital diplomacy has transformed traditional diplomatic practices, allowing politicians and diplomats to craft their public image, enhance public relations, and engage voters more effectively (Cansever, 2024).

Digital diplomacy varies across platforms and contexts. For instance, Chinese diplomats employ different communication strategies on international platforms, such as Twitter, versus domestic platforms, such as Weibo, adapting their messaging to suit different audiences and goals (M. Li, 2024). This strategic use of social media serves both diplomatic objectives and aligns with domestic political agendas of the countries. Additionally, the use of hashtags and targeted messaging has become a crucial aspect of digital diplomacy, as seen in China's COVID-19 public diplomacy campaign and the Israeli-Palestinian conflict on TikTok (R. Wang & Xu, 2023; Yarchi, 2024).

While digital diplomacy offers unprecedented opportunities for states to shape their images and engage with global audiences, it also presents ethical challenges and potential pitfalls. The balance between transparency and confidentiality, as well as national interests versus public goods, remains a concern for practitioners (Z. A. Huang & Arceneaux, 2024). Moreover, the rise of confrontational diplomatic communication and the potential for digital disinformation pose significant challenges to the future of international relations (Duncombe, 2019; M. Li, 2024). As digital diplomacy continues to evolve, it will play an increasingly crucial role in shaping global perceptions and narratives, requiring careful strategic management and ethical considerations by diplomatic actors.

6.5 Influencing Perceptions

6.5.1 Information Warfare

States engage in information warfare to influence public opinion and political outcomes in other countries through various means, including social media manipulation, disinformation campaigns and psychological operations. This practice has become increasingly prevalent in the digital age, with a significant impact on international relations and domestic politics (Mitrović, 2018; Mugurtay et al., 2024). Russian interference in the 2016 US presidential election highlighted the potential impact of information warfare on a nation's political fate (H. Lin, 2020).

Similarly, China's "wolf warrior" statecraft employs public opinion warfare strategies to influence the attitudes, behaviors, and decisions of target entities globally (Chung, 2021). The scope of cyberspace weapons has expanded from physical networks to the cognitive information domain, with technologies such as public opinion guidance and cognitive intervention becoming the main development directions (L. Chen et al., 2022).

Information warfare has become a tradition in modern international relations, with states actively using it to break the will of opponents, subject consciousness to their will, and achieve foreign policy objectives (Kanet, 2024; Manoilo* et al., 2019). The effectiveness of social media in modern warfare has made it a force multiplier, leading many countries to strengthen research on fundamental cognitive theories and deploy weapons directed at social network users for incident reconnaissance, sentiment analysis, and active intervention (L. Chen et al., 2022). As this trend continues, it poses significant challenges to national security and international stability, necessitating the development of countermeasures and legal mechanisms to address these evolving threats (Sheremet et al., 2021; Shibaev & Uibo, 2016).

6.5.2 Cyber Propaganda

The spread of propaganda and disinformation through cyberspace affects perceptions and can escalate such tensions. Constructivist scholars analyze how propaganda and disinformation in cyberspace significantly impact perceptions, shape narratives, and influence international relations by exploiting identity-based differences and manipulating public opinion. The COVID-19 pandemic intensified the spread of aggressive information campaigns aimed at managing perceptions, with some activities linked to state or state-sponsored actors (Milewski, 2020). These campaigns often employ "identity propaganda," which strategically targets and exploits identity-based differences to maintain hegemonic social orders (Reddi et al., 2023).

While concerns over disinformation have intensified, some argue that its effectiveness in changing foreign policy alignments, and the balance of power is limited. Drawing on neoclassical realism, it is suggested that international anarchy induces uncertainty and skepticism, especially between adversaries, making it challenging for disinformation campaigns to overcome partisan and ideological attachments (Lanoszka, 2018).

However, this view contradicts the widespread belief that disinformation shapes public opinion and influences policymaking. The impact of propaganda and disinformation in cyberspace on international relations is thus multifaceted. While some argue for its limited effectiveness in changing foreign policy, others emphasize its potential to undermine democratic discourse, manipulate elections, and increase societal conflicts (Mareš & Mlejnková, 2021).

The use of disinformation as a geopolitical tool in the struggle for power and status in the international community highlights its centrality in managing international relations and its ability to influence global public discourse (Battista, 2023). As cyberspace continues to

intersect with international relations, understanding these dynamics is crucial for policymakers and scholars alike (AkyeşiLmen, 2024).

6.6 Social Constructs in Cyberspace

The narratives and discourses surrounding cyberspace reflect broader social constructs and power dynamics.

6.6.1 Digital Rights and Freedoms

The discourse on digital rights is rooted in broader human rights principles that advocate for privacy, freedom of expression, and access to information. The United Nations Human Rights Council has recognized Internet access as a human right. These rights are increasingly recognized as fundamental in the context of modern technology and the Internet (Rascão, 2021; Siddiqui et al., 2024).

Digital technologies have disrupted the foundations of human rights, necessitating a reevaluation of how these principles apply in the digital age (Susi, 2019). The right to privacy, freedom of expression, and access to information are particularly affected by digitalization, as they intersect with issues such as surveillance, data breaches, and the digital divide (Boratalievich, 2024; Siddiqui et al., 2024). The Internet has become a crucial platform for exercising these rights, but it also presents new challenges in terms of regulation and protection (Mammadrzali, 2020; Rascão, 2021).

The constructivist approach to digital rights emphasizes the need for an integrated, interdisciplinary approach to ensure respect for human rights in the digital era. This includes strengthening public control, increasing the transparency of technological processes, and fostering international cooperation in regulation and standardization (Boratalievich, 2024).

Additionally, the discourse recognizes the importance of viewing digital rights not just as liberty rights, but also as welfare rights, placing duties on governments to provide access to information and protect digital freedoms (Mammadrzali, 2020; Mathiesen, 2008). As technology continues to evolve, constructivist discourse on digital rights will likely continue to adapt, seeking to balance the benefits of digital innovation with the protection of fundamental human rights.

6.6.2 Security and Rights Tradeoff

Tensions arise between security measures and digital rights, such as surveillance practices justified by national security concerns. Constructivist scholars analyze the tensions between security measures and digital rights by examining how norms, discourse, and social constructions shape perceptions and justifications of surveillance practices. They argue that the relationship between security and democracy is shaped by disputes and critiques in practice rather than fixed logics (Aradau & Mc Cluskey, 2021). This approach allows us to understand how certain arguments for surveillance become accepted as common sense while others are deemed unacceptable. For instance, justifications of surveillance for security often enact a "rise in generality," while critiques based on democratic claims are seen as a "descent into singularity" (Aradau & Mc Cluskey, 2021).

Constructivists also highlight how perceptions of the Internet have shifted over time, from being seen as a tool for democratization to a space that requires control and surveillance (Schulze, 2018). This change in norms reflects a perceived loss of state control and the establishment of a "norm of control" in both democratic and non-democratic states. The militarization of cyberspace is considered a result of this normative shift in international order. Constructivist analysis reveals that the effects of security-based justifications for surveillance vary across political contexts.

While such justifications are more effective in liberal democracies, they may be viewed with suspicion in autocratic countries (Antoine, 2022). This challenges the assumption that security arguments universally outweigh privacy concerns. Constructivist scholars emphasize the importance of examining how security measures and digital rights are socially constructed and contested in literature. They highlight the need for a more nuanced understanding of how surveillance practices are justified and resisted, considering the complex interplay between state power, technology and public perceptions.

6.7 Case Studies

6.7.1 The UN Group of Governmental Experts (GGE) on Cyber Norms

The UN GGE brings together experts from different countries to discuss and propose norms for responsible state behavior in cyberspace. The GGE's recommendations, including norms against attacking critical infrastructure and promoting cooperation, influence international discussions and policies. The UN Group of Governmental Experts (GGE) on cybersecurity demonstrates how international norms emerge through dialogue and consensus building among states.

The GGE process has facilitated negotiations and debates on responsible state behavior in cyberspace since the early 2000s, gradually developing a shared understanding of key issues (Pauletto, 2020). The 2013 GGE report marked a significant breakthrough, with states reaching an agreement on applying international law and principles, such as state sovereignty, to cyberspace, as well as confidence-building measures to reduce risks (Kane, 2014).

This consensus was further extended in the 2015 GGE report, reflecting an emerging alignment of governance arrangements for cyberspace despite broader geopolitical tensions (Raymond, 2019). The GGE's success in norm development has occurred alongside and sometimes in tension with other cyber governance efforts. While the GGE has made progress

on high-level norms, challenges remain in translating these into operational implementation (Pauletto, 2020).

Additionally, some argue that there is a disconnect between aspirational global cyber norms and the practical cybersecurity issues faced by states domestically (Sabbah, 2018a). The GGE exemplifies how dialogue can foster shared meanings and collective understanding of complex international issues.

However, its achievements highlight the ongoing challenges in developing and implementing global cyber norms. This process demonstrates both the potential and limitations of consensus-building approaches in shaping the normative environment for state behavior in cyberspace (Kulikova, 2021).

6.7.2 Russia's Information Warfare in the 2016 US Presidential Election

Russian interference in the 2016 US presidential election allegedly employed a sophisticated combination of cyber operations and social media manipulation to influence its outcome. The Russian cyber disinformation campaign exploited racial divisions in the United States, undermining public confidence in American electoral processes and institutions (D. E. W. Johnson, 2019). This campaign involved the covert use of social media accounts and online properties impersonating Americans for manipulation purposes (Francois & Lin, 2021). This interference was not limited to online activities. Russian operatives have utilized a broad spectrum of tools, including television and social media, to spread propaganda relentlessly (Dylan et al., 2020).

The campaign involved hacking high-profile U.S. political organizations and subsequent information dumps, allegedly aimed at helping then-candidate Donald Trump win the presidential election. Interestingly, while often described as 'disinformation,' a semantic network analysis of the Russian-orchestrated social media campaign revealed that the

information utilized was generally factually correct, and African Americans, rather than white conservatives, appeared to be the primary target demographic (Vićić & Gartzke, 2024).

Russian interference in the 2016 US presidential election allegedly employed a multi-faceted approach, combining cyber operations with sophisticated social media manipulation. This campaign exposed vulnerabilities in the US electoral system and highlighted the potential for foreign actors to exploit social divisions for political gains. This incident led to increased scrutiny of foreign influence in elections and prompted discussions about the need for enhanced cybersecurity measures and media literacy to combat such threats in the future (Eichensehr, 2021). These cases illustrate the role of narratives and perceptions in international relations, showing how states use cyberspace to shape their identities and influence political landscapes.

6.8 Policy Implications

The integration of cyberspace into constructivist theories of international relations has significant implications for understanding global politics and security dynamics in the digital era. Constructivism emphasizes the role of ideas, norms, and social interactions in shaping international relations, and cyberspace provides a new arena for these processes to unfold (Choucri & Clark, 2012b; Yau, 2018). The emergence of cyberspace challenges traditional notions of state sovereignty and power as it transcends physical borders and creates new forms of interaction between state and non-state actors (AkyeşiLmen, 2024; Choucri, 2015).

This shift requires a reevaluation of how identities, norms, and interests are constructed and negotiated in the international system. Constructivist approaches can help explain how cyber-related concepts such as cybersecurity, cyberwar, and cyber diplomacy are socially constructed and how they influence state behavior (Barrinha & Renard, 2017a; Choucri & Goldsmith, 2012b). However, the relationship between cyberspace and international relations is not unidirectional. While technology can shape political outcomes, Taiwan's case

demonstrates that politics can also influence the development and use of technology in cyberspace (Yau, 2018). This co-evolution of cyberspace and international relations presents both challenges and opportunities for constructivist theories to explain the emerging patterns of conflict, cooperation, and power dynamics in the digital realm (Choucri, 2014).

Integrating cyberspace into constructivist theories of international relations allows for a nuanced understanding of how digital technologies reshape global politics. This highlights the need for adaptive strategies and new conceptual frameworks to address the complex interplay between cyber capabilities, state interests, and international norms (AkyeşiLmen, 2024; Choucri, 2015). As cyberspace continues to evolve, constructivist approaches provide valuable insights into the social construction of cyber-related concepts and their impact on international relations.

The integration of cyberspace into constructivist theories of international relations highlights the importance of norms, identities, and social constructs in shaping global interactions during the digital age. By examining norm development, identity formation, and the influence of narratives, this chapter demonstrates how constructivist principles can inform policies and practices for creating a secure and cooperative cyberspace. The insights gained from this analysis underscore the need for continued dialogue, engagement, and ethical considerations to navigate the complexities of cyberspace in the 21st century.

CHAPTER-7

7. Overarching Cyber-Responsive Policies

The integration of cyberspace into international relations theories has profound implications for policymaking at the national and international levels. These implications span various areas, including national security, international cooperation, digital rights, and cyber governance issues.

7.1 Comprehensive Cybersecurity Strategies

States must develop and implement comprehensive cybersecurity strategies that encompass prevention, detection, response, and recovery measures. These strategies should integrate cyber capabilities into broader national-security frameworks. Developing comprehensive cybersecurity strategies is crucial for protecting information, financial, and reputational assets from increasingly sophisticated cyberattacks.

A well-rounded approach integrates various components, including strategic planning, staff training, technological advancements, and collaboration with external entities. Integrating cybersecurity into strategic management is essential for addressing modern cyber threats. Key aspects include incorporating cybersecurity into strategic planning, staff training, and collaboration with external entities (Labazanova et al., 2023). A holistic approach to developing the cybersecurity workforce involves integrating educators, career professionals, employers, and policymakers to create comprehensive solutions (Hoffman et al., 2012).

Cybersecurity strategies must be tailored to specific sectors. For example, higher education institutions require unique approaches because of their open and decentralized networks (Alexei, 2021). National cybersecurity strategies, such as those implemented in the USA, provide frameworks and initiatives for protecting critical infrastructure, emphasizing public-private partnerships and international collaborations (Adegbite et al., 2023).

Leveraging AI for cybersecurity enhances threat detection, predictive analysis, and automation. AI technologies, such as machine learning and natural language processing, are critical for modern cybersecurity solutions (Sangarsu, 2023). Effective cybersecurity risk management involves understanding the threat landscape, conducting risk assessments, implementing mitigation strategies, and maintaining ongoing monitoring (Parsola, 2023). A comprehensive cybersecurity strategy is multifaceted and incorporates strategic management, workforce development, sector-specific approaches, national and international policies, AI integration, and robust risk management. These elements collectively ensure a resilient defence against cyber threats.

7.2 Cyber Defense and Resilience

Investing in robust cyber defenses and resilience measures is crucial for protecting critical infrastructure and mitigating the impact of cyberattacks. This includes both technical measures and enhancing the cyber literacy of the workforce. In the digital age, cyber defense and resilience are crucial for protecting critical systems and infrastructure from increasingly sophisticated cyberattacks. Developing a robust framework for cyber defense and resilience involves integrating various strategies, technologies, and practices to ensure the continued functionality and recovery of systems that are under attack. Managing cyber-resilient systems involves understanding the unique challenges of different industries and implementing managerial actions tailored to specific contextual factors (Annarelli et al., 2020).

A comprehensive systems engineering approach is crucial to ensure resilience in cyber-physical systems. This framework should focus on integrating security measures that address vulnerabilities across multiple domains, including physical, informational, cognitive, and social aspects (DiMase et al., 2015). Integrating cybersecurity and cyber defense practices enhances overall cyber resilience by ensuring protection against adversarial actions and maintaining critical infrastructure security (Galinec & Steingartner, 2017). However,

overregulation can increase stress and vulnerability within organizations. A balanced regulatory approach that considers human factors is necessary for effective cyber resilience (Gisladottir et al., 2017).

Cyber-physical system resilience requires preparation for, absorption of, recovery from, and adaptation to malicious cyber incidents while sustaining essential operations even during attacks (Segovia-Ferreira et al., 2023). Resilience involves not only technological responses but also organizational practices, such as backup plans, additional equipment, and budgeting for unexpected events, integrating concepts from evolution and game theory (Gould, 2019). Cyber defense and resilience require a comprehensive approach that integrates strategic management, cyber-physical security, balanced regulation and organizational practices. This comprehensive approach ensures that systems can resist, bounce back from, and evolve in response to cybersecurity challenges, preserving essential functions even under unfavorable circumstances.

7.3 Public-Private Partnerships (PPP)

Governments must establish robust collaborations with private entities, as they control and manage a substantial portion of vital infrastructure and possess considerable cybersecurity expertise. The exchange of threat intelligence and synchronized response strategies relies heavily on effective cooperation between the public and private sectors. Collaboration between government and private entities in the realm of cybersecurity is essential for tackling the intricate issues presented by digital threats. These joint efforts combine the capabilities of both sectors to improve cybersecurity protocols, safeguard vital infrastructure, and develop comprehensive cyber defense plans.

Public-private cybersecurity involves the private sector taking on quasi-governmental roles in key cybersecurity issues, while the government acts as a market participant. This

system faces challenges in maintaining public law values, such as accountability and transparency (Eichensehr, 2016). There is a serious disconnect in expectations between governments and the private sector in PPPs, particularly regarding critical infrastructure protection and accountability (CARR, 2016). A successful cybersecurity PPP requires trust, clear legislative guidance, autonomy at the local level, and involvement from all organizational levels and the public (Manley, 2015). European PPPs in cybersecurity aim to stimulate competitiveness and innovation in the digital security industry, focusing on trust, privacy, and critical infrastructure protection (Olesen, 2016).

The US Financial Services Sector has developed a model for addressing cybersecurity through PPPs, focusing on information sharing, policy coordination, and threat analytics (Atkins & Lawson, 2021b). India's approach to PPPs in cybersecurity highlights the role of trade associations in developing templates, monitoring industry behavior, and enforcing laws, given the government's resource and expertise limitations (Kshetri, 2015). Public-private partnerships in cybersecurity governance, as seen in the EU, involve agencies like ENISA and EUROPOL working with private IT security companies, although these partnerships require more public transparency and critical reflection (Bossong & Wagner, 2016).

The NIST Cybersecurity Framework in the US is an example of a PPP fostering initiative that provides standards and guidelines to support national cybersecurity efforts (Ponnusamy et al., 2020). Balancing the differing missions and risk assessments of government and private sector partners is essential for the success of PPPs. Governments should compensate private entities for cybersecurity investments that align with national defense objectives (Clinton, 2011). Expanding PPPs to include personal-level considerations in IoT security requires advancements in technology, policy, and societal awareness (Diehl & Hare, 2018).

Public-private partnerships are vital for enhancing cybersecurity through collaborative efforts between the government and private sectors. Effective PPPs require trust, clear guidelines, sector-specific approaches, and balanced governance to address the evolving landscape of cyberthreats.

7.4 Strengthening International Norms

Thus, developing and promoting international norms for state behavior in cyberspace is critical. States should actively participate in forums such as the United Nations Group of Governmental Experts (GGE) and the Open-ended Working Group (OEWG) to build consensus on norms and principles. Strengthening international norms in cybersecurity is essential to address the global and interconnected nature of cyberattacks. Establishing effective norms helps create a stable and secure cyberspace by guiding state and non-state actors in their behavior and responses to cyber incidents. A shift from aspirational norms to practical, incremental, and bottom-up processes is suggested in this study. This approach involves discussions among cybersecurity regulators and authorities, creating common understanding and legal interoperability that can be scaled up globally (Sabbah, 2018b).

Countries approach international cybersecurity capacity building (CCB) assistance based on their normative structures. For instance, Japan prioritizes security-dominant interests, while South Korea focuses on developmental interests, highlighting the fragmentation of global cyber norms (Bimantara & Kunci, 2022). International law plays a crucial role in establishing such norms. Customary international law, treaties, and preventive obligations form the basis of cybersecurity governance, ensuring that states adhere to common standards (Kettemann, 2017). Drawing parallels from successful environmental agreements, such as the Montreal Protocol, can provide insights into creating effective cyber security norms. These models emphasize cooperation, compliance, and the use of incentives to address global challenges (Kasper & Krasznay, 2019).

Technology companies act as norm entrepreneurs and significantly influence global cybersecurity norms. Companies such as Microsoft engage in corporate diplomacy and lobbying to shape international cybersecurity policies (Hurel & Lobato, 2018). Cybersecurity capacity building can lead to fragmented norms if driven by donor states' geopolitical interests rather than collaborative international efforts. This hinders the development of cohesive global norms (Homburger, 2019).

Organizations outside the government, such as the Global Commission on the Stability of Cyberspace (GCSC), play a crucial role in developing cybersecurity norms by offering recommendations and frameworks for ethical conduct in the digital realm (Eggenschwiler, 2020b). The international law of cybersecurity faces a crisis due to states' reluctance to commit to binding treaties and specific legal interpretations. This has led to a reliance on non-binding norms and initiatives by non-state actors (Mačák 2016).

Strengthening international norms in cybersecurity requires a multifaceted approach involving incremental processes, comparative normative practices, the engagement of private companies, and the active role of non-state actors. By leveraging these strategies, the international community can develop cohesive and effective cybersecurity norms to address global cyberthreats.

7.5 Multilateral Agreements

States should work towards multilateral agreements that address specific aspects of cyberspace, such as cybercrime, data protection, and cyber warfare. The Budapest Convention on Cybercrime serves as a model for international cooperation in the fight against cybercrime. Multilateral agreements on cybersecurity are essential for addressing global cyber threats and enhancing international cooperation. These agreements facilitate collaboration among nations, set common standards, and ensure coordinated responses to cyber incidents. Diverging

conceptualizations and political systems among major cyber powers hinder effective multilateral cooperation. This gridlock in cybersecurity governance is rooted in these fundamental differences (Urgessa, 2020). Japan enhances its cybersecurity through international cooperation, particularly with ASEAN, by addressing cyber threats through multilateral agreements such as the RCEP and CPTPP (Melkonyan, 2022).

The Central European Cyber Security Platform (CECSP) exemplifies effective multilateral cooperation, highlighting the achievements and challenges of cross-border information sharing (Tikos & Krasznay, 2022). Multilateral agreements are vital for strengthening global cyber security. Despite these challenges, effective collaboration through bilateral treaties, strategic partnerships, and international legal frameworks can enhance cyber resilience and promote a secure cyberspace.

Multilateral agreements are vital for strengthening global cyber security. Despite these challenges, effective collaboration through bilateral treaties, strategic partnerships, and international legal frameworks can enhance cyber resilience and promote secure cyberspace. The UN's dual-track system and regional collaborations are essential for establishing an international cyberspace order. Multilateralism is crucial for developing comprehensive cyber governance (Guan, 2023).

7.6 Bilateral Arrangements for Cybersecurity

Bilateral Investment Treaties (BITs) for cybersecurity can enhance cybersecurity by protecting trade secrets and promoting cyber peace. The U.S.-China BIT negotiations illustrate how such treaties can serve as interim steps or alternatives to multilateral initiatives (Shackelford et al., 2014). The EU has developed strategic cyber partnerships with key countries to enhance bilateral cooperation, develop its cyber and diplomatic capabilities, and strengthen global Internet governance (Renard, 2018). Bilateral negotiations between the U.S.

and China face significant obstacles due to mutual distrust and differing strategic interests. This limits the potential for meaningful agreements on cybersecurity (J. Lewis, 2021). International law also plays a crucial role in regulating cybersecurity through multilateral agreements, bilateral treaties, and legislative resolutions by international organizations (Milik, 2021).

7.7 Digital Rights and Freedoms in Cyberspace

Policies should balance cybersecurity measures with the protection of digital rights, such as privacy and the freedom of expression. This includes establishing legal frameworks that regulate surveillance practices and ensure transparency and accountability. In the digital age, protecting privacy and freedom of expression is crucial to cybersecurity. These fundamental rights often face challenges due to cyber threats, surveillance, and other regulatory measures. Balancing security with these rights requires careful consideration and the development of robust legal frameworks.

The intersection of privacy and freedom of expression in cyberspace presents unique challenges to researchers. The lack of specific data protection legislation in countries such as India highlights the need for comprehensive cyber laws that protect privacy and freedom of expression while addressing cybercrimes (I. Sharma & Alam, 2016). The protection of privacy, freedom, and autonomy of Internet users in the context of democracy in the digital age emphasizes the importance of ethical and legal safeguards. Laws at both domestic and global levels must safeguard individuals' privacy rights and their ability to express themselves freely (Rascão, 2020).

Through initiatives such as the General Data Protection Regulation (GDPR), the European Union has established stringent privacy safeguards for cybersecurity. These measures guarantee the secure transmission of data and safeguard individual rights, providing a benchmark for other parts of the world (Dunaj, 2023). The EU Cybersecurity Act represents a

normative shift towards prioritizing user control over personal data. European courts are increasingly upholding data protection rights and influencing cybersecurity policies to balance data security with freedom of expression (Duić & Petrašević, 2023).

The US prioritizes freedom of expression, whereas Europe emphasizes privacy. This difference impacts the level of human rights protection in cyberspace, highlighting the need for international legal standards that balance these rights (Kittichaisaree, 2017). The German discourse post-Snowden highlights the tension between privacy and security. Government and parliamentary discussions often frame cybersecurity and data protection as conflicting priorities, reflecting broader global debates (Dimmroth & Schünemann, 2017).

Cybersecurity measures often impact human rights, such as the freedom of expression and privacy. Effective cybersecurity policies must balance these rights while protecting against cyberthreats (Cavelty & Kavanagh, 2019). Protecting privacy and freedom of expression in cybersecurity requires robust legal frameworks, international cooperation, and a balance between security and human rights. Ensuring these protections is essential for maintaining trust and safeguarding democratic values in the digital era.

7.8 Ethics in the Cyber Realm

Establishing ethical standards for cyber operations, including clear distinctions between legitimate and malicious activities, can help build trust and promote responsible behavior. Ethical guidelines should be developed in consultation with diverse stakeholders, including civil society and the private sector. Ethical standards in cybersecurity are vital to ensure that cybersecurity practices respect human rights, privacy, and ethical responsibilities of professionals. Current governance in cybersecurity ethics faces challenges, especially in differentiating between academic research and corporate practices. Ethical oversight varies

significantly, and there is a need for comprehensive ethics education and effective codes of conduct (Macnish & Ham, 2020).

Analyzing cybersecurity issues requires consideration of multiple ethical frameworks. Two key approaches include the principlist framework outlined in the Menlo Report and the rights-based principle that has a significant influence on European Union legislation (Bailey et al., 2012). These ethical structures address both the probabilistic nature of cybersecurity risks and the ethical implications of risk (Loi & Christen, 2020). The field of cybersecurity leadership suffers from insufficient regulatory oversight and a lack of ethical guidelines. To address this issue, Cleveland and Spangler (2018) suggested a global framework of ethical principles for cybersecurity executives to foster confidence in organizations that manage user data. Ethics should be a foundational consideration in cybersecurity.

The CSEC 2017 model outlines ethical factors that should be integrated into cybersecurity responses to ensure that they are built on solid ethical grounds (Shoemaker et al., 2019). Mapping the Cybersecurity Body of Knowledge (CyBOK) to ethical concerns reveals specific ethical challenges across different areas of cybersecurity. Detailed guidance based on these mappings can help professionals navigate ethical dilemmas in their fields (Flechais & Chalhoub, 2023).

A principlist ethical approach to cybersecurity is introduced, encompassing key values such as doing good, avoiding harm, respecting individual choice, fairness, and transparency. This ethical framework serves as a tool for comprehending and addressing moral challenges across various cybersecurity scenarios (Formosa et al., 2021). Ethical considerations in cybersecurity research require more attention. A framework for evaluating ethical and privacy considerations in research helps ensure that studies are conducted ethically (Davis et al., 2018).

Translating ethical principles into practical guidelines for Ethics Review Boards is essential. A set of self-assessment questions and a Coordinated Vulnerability Disclosure procedure can help embed ethical considerations in cybersecurity research (Reidsma et al., 2023). Establishing and adhering to ethical standards in cybersecurity are crucial for protecting human rights, ensuring privacy, and maintaining trust in digital systems. These standards guide both research and practical applications, ensuring that cybersecurity measures are ethically and socially responsible.

7.9 Cyber Governance

Effective cyber governance requires the involvement of multiple stakeholders, including governments, international organizations, the private sector, and civil society. Multistakeholder forums, such as the Internet Governance Forum (IGF), provide platforms for inclusive dialogue and decision-making. Inclusive multi-stakeholder governance in cybersecurity is essential for addressing the complex and global nature of cyberthreats. This approach involves collaboration among various stakeholders, including governments, the private sector, civil society, and international organizations to develop and implement effective cybersecurity policies and practices. Cybersecurity management must adapt to address the global and interlinked nature of digital threats. This necessitates a collaborative approach that emphasizes shared accountability, adaptability, and public engagement. Such an approach should be implemented within a diverse stakeholder structure that incorporates consultative methods, establishes standards, and enacts laws (Pernice, 2018).

Current governance mechanisms often involve private actors who voluntarily internalize externalities through the network governance. These mechanisms, while not always sufficient, represent a starting point for improving cybersecurity governance through multi-stakeholder collaboration (Eeten, 2017). A comprehensive model addressing key aspects such as strategy, standardized procedures, regulatory adherence, top-level management supervision,

and resource allocation is essential for successful cyber security governance. Ongoing assessment and analysis of these critical elements are vital for maintaining their effectiveness (Yusif & Hafeez-Baig, 2021).

7.10 Multi-Stakeholder Internet Governance

The concept of multi-stakeholder governance is both practical and performative in Internet governance. This model aims for inclusivity and bottom-up policy-making, despite the challenges in achieving genuine global representation and improved outcomes (Hofmann, 2016). For multistakeholder governance to be effective, it must offer the meaningful inclusion of diverse stakeholders. The criteria for such inclusion involve transparency, accountability, and genuine participation from all affected parties (Malcolm, 2015). To effectively combat the ever-changing landscape of cybersecurity threats, a flexible and responsive governance structure is essential. This approach should encompass elements such as collaboration between the public and private sectors, cooperation at both regional and global levels, and adherence to legal and regulatory requirements (Melaku, 2023).

Governance plays a critical role in sustaining cybersecurity in business corporations. A comprehensive approach includes technical, organizational, and social measures to protect trade secrets and ensure business continuity (Alashi & Badi, 2020). Inclusive multi-stakeholder governance is crucial for effective cyber security. By involving diverse stakeholders in policymaking and implementation, we can develop comprehensive strategies that address the global and interconnected nature of cyberattacks.

7.11 Regulatory Frameworks

It is crucial to establish regulatory frameworks that address new challenges in the digital realm, including AI, IoT, and data privacy, to ensure cybersecurity and encourage innovation. These regulations should be flexible and capable of adapting to new technological

advancements. Regulatory frameworks in cybersecurity are crucial for protecting sensitive information, ensuring compliance with legal standards, and mitigating risks associated with cyberattacks. These frameworks vary across jurisdictions and industries, reflecting the diverse challenges and approaches to cyber security. The financial sector is at the forefront of cybersecurity regulations, with various jurisdictions adopting customized cybersecurity laws and regulations.

These frameworks aim to harmonize international cybersecurity standards to overcome regulatory challenges and enhance financial sector security (Didenko, 2020). Higher-education institutions face unique cybersecurity challenges. Adopting regulatory frameworks, such as the NIST Cybersecurity Framework, helps institutions manage cyber risks and align with international information security standards (Bondoc & Malawit, 2020).

A blend of regulatory approaches, including management-based regulatory delegation and directive regulations, is more effective in preventing security breaches. Engaging private entities in establishing cybersecurity standards enhances the regulatory process (Thaw, 2013). Compliance with federal and state regulations is essential for protecting digital assets in the financial industry. Regulatory frameworks, including the Gramm-Leach-Bliley Act (GLBA), offer directives for safeguarding the privacy and protection of individuals' personal data (Mohammed et al., 2020).

The fast-evolving EU cybersecurity regulatory framework impacts the Internet of Things (IoT) domains. The Cybersecurity Act, along with other sector-specific regulations, addresses the challenges of securing IoT and its supply chain (Chiara, 2022). The European Union employs a unified regulatory framework to safeguard personal information and enhance cybersecurity. This approach incorporates several key principles, including risk assessment, built-in protection measures, mandatory reporting, system resilience, and implementation of

certification programs (Mantelero et al., 2020). A flexible and responsive governance structure is crucial to effectively address cybersecurity threats. These structures should encompass collaboration between the public and private sectors, cooperation at both regional and international levels, and adherence to legal and regulatory requirements (Melaku, 2023).

Proactive cybersecurity norms, shaped by industry practices and international law, are essential for better protection of IT assets. Polycentric partnerships involving the public and private sectors can enhance cybersecurity governance (Craig et al., 2015). Cybersecurity regulatory frameworks are vital for protecting digital assets and ensuring compliance with legal standards. By adopting dynamic, adaptive, and harmonized approaches, stakeholders can effectively address the complex and evolving landscapes of cyber threats.

7.12 Future of Cyber Diplomacy

Cyber diplomacy, or e-diplomacy, is becoming increasingly important as states use digital platforms for diplomatic engagement, public diplomacy, and soft-power projection. Cyber diplomacy involves diplomatic efforts to address and manage the complex challenges posed by cyber threats. The future of cyber diplomacy will likely see enhanced cooperation among nations, the integration of advanced technologies, and the establishment of international norms and regulations to ensure secure and stable cyberspace.

In international relations, cyber diplomacy has emerged as a crucial component, emphasizing the safeguarding of human security and socioeconomic interests within the digital landscape. This approach is vital for fostering positive relationships between nations and securing a global cyber environment (Shrestha, 2023). In the realm of cyber diplomacy, artificial intelligence (AI) technologies are expected to have a profound impact. AI has the potential to bolster diplomatic endeavors by enhancing the ability to identify and respond to threats and creating new avenues for political and diplomatic interactions (Minchev, 2023).

The evolving cyberspace landscape necessitates robust cyber diplomacy to manage conflicts and promote peaceful international relations. Digital strategies and coordinated efforts can help prevent cyber conflicts and establish common digital standards (Y. Maulana & Fajar, 2023). The development of international norms and values through cyber diplomacy is essential for achieving long-term cyber security and stability. Diplomatic efforts should focus on confidence-building measures and cooperative strategies to reduce cyber threats (Meer, 2015).

The EU's approach to cyber diplomacy involves integrating cybersecurity with broader digital policies to enhance technological sovereignty and ensure a secure digital single market. This approach highlights the importance of a coherent and strategic cyber diplomacy framework (Bendiek & Kettemann, 2021). In the Asia-Pacific region, countries such as Japan and Australia are incorporating deterrence into their cyber diplomacy strategies. This involves enhancing cyber capabilities and adopting public attribution practices to strengthen cybersecurity cooperation (Manantan, 2021).

Cyber diplomacy is evolving into an international practice that bridges national interests and global dynamics. It involves diplomatic actions to manage state and non-state actors' behavior in cyberspace, ensuring a secure and stable cyber environment (Barrinha & Renard, 2017b). The future of cyber diplomacy will involve enhanced international cooperation, integration of advanced technologies, and establishment of comprehensive international norms and regulations. These efforts are crucial for maintaining global cybersecurity and fostering peaceful international relations in the digital age.

7.13 Cybersecurity and Global Stability

Cyberspace plays a critical role in maintaining global stability, and cybersecurity is a key component of this effort. Ensuring cybersecurity involves addressing technical, political, and social dimensions to prevent conflicts and promote peace.

- **Preventing Cyber Conflicts**

States should implement confidence-building measures (CBMs) to build trust and reduce the risk of misperceptions and escalation in cyberspace. Examples of CBMs include transparency, communication channels, and joint cyber exercises. Enhancing capabilities for the accurate attribution of cyber-attacks and holding perpetrators accountable is crucial for deterrence and stability. International cooperation in attribution efforts can improve the credibility and effectiveness of response. Promoting and adhering to norms that prohibit cyberattacks on civilian infrastructure and critical services is essential for maintaining peace and stability. States should commit to non-aggression pacts in cyberspace. To de-escalate cyber conflicts, it is crucial to create systems for peaceful dispute resolution such as arbitration and mediation. International bodies can assist in implementing conflict resolution processes.

- **Enhancing Cyber Resilience**

A crucial aspect of national and global security is the development of resilient infrastructure capable of enduring and bouncing back from cyberattacks. This involves allocating resources to create redundant systems, establish backup capabilities, and implement robust cybersecurity measures. Promoting cyber hygiene and resilience at the community level, including education and awareness programs for citizens, can enhance the overall societal resilience to cyber threats.

National governments should develop holistic cybersecurity strategies that integrate technical, legal and social dimensions. These strategies should address prevention, detection, response, and recovery and involve all relevant stakeholders. States should actively participate in international forums to develop and promote norms and agreements for responsible behavior in cyberspace. Multilateral agreements on issues such as cybercrime, cyber warfare, and data

protection are essential for ensuring global stability. Governments should foster strong partnerships with the private sector to leverage its expertise and resources. Public-private collaboration is crucial for effective threat intelligence sharing, coordinated response efforts, and developing innovative cybersecurity solutions.

Policymakers should strive to implement cybersecurity protocols that safeguard digital rights, including privacy and free speech. Legal frameworks should regulate surveillance practices and promote transparency and accountability in their use. Strengthening cybersecurity skills and fostering digital awareness require crucial efforts in skill development and educational initiatives to be effective. Closing the technology gap can be achieved through global collaboration to offer technical support, skill-building programs, and the necessary tools.

The integration of cyberspace into international relations has far-reaching implications for policymaking, diplomacy, and global stability. By developing comprehensive cybersecurity strategies, promoting international norms, enhancing public-private partnerships, protecting digital rights, and investing in capacity building, states can effectively navigate the complexities of cyberspace. The insights and recommendations provided in this chapter underscore the need for continued interdisciplinary research, dialogue, and cooperation to address the evolving challenges and opportunities of the digital era.

CHAPTER-8

8. Pakistan’s Realization Episodes and Response

Pakistan has experienced numerous serious cyberattacks over the years, highlighting vulnerabilities in its cybersecurity infrastructure and raising concerns about national security. These attacks have targeted various sectors, including government institutions, financial systems, and critical infrastructure, reflecting the growing trend of cyber threats in the region. One of the most significant incidents occurred in 2018, when Pakistan's banking sector faced a massive cyberattack that compromised many debit card accounts in major banks. This attack was characterized as one of the most intense in the history of Pakistan's banking industry, leading to substantial financial losses and a crisis of trust among customers (Bajwa, 2023). The attack involved sophisticated techniques that exploited vulnerabilities in the banking system, prompting calls for improved cybersecurity measures in the financial sector (Imran, 2022).

In addition to banking, government websites are frequent targets of cyberattacks. For instance, in 2016, the Pakistan Electronic Media Regulatory Authority (PEMRA) was hacked, resulting in the defacement of its official website. Such attacks not only disrupt services but also undermine public confidence in government institutions (Tariq et al., 2013). The frequency of these incidents indicates a broader trend of cyber threats aimed at destabilizing governmental operations and spreading misinformation. The threat of cyber warfare, particularly from India, has been highlighted as a pressing issue, with both nations reportedly engaging in cyber operations to gain a strategic advantage (Ashraf & Kayani, 2023).

The lack of a comprehensive national cybersecurity framework exacerbates these vulnerabilities in Pakistan’s case. Research indicates that Pakistan's cybersecurity policies are outdated and insufficient to address the evolving nature of cyberthreats (Ahmad, 2024). The absence of effective legislation and enforcement mechanisms has made it challenging to

combat cybercrime and protect critical infrastructure (Awan et al., 2019). Consequently, Pakistan faces a complex and extremely hostile cyber threat landscape that requires urgent attention and strategic planning. Serious cyberattacks in Pakistan, particularly in the banking sector and government institutions, underscore the urgent need for enhanced cybersecurity measures. The increasing sophistication of cyber threats, coupled with the challenges posed by state-sponsored cyber espionage, necessitates a comprehensive approach to safeguard a nation's digital infrastructure and ensure national security.

8.1 Pakistan's Cyber Threat Matrix

Notwithstanding Pakistan's advancement in the ITU 2024 'Global Cybersecurity Index', substantial efforts remain necessary to comprehensively secure the nation's digital infrastructure. While this positive trajectory is noteworthy, it underscores the significant challenges in establishing robust cybersecurity measures across the country. Pakistan's advancement from the 79th position in 2021 to among the top 46 nations demonstrates significant progress, particularly in regulatory frameworks, skill development, and emergency response mechanisms. However, this improved ranking should not divert attention from the persistent challenges the nation faces and the substantial deficiencies in its preparedness, adaptability, and governance (Salman, 2024).

With the increasing global reliance on Information and Communication Technology (ICT), the risk of cyber disturbances is escalating. Pakistan faces complex cyber security challenges, as evidenced by a significant 300% increase in cyberattacks compared to the equivalent period in 2023 (The Tribune, 2024). These challenges encompass both the threat of malicious entities seeking to compromise networks and the imperative to safeguard citizens' data and information systems.

Exacerbating these challenges is the pervasive lack of understanding among Pakistani

Internet users, who often have minimal knowledge of IT, rendering them susceptible to numerous cybersecurity risks. This dearth of expertise, coupled with the nation's scarcity of technological proficiency and assets, impedes effective oversight and the implementation of robust digital security protocols, highlighting the urgent requirement for improved governance in this sphere (U. P. Khan & Anwar, 2020).

As of January 2024, 45.7 percent of Pakistan's population had access to the internet, with its digital user base expanding by 24 million within a single year between 2023 and 2024 (“Digital 2024,” 2024). In January 2024, Pakistan was the 7th country with the largest digital population of approximately 111 million (“Number of Internet Users by Country 2024,” n.d.). This substantial online presence offers potential for digital economic expansion while simultaneously posing challenges in implementing robust cybersecurity protocols to safeguard the growing number of Internet users.

Pakistan's cybersecurity threat landscape is influenced by three primary factors: insufficient cybersecurity preparedness, sociopolitical tensions at the domestic and regional levels, and fragmented cybersecurity governance. Vulnerabilities in digital governance infrastructure particularly render the country susceptible to diverse cyber threats. These risks are exacerbated by internal and regional sociopolitical hostilities, increasing the likelihood of politically motivated cyberattacks (Shad, 2019).

In 2021, the Federal Investigation Agency (FIA) reported that complaints pertaining to cybercrimes crossed the 100,000 mark (Ashfaque, n.d.), while the Pakistan Telecommunications Authority (PTA) noted 10,000 cyberattacks in 2022 (PTA Cyber Security Annual Report 2022, n.d.). These attacks primarily targeted the banking, telecom, educational, and critical infrastructure sectors, with the military and government sectors being the main targets.

8.1.1 Data Security

The unauthorized acquisition of personal, financial, and technical information, commonly referred to as data theft, has significantly increased in Pakistan, particularly with the expansion of digital banking services. This phenomenon has notably impacted key government institutions and the telecommunications sector. In 2018, the head of FIA's cybercrime wing disclosed that data from virtually all Pakistani banks had been compromised due to a significant security breach, resulting in the exposure of card details belonging to approximately 19,000 individuals from 22 banks on the dark web (Qarar, n.d.).

In 2018, personal information, including data from the Punjab Information Technology Board (PITB), was breached, allegedly comprising Computerized National Identity Card details and mobile phone user databases. Although the PITB denied these claims, sources indicated that the stolen data were being sold on platforms such as Facebook and WhatsApp (Shad, 2019). In 2021, the Federal Investigation Agency (FIA) informed the National Assembly's Standing Committee on Information Technology that biometric data from the National Database and Registration Authority (NADRA) were compromised. (Express Tribune, 2021).

8.1.2 Phishing

Phishing is a deceptive form of online crime that tricks Internet users into revealing confidential personal or financial data, such as login credentials, credit card information, or banking details. This fraudulent practice is a type of cybercrime that aims to obtain sensitive information through deceit. Malicious actors on the Internet manipulate the mechanisms that guide users to web addresses, redirecting them to deceptive sites. These practices were termed phishing and pharming, drawing analogies with casting a lure into the sea to capture potential victims or creating backdoors for subsequent attacks (Bayuk, 2012, p. 34).

Victims may experience substantial adverse consequences, including the misappropriation of personal information, identity theft, and the compromise of confidential business or government data. In Pakistan, where much of the public is not familiar with the idea of cybersecurity, social engineering techniques are easily used for cybercrimes. An overarching strategy, starting from early childhood education to universities, is required to raise awareness of safe cyber practices.

The National Telecommunication and Information Security Board (NTISB) released a warning in 2023 regarding the increase in financial fraud. This advisory was issued in response to an observed increase in monetary scams utilizing phishing and vishing methods. The NTISB attributed this surge primarily to the public's insufficient awareness of cybersecurity measures. Unfortunately, there is no technical solution to social engineering because it is not aimed directly at the systems but rather at the user. (Amin, 2023)

8.1.3 Ransomware

Ransomware is a form of cyberattack in which an attacker employs malicious software and scripts to encrypt data on the target system and eliminate all backups. In numerous instances, the data are important to individuals and organizations, compelling them to remit payment for the decryption key to recover their data. In the case of ransomware, the data is effectively held hostage, and a monetary ransom is demanded (Buchanan, 2020, p. 279). In some cases, ransomware attacks can cause irreversible damage beyond data encryption. The impact of ransomware extends to downtime costs, reputation damage, and potential loss of life in critical sectors, such as healthcare (Wazid, Kumar Das, & Shetty, 2023).

Cybersecurity experts do not recommend paying ransom for data on the premise that it further reinforces the pattern and increases the number of ransomware attacks in the future. Paying a ransom does not guarantee data recovery or system restoration. Even after payment,

there is no assurance that the attackers will provide a functional decryption key or release the locked resources (Al-rimy, Maarof, & Shaid, 2018). Paying ransomware encourages and funds additional criminal activities. Successful ransom payments make ransomware a lucrative business for attackers, leading to an increase in such attacks worldwide. The ransomware market has grown significantly, with a minimum worth of USD 12,768,536 from 2013 to mid-2017 (Paquet-Clouston, Haslhofer, & Dupont, 2019). Instead of paying ransoms, cybersecurity experts suggest focusing on prevention, detection, and mitigation strategies to address ransomware attacks.

In 2020, the Netwalker ransomware group perpetrated a significant cyberattack against K-Electric, the nation's largest energy supplier. The cybercriminals issued an ultimatum to the company, demanding a ransom payment of USD 3.85 million within a seven-day period (Jajja, 2020). The same ransomware group targeted Argentina's immigration department and the University of California, San Francisco (UCSF). The UCSF later confirmed that it had paid a ransom of $1.14 million (Winder, 2020).

In July 2023, the Election Commission of Pakistan (ECP), the electoral watchdog of the country, issued an alert after its employees were targeted by a ransomware attack (I. A. Khan, 2023). All these incidents point to serious shortcomings in the entire cybersecurity architecture of the country, which needs to be revamped at varying levels, starting from individuals to organizational audits, robust cyber compliance systems, and an enhanced focus on business continuity and disaster recovery plans for critically important sectors.

8.1.4 Distributed Denial of Service (DDoS)

Distributed denial-of-service (DDoS) attacks are a significant threat to Internet security, characterized by a group of collaborative attackers using compromised systems to overwhelm and deny legitimate users access to server resources (Manavi, 2018). These attacks involve

sending a large number of packets to create a crowding effect, with traffic generated from multiple compromised nodes that are spread across various geographical locations. Over time, DDoS attacks have evolved in both frequency and complexity, making them increasingly difficult to detect and mitigate.

The COVID-19 pandemic has exacerbated this issue, as traditional perimeter-based security measures have become more vulnerable to attackers targeting health services, e-commerce, and educational services (De Neira, Kantarci, & Nogueira, 2023). Attackers no longer need to be highly skilled, as tools for orchestrating attacks can be easily found online with little to no knowledge required (Kotey, Tchao, & Gadze, 2019). DDoS attacks pose a critical threat to network-based service providers, potentially resulting in significant economic losses for businesses owing to increased operating and financial costs. As defense mechanisms continue to develop, attackers are also evolving their techniques to evade detection, necessitating ongoing research and development of more effective countermeasures

The Pakistani government disclosed in an advisory in 2023 that a Russian hacking group, ‘Kill Net’ had orchestrated attacks on Pakistan's military and civilian infrastructure. These attacks employed various methods, with Distributed Denial of Service (DDoS) being one of the primary techniques utilized (Paracha, 2023). Since 1998, these attacks have intensified periodically in Pakistan, particularly following the establishment of the Indian Cyber Army (ICA) in 2010. The formation of the ICA marked a significant juncture, resulting in more systematic cyber intrusions into Pakistan.

This escalation underscores the ongoing cyber warfare between the two nations and highlights the vulnerabilities in Pakistan's cybersecurity infrastructure (Shad, 2019). In another incident in April 2023, Pakistan International Airlines (PIA) came under a DDoS attack by an ISIS-linked hacking group, the United Cyber Caliphate (UCC), resulting in website defacement

and blocked user access (Khaitan, 2023).

8.2 K-Electric Attack

K-Electric, the primary electricity supplier in Karachi, Pakistan, has faced significant cyberattacks that have raised concerns regarding the security of its infrastructure and the potential for widespread disruption. One of the most notable incidents occurred in October 2020, when K-Electric's systems were reportedly targeted by a cyber-attack that led to disruptions in electricity supply across various areas of Karachi. The attack was characterized by unauthorized access to the company's operational technology systems, which are critical for managing power distribution and grid stability (Teryak, 2023).

The nature of the attack involved sophisticated techniques that exploited vulnerabilities in K-Electric's cyber-physical systems, which integrate information technology with operational technology to manage the electricity grid. Such systems are increasingly susceptible to cyber threats because of their reliance on interconnected networks and real-time data communication (Nguyen et al., 2020; Oughton et al., 2019).

The incident not only disrupted the power supply but also raised concerns about the potential for more severe consequences, including the risk of physical damage to infrastructure and public safety (Teryak, 2023). In the wake of the attack, K-Electric acknowledged the incident and stated that it was working with cybersecurity experts to assess the damage and restore normal operations. The company emphasized its commitment to enhancing its cybersecurity measures to prevent future incidents ("Cyber Physical Security of Distributed Energy Resources", 2023). This response reflects the growing recognition among utility companies worldwide of the importance of robust cybersecurity frameworks, especially considering increasing cyber threats targeting critical infrastructure (Mohammed, 2024).

The implications of such cyberattacks extend beyond immediate disruptions. They

highlight the vulnerabilities inherent in modern power systems, which are increasingly digitized and interconnected. As noted by Nguyen et al. (2020), the integration of advanced technologies into power grids enhances efficiency but also introduces significant risks, making them attractive targets for cyber adversaries. The K-Electric incident serves as a reminder of the need for continuous investment in cybersecurity measures, including employee training, system upgrades, and incident response planning, to safeguard against evolving cyberthreats (Rahimpour et al., 2023). Moreover, the cyberattack on K-Electric underscores the critical vulnerabilities faced by utility companies in Pakistan and globally. As the reliance on digital technologies in power systems increases, so does the necessity for comprehensive cybersecurity strategies to protect against potential disruptions and ensure the resilience of essential services.

8.3 Cyber-attack on Pakistan Airforce

In July 2022, the Pakistan Air Force (PAF) experienced a significant cyberattack that raised concerns about the security of its digital infrastructure. This incident was part of a broader trend of increasing cyber threats targeting military and governmental institutions in Pakistan, reflecting the evolving nature of warfare in the digital era. The cyber-attack on the PAF reportedly involved sophisticated tactics aimed at compromising sensitive data and disrupting its operational capabilities. Although specific details about the attack's execution and its immediate impacts were not extensively disclosed, it was noted that the attack was part of a series of cyber operations that have been attributed to state-sponsored actors, particularly in the context of regional tensions with neighboring countries (Farooq & Ahmad, 2022).

This incident highlighted the vulnerabilities of military networks, which are increasingly reliant on digital technologies for communication, command, and control. The implications of such cyber-attacks on military institutions are significant. As noted by Onesimiuc, the cyber dimension plays a crucial role in modern military operations, and air

forces are particularly vulnerable because of their reliance on advanced technologies and interconnected systems (Onesimiuc, 2023).

The attack on the PAF underscores the necessity of robust cybersecurity measures to protect critical military infrastructure from potential adversaries. In response to the cyber-attack, the PAF and other military branches in Pakistan have been urged to enhance their cyber security protocols. This includes investing in advanced security technologies, conducting regular vulnerability assessments, and implementing comprehensive training programs for personnel to recognize and respond effectively to cyber threats. The need for collaboration between military and civilian cybersecurity efforts has also been emphasized, as a unified approach can strengthen the overall resilience of the national security infrastructure.

Furthermore, the incident reflects a broader trend of increasing cyber warfare capabilities among state actors, particularly in South Asia and Pakistan. As highlighted by Farooq and Ahmad, the growing cyber partnerships and capabilities of countries such as India pose significant challenges for Pakistan, necessitating a proactive stance on cybersecurity (Farooq & Ahmad, 2022).

The PAF's experience serves as a critical reminder of the importance of safeguarding military assets in an era in which cyber threats are becoming increasingly sophisticated and prevalent. This attack also illustrates the vulnerabilities of military institutions in the digital age. As cyber threats continue to evolve, it is imperative for the PAF and other military branches to adopt comprehensive cyber security strategies to protect sensitive information and maintain operational readiness.

In November 2022, a significant cyber-attack attributed to Indian hackers targeted various sectors in Pakistan, including government and military institutions. This incident was part of a broader pattern of cyber hostilities between the two nations, reflecting ongoing

geopolitical tensions in South Asia. Reports indicate that attackers have employed sophisticated techniques to infiltrate systems and disrupt operations, aiming to undermine Pakistan's national security and public confidence (Ashraf & Kayani, 2023). This cyber-attack involved the use of Distributed Denial-of-Service (DDoS) tactics, which overwhelmed the targeted systems with excessive traffic, rendering them inaccessible.

Such attacks are particularly concerning for critical infrastructure because they can disrupt essential services and create chaos. The attackers reportedly aimed to exploit vulnerabilities in Pakistan's cybersecurity defenses, which have been criticized for being inadequate against evolving cyber threats (Farooq & Ahmad, 2022). The implications of this cyber-attack were significant, as it not only targeted governmental and military systems but also aimed to increase discontent among the civilian population.

The psychological impact of such attacks can be profound, as they contribute to a climate of fear and uncertainty, exacerbating existing tensions between the two countries. Furthermore, the incident highlighted the need for Pakistan to enhance its cybersecurity measures and develop a more robust national strategy to counter cyber threats. In response to the attack, experts emphasized the importance of international cooperation in cybersecurity, particularly in sharing intelligence and best practices to mitigate risks.

The State Bank of Pakistan and other regulatory bodies have been urged to implement stricter cybersecurity protocols across all sectors, particularly in critical infrastructure, to safeguard against future cyberattacks. Moreover, the incident underscored the necessity for Pakistan to invest in advanced cybersecurity technologies and training personnel to recognize and respond to cyber threats effectively. As noted by Ashraf and Kayani, India's growing cyber capabilities pose a significant challenge for Pakistan, necessitating a proactive approach to cybersecurity (Ashraf & Kayani, 2023).

The November 2022 cyber-attack on Pakistan by Indian hackers serves as a stark reminder of the vulnerabilities that nations face in the digital age. As cyber threats continue to evolve, Pakistan must strengthen its cybersecurity framework to protect its national interests and maintain regional stability.

8.4 Pakistan's Lagging Cyber Defense

Pakistan's cybersecurity strategy faces several shortcomings that hinder its ability to effectively counter the growing threat of cyberattacks. These deficiencies can be categorized into several key areas, including inadequate legal frameworks, insufficient investment in cybersecurity infrastructure, lack of skilled personnel, and ineffective response mechanisms. One of the primary issues is the lack of a comprehensive legal framework governing cybersecurity in Pakistan.

As highlighted by Watto, current cyber laws are outdated and do not adequately address the complexities of modern cyber threats (Watto, 2024). This legislative gap hinders law enforcement agencies' ability to effectively prosecute cybercriminals and protect citizens from cyber threats. Furthermore, the lack of clear regulations regarding data protection and privacy exacerbates vulnerabilities, leaving individuals and organizations exposed to potential breaches (Anjum, 2020).

Another significant shortcoming is insufficient investment in cybersecurity infrastructure. Many organizations in Pakistan, including critical sectors such as banking and energy, have not prioritized cybersecurity, leading to outdated systems that are ill equipped to defend against sophisticated cyberattacks. Reliance on legacy systems increases the attack surface and makes it easier for adversaries to exploit vulnerabilities. As noted by Elradi et al., organizations must adopt a proactive approach to cybersecurity, which includes investing in advanced technologies and establishing Security Operations Centers (SOCs) to monitor and

respond to threats in real time (Elradi et al., 2021).

The shortage of skilled cybersecurity professionals is another critical challenge in this field. The rapid evolution of cyber threats requires a workforce that is not only knowledgeable but also capable of adapting to new technologies and attack vectors. However, the current educational and training programs in Pakistan do not adequately prepare individuals for careers in cybersecurity, leading to a significant skills gap in the industry (Watto, 2024). This deficiency limits the effectiveness of existing cybersecurity measures and hampers the country's ability to respond to incidents effectively. Moreover, the response mechanisms to cyber incidents are often slow and ineffective. Many organizations lack established incident response plans, which can lead to confusion and delays in addressing cyber threats (Żebrowski et al., 2022). A coordinated response among various stakeholders, including government agencies, private sector organizations, and law enforcement, is crucial for mitigating the impact of cyberattacks. As emphasized by Ahn et al., a proactive and well-coordinated approach is essential for effectively managing cyber risks and ensuring national security (Ahn et al., 2020).

In 2013, Pakistan was reported to be the second-most spied-upon country by the U.S. National Security Agency (NSA), Iran topped the list (Cassidy, n.d.). The same year, a Pakistani daily reported that British intelligence hacked Cisco routers in Pakistan, which not only allowed them unauthorized access to all internet users in the country but also rerouted their traffic to the agency’s filters (AFP, 2015).

India's cyber warfare capabilities pose a significant threat to Pakistan's national security across multiple domains. The Indian Cyber Army has developed robust capabilities that can potentially cause financial damage, political instability, societal unrest, and radicalization in Pakistan (Ashraf & Kayani, 2023). India's cyber-attacks on Pakistan's infrastructure are likely to exploit zero-day vulnerabilities in cyber-physical systems, targeting critical assets such as

nuclear facilities (Poornima, 2022).

Pakistan's cybersecurity strategy has several shortcomings, including inadequate legal frameworks, insufficient investment in infrastructure, a lack of skilled personnel, and ineffective response mechanisms. Addressing these issues is critical for enhancing the country's resilience to cyber threats and ensuring the protection of its critical infrastructure and citizens.

8.5 Raising the Cyber Guard

Pakistan's cybersecurity strategy has evolved in response to the increasing threats posed by cybercrime, cyber terrorism, and cyber warfare. However, several shortcomings hinder its effectiveness. Despite serious challenges, Pakistan has made strides in establishing a legal framework for cybersecurity, notably through the Prevention of Electronic Crimes Act (PECA) and the National Cyber Policy. However, the implementation of these laws is often inconsistent, and there is a lack of comprehensive regulations that address the complexities of modern cyber threats (Imran, 2022; Zahoor & Razi, 2020). The existing legal framework does not adequately cover issues such as data protection and privacy, which are critical for safeguarding citizens' information (Zahoor & Razi, 2020).

There is a pressing need for increased investment in cybersecurity infrastructure across both the public and private sectors. Many organizations, including critical infrastructure providers, have not prioritized cybersecurity, leading to outdated systems that are vulnerable to attacks (Imran, 2022; Mirza & Akram, 2022). The government has been urged to consolidate resources and establish national agencies dedicated to cybersecurity to enhance the protection of critical assets (Baloch, 2019).

Another significant challenge for Pakistan is the shortage of skilled cyber security professionals. Current educational and training programs do not sufficiently prepare individuals for careers in cybersecurity, resulting in a skills gap that limits the effectiveness of

existing measures (Mirza & Akram, 2022). Enhancing educational initiatives and training programs is essential for building a competent workforce capable of addressing cyber threats.

Pakistan's incident response capabilities are often slow and ineffective. Many organizations lack established incident response plans, which can lead to confusion and delays in addressing cyber threats (Tariq et al., 2013). A coordinated response among various stakeholders, including government agencies, private sector organizations, and law enforcement, is crucial for mitigating the impact of cyberattacks (Akram, 2023).

The concept of deterrence has been applied to counter non-traditional security threats, including cyberattacks. However, the effectiveness of deterrence as a strategy against cyber warfare remains questionable, as the nature of cyber-attacks often blurs the lines between state and non-state actors (Syed & Javed, 2017; Ashraf & Kayani, 2023). A more nuanced approach that combines deterrence with proactive cybersecurity measures is necessary to address the evolving threat landscape.

Given the transnational nature of cyber threats, international cooperation is vital to enhance Pakistan's cybersecurity capabilities. Collaboration with other nations to share intelligence, best practices, and resources can strengthen Pakistan's defenses against cyber-attacks (Mirza & Akram, 2022). While Pakistan has made progress in developing its cybersecurity strategy, significant shortcomings remain, such as enhancing the legal framework, investing in infrastructure, building a skilled workforce, improving incident response mechanisms, and fostering international cooperation in cybersecurity. Making progress in these areas is essential for effectively safeguarding the nation against growing threats in cyberspace.

8.6 Pakistan’s Cyber Capabilities

8.6.1 Pakistan Computer Emergency Response Team (PKCERT)

The Pakistan Computer Emergency Response Team (PKCERT) plays a crucial role in enhancing Pakistan’s cybersecurity posture by addressing various challenges and implementing strategies to improve the country’s cybersecurity ranking. It serves as a central hub for coordinating responses to cybersecurity incidents across various sectors, including government, private, and critical infrastructure sectors. By providing timely assistance and guidance during cyber incidents, PKCERT helps organizations mitigate the impact of attacks and recover effectively. This coordination is essential for building a resilient cybersecurity framework in Pakistan (Khan et al. 2023).

One of the significant challenges in Pakistan's cybersecurity landscape is the lack of awareness and training among users and organizations. PKCERT conducts awareness campaigns and training sessions to educate individuals and organizations about cybersecurity best practices. These initiatives are designed to empower users to recognize and respond to cyber threats, thereby reducing the overall risk of cyberincidents (Alqahtani & Kavakli, 2020; Hakimi, 2024).

PKCERT also actively collaborates with international cybersecurity organizations and initiatives to share knowledge, resources and best practices. This collaboration helps Pakistan stay updated on global cybersecurity trends and threats, enabling the country to adopt more effective strategies and technologies to combat cyber threats (Ramakrishnan, 2024). PKCERT advises the government on developing and implementing cybersecurity policies and regulations. By contributing to the formulation of comprehensive cybersecurity laws, PKCERT helps establish a legal framework that supports the protection of critical infrastructure and enhances the overall cybersecurity posture of the country (Bokhari, 2023). Recognizing the shortage of skilled cybersecurity professionals in Pakistan, PKCERT is involved in capacity-

building initiatives aimed at developing a skilled workforce in Pakistan. This includes partnerships with educational institutions to enhance cybersecurity curricula and promote careers in the field, thereby addressing the talent gap (Nobles, 2018).

PKCERT encourages research and development of cybersecurity technologies and methodologies. By fostering innovation in cybersecurity solutions, PKCERT aims to strengthen the defenses of Pakistani organizations against emerging cyberthreats (Ramakrishnan, 2024). It promotes collaboration between the public and private sectors to enhance cybersecurity resilience. By facilitating partnerships, PKCERT helps organizations share threat intelligence and best practices, thereby creating a more robust cybersecurity ecosystem (Bokhari, 2023).

PKCERT's multifaceted approach to improving cybersecurity in Pakistan encompasses all key areas, including incident response coordination, awareness and training programs, international collaboration, policy development, capacity building, research and development, and public-private partnerships. These efforts are essential for enhancing Pakistan’s cybersecurity ranking and ensuring the protection of its critical infrastructure and digital assets.

8.6.2 National Centre for Cyber Security (NCCS)

In 2018, the government founded the National Centre for Cyber Security (NCCS) in collaboration with the Higher Education Commission (HEC) and the Planning Commission to enhance national capabilities and produce local professionals and solutions in Cyber Security (Qazi, 2024). Following a public solicitation for proposals, ten universities were selected through a rigorous evaluation process to establish specialized R&D laboratories under the NCCS. Air University was designated as the NCCS Secretariat and accommodated two affiliated laboratories: the 'National Cyber Crime and Forensics Lab' and the 'Devices & Network Security Lab'.

Since 2018, the NCCS has played a crucial role in enabling the creation of various startups by offering support for product and prototype development through its laboratories. Prominent among these startups are Thingz Eye Pvt. Ltd. and Lynx Information Security Pvt. Ltd. Additionally, Cyber Droid Pvt Ltd and TRIC Tech Pvt Ltd stand out as significant ventures, showcasing the NCCS's contribution to nurturing innovation and the entrepreneurial spirit within Pakistan's cyber security sector (NCCS Research And Collaboration, n.d.).

Through more than 112 workshops, technical training sessions, and relevant seminars, the NCCS laboratories have educated more than 4,000 individuals. The development of a robust cybersecurity ecosystem depends on competent human resources. The National Cyber Security Academy (NCSA) addresses the human element in cybersecurity across both governmental and commercial sectors (Workshops and Trainings, n.d.).

8.7 National Cyber Security Policy 2021

In 2021, Pakistan's Ministry of Information Technology and Telecommunication (MoITT) announced the country's first National Cyber Security Policy (NCSP), which aims to safeguard Pakistan's entire digital landscape, including all national digital assets, information processed, administered, retained, or transmitted within both the public and private sectors. It also covers the information and communication systems utilized by Pakistani citizens.(Shad, 2022)

According to the NCSP, a 'Cyber Governance Policy Committee' (CGPC) should be established at the state level to oversee national cybersecurity matters. This committee would be tasked with developing policies, establishing legal frameworks, and addressing the structural needs. The CGPC is intended to serve as a crucial liaison between various departments and ensure compliance with international cybersecurity norms. The CGPC also allocates responsibilities for global representation and discussions regarding cyber governance. Its

proposals require approval from the Federal Cabinet, thereby ensuring a national-level commitment and coherence with evolving cyberspace challenges.

The NCSP's two primary guiding tenets concentrate on protecting online data privacy and bolstering citizens' security, thus fostering national growth in the digital domain. Additionally, the policy emphasizes the seriousness of cyber-attacks targeting the nation's Critical Infrastructure (CI) and Critical Information Infrastructure (CII), considering such actions as 'an act of aggression against national sovereignty (National CYBER SECURITY POLICY 2021, 2021).

Consequently, the NCSP allows Pakistan to claim its entitlement to safeguard itself through suitable countermeasures to secure its digital infrastructure and address national concerns. Academics contend that while the NCSP is a step in the right direction, its success relies on appropriate and swift execution. This necessitates robust collaboration and synchronization among different agencies and departments, coupled with public information campaigns to enlighten citizens about cybersecurity risks.

However, several crucial aspects of the CGPC remain ambiguous, including its operational framework, hierarchical structure, authority, and composition. Without precise definitions, these entities risk becoming dormant in the future. To ensure successful execution, decision-makers must establish a comprehensive cybersecurity framework applicable to all organizations and implement a rigorous auditing process to maintain compliance. Elucidating the CGPC's structure and duties is vital for achieving effective cybersecurity governance across all sectors.

8.8 Cyber Security Strategy 2023-2028 for Telecom Sector

Aligning with the NCSP, in December 2023, the Pakistan Telecom Authority (PTA) unveiled its 'Cyber Security Strategy 2023-2028 for Telecom Sector'.(Pakistan Telecom

Authority, Cyber Security Strategy for Telecom Sector 2023-2028, n.d.) The comprehensive five-year strategy aims to bolster the cybersecurity of the nation's telecommunications network. Its primary objective is to fortify the digital defenses of the existing infrastructure against potential cyber-attacks.(Amin, 2023b)

The blueprint of this strategy highlights six essential components, each addressing a distinct aspect of cybersecurity. These components encompass the legal framework, cyber resilience, proactive surveillance and emergency response, skill development, teamwork and partnerships, and public education. (Pakistan Telecom Authority, Cyber Security Strategy for Telecom Sector 2023-2028, n.d.)

Additionally, the PTA outlined a set of criteria for telecommunications companies to support the implementation of the strategy. These firms are obligated to safeguard customer information through the adoption of stringent security protocols and educate their clients about cybersecurity risks and methods to mitigate these threats.

Telecom firms should establish cybersecurity strategies spanning various timeframes: annual, two to three years, and three to five years. It is crucial to ensure adherence to PTA guidelines and implement the prescribed cybersecurity framework. Additionally, all staff members should receive comprehensive training in cybersecurity protocols to mitigate internal risks and enhance the organization's preparedness (Ahmadani, 2023). Although this strategy for telecom cyber security provides a robust framework to bolster the protection of telecommunications firms against emerging cyber threats, it is premature to evaluate its effectiveness, as the implementation is still in its early phases.

8.9 Computer Emergency Response Teams (CERTs) Rules, 2023

In the last ten years, the telecommunications sector has seen substantial growth, propelled by cutting-edge communication technologies that enable global connectivity. This

expansion has resulted in increased cybersecurity threats to organizations operating in digital, computer-centric environments. Historically, Pakistan has lacked a robust institutional structure for managing and safeguarding its cyberspace. Nevertheless, a crucial advancement occurred in September 2023 with the establishment of the 'Computer Emergency Response Teams (CERTs) Rules, 2023' (Amin, 2023).

The legislation aims to safeguard against cybersecurity risks at various levels, including national, industry-specific, and organizational levels. To facilitate the practical application of these regulations, the establishment of National Security Operations has been declared. The true effectiveness of these measures in addressing cybersecurity risks will only be fully ascertained through a thorough assessment after an extended period of implementation.

8.10 National Cyber Crimes Investigation Agency (NCCIA), 2024

In May 2024, the Federal Government of Pakistan officially announced the formation of the National Cyber Crimes Investigation Agency (NCCIA), signaling a major shift in the country's strategy for tackling electronic offences (Momand, 2024). Interestingly, this development effectively renders the FIA's Cybercrime Wing obsolete, as its staff, resources, obligations, and ongoing cases are transferred to the newly established agency. This reorganization, implemented under Sections 51 and 29 of the Prevention of Electronic Crimes Act of 2016, demonstrates Pakistan's commitment to consolidating and enhancing its cybercrime enforcement capabilities.

As per government guidelines, this shift also seeks to address the disparity in collaboration between domestic and international efforts to combat cybercrimes. The establishment of the NCCIA aims to bolster Pakistan's cyber security framework; however, the transitional phase, during which former FIA staff continue their roles until the NCCIA is fully staffed, may present obstacles in ensuring smooth operational continuity. Nonetheless, the

creation of the NCCIA demonstrates a forward-thinking strategy to address escalating cyber threats through enhanced governance and international cooperation.

8.11 Cybersecurity Risk Governance

Studies show that numerous developing nations often experience a substantial gap between policy creation and successful execution. This disparity typically stems from organizational ineffectiveness, insufficient resources, and poor synchronization among crucial governmental bodies. This phenomenon, known as the "burden-capacity gap," varies across countries and sectors, depending on the integration between policymaking and implementing bureaucracies (Fernández-I-Marín et al., 2024). While policies are often well-crafted, they frequently fail to achieve their intended outcomes due to inadequate organizational capacity and a lack of robust, actionable frameworks.

This issue is particularly pronounced in the realm of cybersecurity, where the intricacies of cross-agency cooperation and the swift progression of cyber threats further compound these difficulties. For instance, PECA established the legal groundwork, yet subsequent initiatives, such as the NCSP, continue to grapple with effective implementation. This mirrors the global pattern observed in developing nations, where policy reforms often encounter obstacles during the execution phase. While policies typically inform the creation of strategies and subsequent legislation, the inverse sequence observed in nations such as Pakistan (where PECA preceded the NCSP) is indicative of more extensive governance challenges (Rafiq & Mustafa, 2021).

Recently, the Federal Government has taken steps to enhance Pakistan's cybersecurity framework. However, the complexity and severity of cyber threats are escalating daily. To address these sophisticated threats, there is a pressing need for better cybersecurity risk governance in the country. Robust cyber security risk governance involves responsive strategies, tools, and structures to manage and mitigate cyber-related risks. To secure the digital

environment, Pakistan must prioritize the synchronized implementation of cybersecurity measures in its policies, including effective documentation and reporting to ensure compliance with digital security laws and demonstrate commitment to cybersecurity risk governance. Effective operationalization requires addressing structural and indigenous challenges and focusing on comprehensive solutions to them.

The transition of cybercrime investigations from the FIA Cyber Wing to the NCCIA may potentially disrupt ongoing investigations and compromise cybersecurity enforcement because of discontinuity in institutional processes. This abrupt alteration raises significant concerns regarding resource allocation, expertise transfer, and operational clarity. While the NCCIA aims to safeguard digital rights, the overlap in responsibilities and continued involvement of FIA personnel for an additional year may result in ambiguity, inefficiencies, and delays in addressing cyber threats.

This organizational shift risks undermining public confidence in cybersecurity initiatives, as the transition from an established entity to a newly formed one may be perceived as destabilizing the initiative. It is advisable to avoid sudden changes in governance structures without a clear delineation of roles and accountability measures.

It is imperative for Pakistan to take decisive action to enhance digital literacy, as the current level of digital literacy renders a significant portion of its citizens vulnerable to such threats. A 2020 World Bank report revealed that only 34 percent of adults possess sufficient digital competence, highlighting the pressing need to instruct the populace on navigating the digital realm safely. Addressing Pakistan’s significant digital gap requires a focus on enhancing Internet infrastructure as a top priority. Nearly 40% of individuals who do not use mobile Internet face challenges in operating basic devices, underscoring the importance of implementing targeted programs to promote digital inclusivity.

To fully benefit from digital transformation, the government should enhance infrastructure, ensure universal access, and educate the public about digital engagement. Expanding access and increasing awareness will promote inclusive economic growth and integrate marginalized regions into the digital economy. Many countries have enacted laws to protect citizens' data, requiring organizations to obtain explicit consent before collecting or sharing personal information. The European Union's General Data Protection Regulation (GDPR), for instance, empowers individuals to control their data and holds organizations accountable for proper handling. Similarly, Pakistan urgently requires a comprehensive data protection law that prioritizes personal data rights and ensures responsible data handling.

The implementation of comprehensive data protection and privacy legislation in Pakistan has progressed at a sluggish pace. Despite the existence of various regulations aimed at safeguarding data, the nation still lacks an all-encompassing legal framework to regulate the handling, processing, and transmission of personal information. The 'Personal Data Protection Bill', which was introduced in 2021, remains under consultation in 2024 and has not yet been enacted into law (Amin, 2024). From a technical standpoint, Pakistan must swiftly make it a top priority to safeguard its vital institutions by implementing cutting-edge cybersecurity measures, including systems for detecting intrusions, controlling access, and managing identities. To strengthen defenses against cyber-attacks, it is crucial to maintain an unwavering emphasis on disaster recovery protocols, business continuity plans, network redundancy, rigorous auditing processes and strict compliance measures.

Considering the worldwide scope of cybercrime and its associated threats, it is crucial to establish cross-border partnerships. As digital technology advances rapidly, judicious and careful exchange of information among governmental bodies and international entities can significantly bolster joint efforts to identify and combat cyber risks. However, Pakistan has not

yet signed the Budapest Convention, which is the pioneering and most comprehensive global agreement on cybercrime. Concerns over national sovereignty have led Pakistan to abstain from endorsing the Budapest Convention, as the country is wary of sharing information with foreign law-enforcement agencies (Amin, 2020).

Such collaborative efforts may result in foreign entities gaining access to sensitive data, which may be viewed as an infringement. However, the transnational nature of cyber threats necessitates international cooperation. Pakistan should contemplate developing a secure framework for sharing information that strikes a balance between privacy concerns and the necessity of joint efforts in tracking, investigating, and bringing cybercriminals to justice. By engaging in a multilateral agreement, Pakistan can address its sovereignty issues while enhancing its capacity to tackle cybercrime globally.

8.12 Insights from Interviews with Experts

8.12.1 Insights from Interview with Mr. Ammar Hussain Jaffri

Cyberspace has increased the pace of events

- Cyberspace facilitates rapid global transformation by reducing the response times of states and enhancing the influence of diplomatic communications, such as tweets by world leaders.
- Conventional concepts of power, sovereignty, and borders are being contested, as events and security decisions increasingly unfold rapidly on digital platforms.
- Recent developments, such as the conflict between Pakistan and India, underscore the critical importance of cyberspace in national security, necessitating adaptive statecraft.

Pakistan's Readiness for Modern Cyber Threats

- There are gaps in Pakistan’s preparedness against supply chain attacks and Advanced Persistent Threats (APTs)
- Although physical inspections of equipment are routinely conducted, there is currently no specialized agency responsible for assessing technological imports for software or hardware vulnerabilities within critical sectors.
- The increasing reliance on the Internet of Things (IoT) in agriculture introduces new vulnerabilities that are not being adequately addressed.

Human Resource and Cyber Literacy Challenges

- Education is a fundamental concern. With a significant number of children not attending school, digital literacy levels remain low, thereby increasing the population's susceptibility to cyberattacks.
- Human factors are pivotal in cybersecurity; even the most secure systems remain vulnerable if users lack cyber awareness, particularly as threats from AI-driven social engineering become more prevalent.
- Pakistan is approximately a decade behind in the development of its cyber workforce and the promotion of public digital hygiene. However, efforts are being made to address these deficiencies and advance in these areas.

Public-Private Partnerships and Compliance Structures

- The collaboration between the public and private sectors is recognized as essential; however, it has been largely overlooked.
- The inauguration of the National Aerospace Science and Technology Park (NASTP) and initiatives promoting collaboration in critical technology sectors.

- The establishment of a Computer Emergency Response Team (CERT) and the implementation of new banking security guidelines.
- The recent reorganization of the FIA's cyber wing has resulted in its transformation into the National Cyber Crimes Investigation Agency (NCCIA).
- The necessity for a comprehensive and well-formulated cybersecurity policy is underscored as crucial for the effective mitigation of cybercrime.

8.12.2 Insights from Interview with Dr. Salman Ali

Influence of Cyberspace on Traditional Concepts of Power and Sovereignty

- Cyberspace has fundamentally altered global politics by surpassing the constraints of traditional Westphalian statism, thereby challenging long-standing conceptions of state power that are associated with physical borders….
- The cyberspace domain is characterized by its fluidity and lack of physical boundaries, enabling actors to operate without the physical limitations imposed by visas or immigration controls….
- States are increasingly allocating resources to enhance their cyber capabilities, as concepts such as cyberwarfare, cyber defense, and cyber operations become integral to the field of international relations….
- The concept of sovereignty is influenced by the intangible and pervasive characteristics of cyberspace.

Limitations of Traditional International Relations Theories

- Current theoretical frameworks are insufficient in comprehensively elucidating cyber conflicts, cyber norms, and interstate digital cooperation.

- While ongoing academic endeavors continue, the inherent novelty and complexity of cyberspace present significant challenges.

Pakistan’s Cybersecurity Landscape and Its Challenges

- Pakistan is increasingly cognizant of the necessity to enhance its strategies for addressing cyberspace challenges, as evidenced by the growing legislative initiatives and the acceptance of digital evidence in judicial proceedings.
- As digital infrastructure and participation continue to expand, Pakistan seeks to establish more comprehensive regulatory frameworks to address emerging cyber issues.
- The legal and regulatory framework is anticipated to progressively adapt to address the complexities inherent in cyberspace.

8.12.3 Insights from Interview with Dr. Yasir Masood

Cyberspace’s Influence on Power, Sovereignty, and Borders

- Contemporary power dynamics are increasingly predicated on the ability to control information flows, execute cyber disruptions, and project influence instantaneously, rather than solely relying on military or economic strength.
- The concept of sovereignty has become increasingly fluid as governments endeavor to assert control through domestic cyber regulations. However, they encounter significant challenges due to the Internet's inherently borderless nature and the presence of multinational platforms.
- The significance of physical borders has diminished as cyberspace redefines them as nodes of network control rather than mere geographic demarcations, thereby posing challenges to traditional concepts of territorial integrity.

Limitations of Traditional International Relations Theories in Cyberspace

- The realist paradigm's emphasis on state actors and military capabilities overlooks the significance of non-state entities and the influence of digital power.

- The focus of liberalism on institutional frameworks is undermined by the sluggishness of global organizations and the clandestine accumulation of cyber weapons. Consequently, there is a pressing need for more rapid and pragmatic collaboration between public and private sectors.
- Constructivism offers valuable insights into the understanding of norms and identity. However, its explanatory power can be significantly enhanced through the integration of digital network analysis and ethnographic methods to effectively capture the complexities of diverse online cultures.
- A comprehensive framework that integrates elements of power, cooperation, and digital culture is essential for a thorough understanding of cyberspace.

Adaptation of International Relations Theories to Cyber Conflict and Cooperation

- Realism now considers cyberspace to be a strategic domain comparable to traditional domains of warfare.
- Liberalism promotes cyber diplomacy through the establishment of new forums, coalitions, and confidence-building measures that engage both state actors and the private sector.
- Constructivism examines the development of norms in cyberspace through the lens of repeated interactions and voluntary agreements.
- Integrated methodologies that synthesize these perspectives are currently emerging, although they remain in a developmental stage.

Pakistan's Cybersecurity Landscape and Challenges

- Pakistan has made advancements in establishing a national cybersecurity policy and a Computer Emergency Response Team (CERT). However, these initiatives are hindered by inadequate funding and a shortage of skilled personnel.

- Identified deficiencies encompass antiquated legislation, insufficient public awareness of cybersecurity, and susceptibilities within critical infrastructure that depend on foreign technology and outdated systems.
- Recommendations include prioritizing the training of the cyber workforce, revising legal frameworks to enhance breach response capabilities, fostering public-private collaboration, and engaging in regional and global intelligence sharing to bolster resilience.

8.12.4 Insights from Interview with Dr. Baqir Malik

Cyberspace and Traditional IR Concepts:

- In cyberspace, power is intangible and challenging to quantify, with a tendency to favor offensive strategies due to the low barriers to entry. Conversely, defensive measures are more complex and incur greater costs.
- The concept of sovereignty becomes increasingly ambiguous as virtual presence transcends national boundaries, and cyber operations seldom infringe upon sovereignty unless they target critical infrastructure.
- While cyberspace transcends physical boundaries, mechanisms such as firewalls and censorship function as digital boundaries.

Limitations of Established IR Theories

- Realism, liberalism, and constructivism continue to hold significance; however, they face challenges posed by cyberspace and require substantial adaptation.
- While states continue to hold a pivotal position, particularly in the domains of legislation and international treaties, it is imperative that theoretical frameworks adapt to encompass the complexities introduced by cyber realities.

Adaptation of IR Theories to Cyber Issues:

- Current theoretical frameworks are insufficient in comprehensively elucidating the dynamics of cyber conflict, cooperation, and the establishment of norms.
- Recent literature is emerging; however, significant conceptual modifications are necessary to address the distinctive structure of cyberspace.

Pakistan's Cybersecurity Landscape:

- In Pakistan, cyber laws are frequently employed for political purposes rather than for genuine security concerns, and they suffer from a lack of widespread consensus and effective enforcement.
- There is a lack of collaboration between public and private sectors, inadequate data protection measures, and frequent breaches that often go unpunished.
- An urgent and comprehensive reform of legislation, enforcement mechanisms, privacy safeguards, and judicial proficiency is necessary.

8.12.5 Insights from Interview with Dr. Muhammad Shoaib

- **Cyberspace and International Relations Theory**

  Conventional international relations theories encounter significant challenges in addressing cyberspace, as it disrupts established notions such as sovereignty and necessitates the development of novel frameworks that have yet to be fully established.

- **Limitations of Traditional Theories**

  Traditional theoretical frameworks such as realism, liberalism, and constructivism were developed in the context of a world characterized by distinct borders and state sovereignty, rendering them inadequate for addressing the complexities of cyberspace. To effectively adapt these theories, scholars should prioritize the examination of foundational philosophical principles rather than focusing solely on superficial characteristics.

- **Adaptation to Cyber Issues**

  International relations theories have not sufficiently evolved to account for cyber conflict or digital cooperation. This inadequacy is partly attributable to the reluctance of leading states to transcend traditional mindsets and prioritize collective solutions.

- **Pakistan's Cybersecurity Landscape**

  In Pakistan, the regulation of cyberspace is predominantly aimed at suppressing dissent rather than enhancing security. Authorities prioritize restricting access over implementing constructive management strategies, an approach that is increasingly proving to be ineffective and problematic both domestically and internationally.

Conclusion

This thesis explores the profound impact of cyberspace on international relations theories, examining how traditional and contemporary frameworks have adapted to the digital age. Cyberspace has introduced new dimensions of power and conflict, necessitating the re-evaluation of national security strategies and the concept of state sovereignty. Realist perspectives now incorporate cyber warfare, cyber deterrence, and the strategic importance of cyber capabilities in national security. Cyberspace aligns with the liberal principles of cooperation, international institutions, and economic interdependence. The digital economy, e-commerce, and international cyber governance highlight the potential for collaborative solutions to shared challenges. The role of norms, identities, and social constructs in cyberspace is critical to understanding the phenomenon. Constructivist perspectives illuminate how cyber norms are developed, contested, and internalized and how cyber identities and narratives influence state behavior.

This demonstrates how cyberspace challenges and enriches traditional IR theories, prompting the development of new frameworks that account for the digital dimensions of global interactions. By incorporating perspectives from realism, liberalism, and constructivism, this thesis provides a comprehensive and nuanced understanding of cyberspace in IR. It offers actionable recommendations for policymakers, emphasizing the importance of comprehensive cyber security strategies, international cooperation, digital rights protection, and capacity building. The analysis of digital diplomacy provides insights into how states can effectively use digital platforms for diplomatic engagement and public diplomacy to enhance their soft power and strategic communication capabilities. The discussion on multi-stakeholder governance highlights the need for inclusive and adaptive regulatory frameworks that address emerging cyberspace issues. The constantly changing and fluid nature of the digital realm

continually creates new challenges and possibilities for scholars and professionals in international relations. Future studies should focus on the following topics:

Further investigation is needed to understand how cutting-edge technologies such as artificial intelligence, quantum computing, and the Internet of Things (IoT) affect cybersecurity and global diplomatic relations. The increasing sophistication of cybercrimes and cyberterrorism poses a significant threat to global security. Future research should investigate effective strategies for prevention, detection, and responses. Continued efforts are required to develop and promote international norms for responsible state behavior in cyberspace. Future research should explore the processes of norm formation, contestation, and internalization. The ethical implications of cyber operations, surveillance, and data privacy require continuous examination. Future research should address the balance between security and individual rights issues. Future investigations should focus on methods to narrow the digital gap and guarantee fair access to digital innovations and prospects for everyone. This encompasses the analysis of the impact of global organizations and developmental programs.

Subsequent studies should investigate successful approaches to multi-stakeholder governance that incorporates a wide range of participants in the decision-making process and examine the functions of global organizations, businesses, and community groups in these governance models. Similarly**,** investigating the development and implementation of international agreements on cyber issues such as cybercrime, data protection, and cyber warfare is essential for promoting global stability. The incorporation of cyberspace into international relations theories marks a crucial development in the comprehension and handling of global interactions. This thesis demonstrates the profound impact of cyberspace on traditional and contemporary IR frameworks, highlighting the need for interdisciplinary approaches and adaptive policies. The continuous development of the digital realm necessitates ongoing study

and discussion to address the intricacies of our technological era and foster a global environment that is secure, all-encompassing and equitable. This dissertation offers valuable perspectives and suggestions that enhance our collective knowledge of cyberspace in the context of international relations. It also provides actionable guidance for decision-makers, diplomatic professionals, and academics as they navigate the complexities and possibilities of the digital age.

In Pakistan's case, the country is catching up fast with the developed world, be it the rising numbers of freelancers who work and are a source of steady inflow of foreign exchange in the dollar-starved economy but are also an irreducible part of the evolving digital ecosystem in the country. Pakistan's improvement in the 2024 Global Cybersecurity Index is a positive development; however, the political turmoil within the country and frequent Internet disruptions are taking their toll in the form of economic losses. The Pakistan Institute of Development Economics (PIDE) in 2023 estimated the cost of an Internet shut down for a single day at about PKR 1.3 billion, which is a staggering cost for an already struggling economy. The loss equals approximately .57 percent of the daily average GDP to an economy that is already under stress due to its USD payment and adverse balance of payments. While the state's concerns about propaganda and information waged on the internet against it are genuine, its response needs to be calibrated. The entire criminal justice system requires a major overhaul to extend the deterrent effect of existing laws in cyberspace.

References

Abbasi, M. (2021). Security in cyberspace in the field of international relations. *Journal of Archives in Military Medicine*, *8*(4). https://doi.org/10.5812/jamm.114485

Abosata, N., Al-Rubaye, S., Inalhan, G., & Emmanouilidis, C. (2021). Internet of Things for System Integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications. *Sensors*, *21*(11), 3654. https://doi.org/10.3390/s21113654

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons*, *62*(4), 539–548. https://doi.org/10.1016/j.bushor.2019.03.010

Acton, J. M. (2018). Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War. *International Security*, *43*(1), 56–99. https://doi.org/10.1162/isec_a_00320

Adamson, L. (2019). Let them roar: Small States as Cyber Norm Entrepreneurs. *European Foreign Affairs Review*, *24*(Issue 2), 217–234. https://doi.org/10.54648/eerr2019014

Adegbite, N. a. O., Akinwolemiwa, N. D. I., Uwaoma, N. P. U., Kaggwa, N. S., Akindote, N. O. J., & Dawodu, N. S. O. (2023b). REVIEW OF CYBERSECURITY STRATEGIES IN PROTECTING NATIONAL INFRASTRUCTURE: PERSPECTIVES FROM THE USA. *Computer Science & IT Research Journal*, *4*(3), 200–219. https://doi.org/10.51594/csitrj.v4i3.658

Adiputera, Y. (2017). Evaluating the normative and structural explanations of democratic peace theory. *Global South Review*, *1*(1), 21. https://doi.org/10.22146/globalsouth.28817

AFP. (2015, June 24). British hacking claims Rights campaigners urge Islamabad to protect privacy of citizens. *The Express Tribune*. Accessed at https://tribune.com.pk/story/908953/pakistani-privacy-activists-slam-unethical-british-hacking-claims

Agharebparast, M., & Zeinali, A. (2016). The role of foreign policy and international relations in economic development based on the philosophy of liberalism. *Journal of Social Science Studies*, *4*(1), 1. https://doi.org/10.5296/jsss.v4i1.9706

Agius, C. (2022). 6. Social constructivism. In *Oxford University Press eBooks* (pp. 73–89). https://doi.org/10.1093/hepl/9780198862192.003.0006

Ahmadani, A. (2023, December 22). Pakistantoday.com. Retrieved July 30, 2025, from https://www.pakistantoday.com.pk/2023/12/22/Fortifying-Telecom-Sector-Pta-Unveils-Cyber-Security-Strategy-2023-2028/

Ahmed, A. M., Hussaini, A., & Abdulhamid, A. (2022). Cyber warfare and national security: imperative for naval operations. *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, 990–996. https://doi.org/10.1109/csci58124.2022.00176

AkyeşiLmen, N. (2024). GEOPOLITICAL IMPLICATIONS OF CYBERSPACE ON INTERNATIONAL RELATIONS: AN INDEPTH ANALYSIS. In *Turkish Academy of Sciences eBooks* (pp. 501–520). https://doi.org/10.53478/tuba.978-625-6110-04-5.ch36

Al-Hawawreh, M., & Moustafa, N. (2023). Explainable deep learning for attack intelligence and combating cyber–physical attacks. *Ad Hoc Networks*, *153*, 103329. https://doi.org/10.1016/j.adhoc.2023.103329

Alaranta, T. (2023). Turkey's transformed state identity. In *Edinburgh University Press eBooks* (pp. 133–143). https://doi.org/10.3366/edinburgh/9781474492515.003.0011

Alashi, S. A., & Badi, D. H. (2020). The role of governance in achieving sustainable cybersecurity for business corporations. *Journal of Information Security and Cybercrimes Research*, *3*(1), 97–112. https://doi.org/10.26735/eint7997

Alexei, A. (2021). CYBER SECURITY STRATEGIES FOR HIGHER EDUCATION INSTITUTIONS. *Journal of Engineering Science*, *XXVIII*(4), 74–92. https://doi.org/10.52326/jes.utm.2021.28(4).07

Allahrakha, N. (2023). Balancing cyber-security and privacy: Legal and ethical considerations in the digital age. *Legal Issues in the Digital Age*, *4*(2), 78–121. https://doi.org/10.17323/10.17323/2713-2749.2023.2.78.121

Amin, T. (2020, January 22). Ministry creating hurdles in signing MLAT, Budapest Convention with USA. *Business Recorder*. https://www.brecorder.com/news/547196

Amin, T. (2023a, October 13). CERT Rules, 2023 notified to bolster cyber security defences. *Business Recorder*. https://www.brecorder.com/News/40267846

Amin, T. (2023b, December 13). PTA unveils 'Cyber Security Strategy' *Business Recorder*. https://www.brecorder.com/News/40278325

Amin, T. (2024, May 22). IT Ministry finalising Personal Data Protection Bill. *Business Recorder*. https://www.brecorder.com/News/40304612

Ananda, S., Putranti, I., & Dir, A. (2022). ANALYSIS OF THE EU CYBERSECURITY ACT UNDER THE THEORY OF NEOLIBERAL INSTITUTIONALISM. *Arena Hukum*, *15*(1), 176–199. https://doi.org/10.21776/ub.arenahukum.2022.01501.9

Ananda, S., Putranti, I., & Dir, A. (2022). ANALYSIS OF THE EU CYBERSECURITY ACT UNDER THE THEORY OF NEOLIBERAL INSTITUTIONALISM. *Arena Hukum*, *15*(1), 176–199. https://doi.org/10.21776/ub.arenahukum.2022.01501.9

Andress, J., & Winterfeld, S. (2013). Computer network defense. In *Elsevier eBooks* (pp. 193–205). https://doi.org/10.1016/b978-0-12-416672-1.00011-8

Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. *Computers & Industrial Engineering*, *149*, 106829. https://doi.org/10.1016/j.cie.2020.106829

Antoine, L. (2022). The power of a promise: whom do governments' security justifications convince to accept surveillance? *Political Research Exchange*, *4*(1). https://doi.org/10.1080/2474736x.2022.2101380

Aradau, C., & Cluskey, E. M. (2021). Making digital surveillance unacceptable? Security, democracy, and the political sociology of disputes. *International Political Sociology*, *16*(1). https://doi.org/10.1093/ips/olab024

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, *147*, 113580. https://doi.org/10.1016/j.dss.2021.113580

Ashizawa, K. (2008). When Identity Matters: State Identity, Regional Institution-Building, and Japanese Foreign policy1. *International Studies Review*, *10*(3), 571–598. https://doi.org/10.1111/j.1468-2486.2008.00805.x

Ashraf, N., & Kayani, S. A. (2023). INDIA'S CYBER WARFARE CAPABILITIES: REPERCUSSIONS FOR PAKISTAN'S NATIONAL SECURITY. *NDU Journal*, *37*, 34–45. https://doi.org/10.54690/ndujournal.37.152

Assessing the risks of cyber terrorism, cyber war and other cyber threats | *Office of Justice Programs*. (n.d.). https://www.ojp.gov/ncjrs/virtual-library/abstracts/assessing-risks-cyber-terrorism-cyber-war-and-other-cyber-threats

Atkins, S., & Lawson, C. (2020). An improvised patchwork: success and failure in cybersecurity policy for critical infrastructure. *Public Administration Review*, *81*(5), 847–861. https://doi.org/10.1111/puar.13322

Atkins, S., & Lawson, C. (2021). Cooperation amidst competition: cybersecurity partnership in the US financial services sector. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab024

Avraam, C., Ceferino, L., & Dvorkin, Y. (2023). Operational and economy-wide impacts of compound cyber-attacks and extreme weather events on electric power networks. *Applied Energy*, *349*, 121577. https://doi.org/10.1016/j.apenergy.2023.121577

Babiceanu, R. F., & Seker, R. (2016). Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook. *Computers in Industry*, *81*, 128–137. https://doi.org/10.1016/j.compind.2016.02.004

Back, S., LaPrade, J., & Soor, S. (2018). Spatial and Temporal Patterns of Cyberattacks: Effective CYBERCRIME Prevention Strategies around the Globe. *J-Institute*, *3*(1), 7–13. https://doi.org/10.22471/protective.2018.3.1.07

Backhaus, S., Gross, M. L., Waismel-Manor, I., Cohen, H., & Canetti, D. (2020). A cyberterrorism effect? emotional reactions to lethal attacks on critical infrastructure. *Cyberpsychology Behavior and Social Networking*, *23*(9), 595–603. https://doi.org/10.1089/cyber.2019.0692

Badar, M. E. (2003). Basic principles governing limitations on individual rights and freedoms in human rights instruments. *The International Journal of Human Rights*, *7*(4), 63–92. https://doi.org/10.1080/13642980310001726226

Baezner, M. (2018). Cyber and Information warfare in the Ukrainian conflict. *Research Collection*. https://doi.org/10.3929/ethz-b-000321570

Baezner, M., & Robin, P. (2017). Stuxnet. *Research Collection*. https://doi.org/10.3929/ethz-b-000200661

Bailey, M., Dittrich, D., Kenneally, E., & Maughan, D. (2012). The Menlo report. *IEEE Security & Privacy*, *10*(2), 71–75. https://doi.org/10.1109/msp.2012.52

Baillon, A., De Bruin, J., Emirmahmutoglu, A., Van De Veer, E., & Van Dijk, B. (2019). Informing, simulating experience, or both: A field experiment on phishing risks. *PLoS ONE*, *14*(12), e0224216. https://doi.org/10.1371/journal.pone.0224216

Balajanov, E. (2017). Setting the minimum age of criminal responsibility for cybercrime. *International Review of Law Computers & Technology*, *32*(1), 2–20. https://doi.org/10.1080/13600869.2018.1417764

Banta, B. R. (2020). International Cyberpolitics. *Oxford Research Encyclopedia of International Studies*. https://doi.org/10.1093/acrefore/9780190846626.013.553

Baram, G. (2017). Israeli Defense in the Age of Cyber War. In *MIDDLE EAST QUARTERLY*. Middle East Quarterly. Retrieved July 30, 2025, from https://cdn-mef.meforum.org/a7/c3/ccec3465ab3bafe0c828444b238e/6399.pdf

Barcomb, K. E., Krill, D. J., Mills, R. F., & Saville, M. A. (2012). Establishing cyberspace sovereignty. *International Journal of Cyber Warfare and Terrorism*, *2*(3), 26–38. https://doi.org/10.4018/ijcwt.2012070103

Barkawi, T. (1998). Strategy as a vocation: Weber, Morgenthau and modern strategic studies. *Review of International Studies*, *24*(2), 159–184. https://doi.org/10.1017/s0260210598001594

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, *3*(4–5), 353–364. https://doi.org/10.1080/23340460.2017.1414924

Barrinha, A., & Renard, T. (2020). Power and diplomacy in the post-liberal cyberspace. *International Affairs*, *96*(3), 749–766. https://doi.org/10.1093/ia/iiz274

Barrinha, A., & Turner, R. (2023). Strategic narratives and the multilateral governance of cyberspace: The cases of European Union, Russia, and India. *Contemporary Security Policy*, *45*(1), 72–109. https://doi.org/10.1080/13523260.2023.2266906

Battista, D. (2023). Disinformation as a danger to international security: An exploration of the implications in the Italian context. *Geopolitical, Social Security and Freedom Journal*, *6*(1–2), 1–19. https://doi.org/10.2478/gssfj-2023-0001

Baylon, C. (2016). Lessons from Stuxnet and the Realm of Cyber and Nuclear Security: Implications for Ethics in Cyber Warfare. In *Springer eBooks* (pp. 213–229). https://doi.org/10.1007/978-3-319-45300-2_12

Beatty, G. (2020). War crimes in cyberspace: prosecuting disruptive cyber operations under Article 8 of the Rome Statute. *The Military Law and the Law of War Review*, *58*(2), 209–239. https://doi.org/10.4337/mllwr.2020.02.17

Behr, H., & Heath, A. (2009). Misreading in IR theory and ideology critique: Morgenthau, Waltz and neo-realism. *Review of International Studies*, *35*(2), 327–349. https://doi.org/10.1017/s0260210509008547

Belanger, F., & Crossler, R. E. (2018). Dealing with digital traces: Understanding protective behaviors on mobile devices. *The Journal of Strategic Information Systems*, *28*(1), 34–49. https://doi.org/10.1016/j.jsis.2018.11.002

Ben-Shahar, O. (2019). Data pollution. *The Journal of Legal Analysis*, *11*, 104–159. https://doi.org/10.1093/jla/laz005

Bennett, W. L., & Livingston, S. (2018). The disinformation Order: disruptive communication and the decline of democratic institutions. *European Journal of Communication*, *33*(2), 122–139. https://doi.org/10.1177/0267323118760317

Berejekian, J. (1997). The Gains debate: Framing state choice. *American Political Science Review*, *91*(4), 789–805. https://doi.org/10.2307/2952164

Berrada, G., Cheney, J., Benabderrahmane, S., Maxwell, W., Mookherjee, H., Theriault, A., & Wright, R. (2020). A baseline for unsupervised advanced persistent threat detection in system-level provenance. *Future Generation Computer Systems*, *108*, 401–413. https://doi.org/10.1016/j.future.2020.02.015

Bhardwaj, A. (2024). *Beyond the Realms: Navigating the metaverse*. https://doi.org/10.2174/9789815238457124010l

Bimantara, A. (2022). The Normative Enactment of International Cybersecurity Capacity Building Assistance: A comparative analysis on Japanese and South Korean practices. *Global Jurnal Politik Internasional*, *24*(1). https://doi.org/10.7454/global.v24i1.684

Blakely, B., Billings, H., Evans, N., Landry, A., & Domingo, A. (2023). *Evaluation of an Autonomous Intelligent Cyberdefense Agent at NATO Cyber Coalition Exercise 2022* (p. 13). https://doi.org/10.1117/12.2662959

Bocean, C. G., & Vărzaru, A. A. (2023). EU countries' digital transformation, economic performance, and sustainability analysis. *Humanities and Social Sciences Communications*, *10*(1). https://doi.org/10.1057/s41599-023-02415-1

Bondoc, N. C. E., & Malawit, N. T. G. (2020). Cybersecurity for higher education institutions: adopting regulatory framework. *Global Journal of Engineering and Technology Advances*, *2*(3), 016–021. https://doi.org/10.30574/gjeta.2020.2.3.0013

Boratalievich, N. Y. (2024). HUMAN RIGHTS AND MODERN TECHNOLOGIES: ETHICAL ASPECTS. *International Journal of Pedagogics*, *4*(5), 112–116. https://doi.org/10.37547/ijp/volume04issue05-24

Borghard, E. D., & Lonergan, S. W. (2017). The logic of coercion in cyberspace. *Security Studies*, *26*(3), 452–481. https://doi.org/10.1080/09636412.2017.1306396

Borghard, E. D., & Lonergan, S. W. (2021). Deterrence by denial in cyberspace. *Journal of Strategic Studies*, *46*(3), 534–569. https://doi.org/10.1080/01402390.2021.1944856

Bossong, R., & Wagner, B. (2016). A typology of cybersecurity and public-private partnerships in the context of the EU. *Crime Law and Social Change*, *67*(3), 265–288. https://doi.org/10.1007/s10611-016-9653-3

Bradshaw, S., & DeNardis, L. (2019). Privacy by infrastructure: the unresolved case of the domain name system. *Policy & Internet, 11*(1), 16–36. https://doi.org/10.1002/poi3.195

Brandom, R. (2014, December 11). Iran hacked the Sands hotel earlier this year, causing over $40 million in damage. *The Verge*. https://www.theverge.com/2014/12/11/7376249/Iran-Hacked-Sands-Hotel-In-February-Cyberwar-Adelson-Israel

Braw, E., & Brown, G. (2020). Personalised deterrence of cyber aggression. *The RUSI Journal*, *165*(2), 48–54. https://doi.org/10.1080/03071847.2020.1740493

Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Praeger. https://ecommons.udayton.edu/law_fac_pub/115

Brizhinev, D., Ryan, N., & Bradbury, R. (2018). Modelling hegemonic power transition in cyberspace. *Complexity*, *2018*(1). https://doi.org/10.1155/2018/9306128

Broadhurst, R., & Chang, L. (2012). Cybercrime in Asia: trends and challenges. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2118322

Brüggemann, K., & Kasekamp, A. (2008). The politics of history and the "War of Monuments" in Estonia. *Nationalities Papers*, *36*(3), 425–448. https://doi.org/10.1080/00905990802080646

Bughin, J., Seong, J., Manyika, J., Chui, M., & Joshi, R. (2018, September 4). *Notes from the AI Frontier: Modeling the impact of AI on the world economy*. McKinsey & Company. Retrieved July 30, 2025, from https://www.mckinsey.com/Featured-Insights/Artificial-Intelligence/Notes-From-The-Ai-Frontier-Modeling-The-Impact-Of-Ai-On-The-World-Economy

Buil-Gil, D., Lord, N., & Barrett, E. (2021). The Dynamics of Business, Cybersecurity and Cyber-Victimization: Foregrounding the Internal Guardian in Prevention. *Victims & Offenders*, *16*(3), 286–315. https://doi.org/10.1080/15564886.2020.1814468

Butrimas, V. (2014). National security and international policy challenges in a post Stuxnet world. *Lithuanian Annual Strategic Review*, *12*(1), 11–31. https://doi.org/10.2478/lasr-2014-0001

Buzan, B. (1984). Economic structure and international security: the limits of the liberal Case. *International Organization*, *38*(4), 597–624. https://doi.org/10.1017/s0020818300026886

Cabantous, L., Gond, J., & Johnson-Cramer, M. (2010). Decision Theory as Practice: Crafting Rationality in Organizations. *Organization Studies*, *31*(11), 1531–1566. https://doi.org/10.1177/0170840610380804

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

Calderaro, A., & Craig, A. J. S. (2020). Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, *41*(6), 917–938. https://doi.org/10.1080/01436597.2020.1729729

Campbell, P. (2018). Generals in Cyberspace: Military Insights for Defending Cyberspace. *Orbis*, *62*(2), 262–277. https://doi.org/10.1016/j.orbis.2018.02.006

Canavese, D., Mannella, L., Regano, L., & Basile, C. (2024). Security at the edge for Resource-Limited IoT devices. *Sensors*, *24*(2), 590. https://doi.org/10.3390/s24020590

Cansever, A. B. (2024). Cat diplomacy. In *Advances in media, entertainment and the arts (AMEA) book series* (pp. 187–223). https://doi.org/10.4018/979-8-3693-0855-4.ch014

Carias, J. F., Borges, M. R. S., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). Systematic Approach to Cyber Resilience Operationalization in SMEs. *IEEE Access*, *8*, 174200–174221. https://doi.org/10.1109/access.2020.3026063

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43–62. https://doi.org/10.1111/1468-2346.12504

Carr, M., & Lesniewska, F. (2020). Internet of Things, cybersecurity and governing wicked problems: learning from climate change governance. *International Relations*, *34*(3), 391–412. https://doi.org/10.1177/0047117820948247

Cassidy, J. (2013, June 10). Why Edward Snowden is a hero. *The New Yorker*. https://www.newyorker.com/news/john-cassidy/why-edward-snowden-is-a-hero

Cavelty, M. D. (2014). Breaking the Cyber-Security dilemma: aligning security needs and removing vulnerabilities. *Science and Engineering Ethics*, *20*(3), 701–715. https://doi.org/10.1007/s11948-014-9551-y

Cavelty, M. D., & Smeets, M. (2023). Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority. *Journal of European Public Policy*, *30*(7), 1330–1352. https://doi.org/10.1080/13501763.2023.2173274

Charitsis, V., Zwick, D., & Bradshaw, A. (2018). Creating Worlds that Create Audiences: Theorising Personal Data Markets in the Age of Communicative Capitalism. *tripleC Communication Capitalism & Critique Open Access Journal for a Global Sustainable Information Society*, *16*(2), 820–834. https://doi.org/10.31269/triplec.v16i2.1041

Chase, M., Macfadyen, L., Reeder, K., & Roche, J. (2002). Intercultural challenges in networked Learning: Hard technologies meet soft skills. *First Monday*, *7*(8). https://doi.org/10.5210/fm.v7i8.975

Checkel, J. T. (1997). International norms and domestic politics: *European Journal of International Relations*, *3*(4), 473–495. https://doi.org/10.1177/1354066197003004003

Checkel, J. T. (2001). Why comply? Social learning and European Identity change. *International Organization*, *55*(3), 553–588. https://doi.org/10.1162/00208180152507551

Chen, F., Mac, G., & Gupta, N. (2017). Security features embedded in computer aided design (CAD) solid models for additive manufacturing. *Materials & Design*, *128*, 182–194. https://doi.org/10.1016/j.matdes.2017.04.078

Chen, J. (2017, December 21). *Cyberdeterrence by engagement and surprise*. National Defense University Press. Retrieved July 30, 2025, from https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1983763/cyberdeterrence-by-engagement-and-surprise/

Chen, L., Chen, J., & Xia, C. (2021). Social network behavior and public opinion manipulation. *Journal of Information Security and Applications*, *64*, 103060. https://doi.org/10.1016/j.jisa.2021.103060

Chen, T. M., & Abu-Nimeh, S. (2011). Lessons from Stuxnet. *Computer*, *44*(4), 91–93. https://doi.org/10.1109/mc.2011.115

Chenou, J., & Bonilla-Aranzales, J. K. (2022). Cyber peace and intrastate armed conflicts. In *Cambridge University Press eBooks* (pp. 94–116). https://doi.org/10.1017/9781108954341.005

Chiara, P. G. (2022). The IoT and the new EU cybersecurity regulatory landscape. *International Review of Law Computers & Technology*, *36*(2), 118–137. https://doi.org/10.1080/13600869.2022.2060468

Cho, Y., & Chung, J. (2017). Bring the State back in: Conflict and cooperation among states in Cybersecurity. *Pacific Focus*, *32*(2), 290–314. https://doi.org/10.1111/pafo.12096

Choucri, N. (2012). *Cyberpolitics in international relations*. https://doi.org/10.7551/mitpress/7736.001.0001

Choucri, N. (2014). Co-Evolution of Cyberspace and International Relations: New challenges for the social sciences. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2514532

Choucri, N. (2015). Explorations in Cyber International Relations: a research collaboration of MIT and Harvard University. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2727414

Choucri, N., & Clark, D. D. (2012a). Integrating Cyberspace and international Relations: The Co-Evolution dilemma. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2178586

Choucri, N., & Clark, D. D. (2012b). Integrating Cyberspace and international Relations: The Co-Evolution dilemma. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2178586

Choucri, N., & Clark, D. D. (2013). Who controls cyberspace? *Bulletin of the Atomic Scientists*, *69*(5), 21–31. https://doi.org/10.1177/0096340213501370

Choucri, N., & Goldsmith, D. (2012). Lost in cyberspace: Harnessing the Internet, international relations, and global security. *Bulletin of the Atomic Scientists*, *68*(2), 70–77. https://doi.org/10.1177/0096340212438696

Christensen, T. J. (1997). Perceptions and alliances in Europe, 1865–1940. *International Organization*, *51*(1), 65–97. https://doi.org/10.1162/002081897550302

Chung, Y. (2021). Hybrid challenges in the PRC's novel public opinion warfare*. *Pacific Focus*, *36*(3), 405–426. https://doi.org/10.1111/pafo.12194

Cil, A. E., Yildiz, K., & Buldu, A. (2020). Detection of DDoS attacks with feed forward based deep neural network model. *Expert Systems With Applications*, *169*, 114520. https://doi.org/10.1016/j.eswa.2020.114520

Clark, A., Zhu, N. Q., Poovendran, R., & Basar, T. (2013). An impact-aware defense against Stuxnet. *American Control Conference*, 4140–4147. https://doi.org/10.1109/acc.2013.6580475

Clarke, R. A., & Knake, R. (2012). *Cyber War: The Next Threat to National Security and What to Do About It*. Ecco.

Clarke, R. A., & Knake, R. K. (2019). *The fifth domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*.

Cleveland, M., & Spangler, T. (2018). Toward a model for ethical cybersecurity leadership. *International Journal of Smart Education and Urban Society*, *9*(4), 29–36. https://doi.org/10.4018/ijseus.2018100103

Clinton, L. (2011). A relationship on the rocks: Industry-Government Partnership for cyber defense. *Journal of Strategic Security*, *4*(2), 97–112. https://doi.org/10.5038/1944-0472.4.2.6

Collins, S., & McCombie, S. (2012). Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing Intelligence and Counter Terrorism*, *7*(1), 80–91. https://doi.org/10.1080/18335330.2012.653198

Connolly, L. Y., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security*, *87*, 101568. https://doi.org/10.1016/j.cose.2019.101568

Copeland, D. (2003). A Realist critique of the English School. *Review of International Studies*, *29*(3), 427–441. https://doi.org/10.1017/s0260210503004273

Cornish, P. (2021). The deterrence and prevention of cyber conflict. In *Oxford University Press eBooks* (pp. 273–294). https://doi.org/10.1093/oxfordhb/9780198800682.013.16

Cortell, A. P., & Davis, J. W. (2005). When norms clash: international norms, domestic practices, and Japan's internalisation of the GATT/WTO. *Review of International Studies*, *31*(1), 3–25. https://doi.org/10.1017/s0260210505006273

Courtney, M. (2017). States of cyber-warfare. *Engineering & Technology*, *12*(3), 22–25. https://doi.org/10.1049/et.2017.0300

Coutinho, B., Ferreira, J., Yevseyeva, I., & Basto-Fernandes, V. (2023). Integrated cybersecurity methodology and supporting tools for healthcare operational information systems. *Computers & Security*, *129*, 103189. https://doi.org/10.1016/j.cose.2023.103189

Cozette, M. (2004). Realistic realism? American Political Realism, Clausewitz and Raymond Aron on the problem of means and ends in international politics. *Journal of Strategic Studies*, *27*(3), 428–453. https://doi.org/10.1080/1362369042000282976

Cozette, M. (2008). Reclaiming the critical dimension of realism: Hans J. Morgenthau on the ethics of scholarship. *Review of International Studies*, *34*(1), 5–27. https://doi.org/10.1017/s0260210508007882

Craig, A. N., Shackelford, S. J., & Hiller, J. S. (2015). Proactive Cybersecurity: A comparative industry and regulatory analysis. *American Business Law Journal*, *52*(4), 721–787. https://doi.org/10.1111/ablj.12055

Crampton, J. W. (2004). The political mapping of cyberspace. *Choice Reviews Online*, *42*(03), 42–1637. https://doi.org/10.5860/choice.42-1637

Cranor, L. F., & Garfinkel, S. (2005). *Security and usability: Designing Secure Systems that People Can Use*. O'Reilly Media, Inc.

Cyber Glossary - c. (n.d.). National Security Archive. https://nsarchive.gwu.edu/cyber-glossary-c

Cyber-Enabled Warfare and Deterrence: The Capability/Vulnerability Paradox of U.S. Doctrine and Technologies. (2016). *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2732188

Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2021). Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. *Education and Information Technologies*, *27*(4), 4729–4752. https://doi.org/10.1007/s10639-021-10806-7

De Neira, A. B., Kantarci, B., & Nogueira, M. (2023). Distributed Denial of service attack prediction: Challenges, open issues and opportunities. *Computer Networks*, *222*, 109553. https://doi.org/10.1016/j.comnet.2022.109553

Deibert, R. J., & Crete-Nishihata, M. (2012). Global governance and the spread of cyberspace controls. *Global Governance a Review of Multilateralism and International Organizations*, *18*(3), 339–361. https://doi.org/10.1163/19426720-01803006

Deibert, R. J., & Rohozinski, R. (2010). Risking Security: Policies and paradoxes of cyberspace security. *International Political Sociology*, *4*(1), 15–32. https://doi.org/10.1111/j.1749-5687.2009.00088.x

Deibert, R. J., Rohozinski, R., & Crete-Nishihata, M. (2012). Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war. *Security Dialogue*, *43*(1), 3–24. https://doi.org/10.1177/0967010611431079

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. L. (2011). Access contested. In *The MIT Press eBooks*. https://doi.org/10.7551/mitpress/9780262016780.001.0001

Delerue, F. (2019). Attribution to state of cyber operations conducted by Non-State Actors. In *Springer eBooks* (pp. 233–255). https://doi.org/10.1007/978-3-030-05648-3_12

Denning, D. E. (2012). Stuxnet: What has changed? *Future Internet*, *4*(3), 672–687. https://doi.org/10.3390/fi4030672

Desierto, D. A. (2021). The Association of Southeast Asian Nations and Southeast Asia's Regional Security. In *Oxford University Press eBooks* (pp. 947–962). https://doi.org/10.1093/law/9780198827276.003.0053

Dessler, D. (1999). Constructivism within a positivist social science. *Review of International Studies*, *25*(1), 123–137. https://doi.org/10.1017/s0260210599001230

Didenko, A. N. (2020). Cybersecurity regulation in the financial sector: Prospects of legal harmonisation in the EU and beyond. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3533664

DiMase, D., Collier, Z. A., Heffner, K., & Linkov, I. (2015). Systems Engineering Framework for Cyber Physical Security and Resilience. *Environment Systems & Decisions*, *35*(2), 291–300. https://doi.org/10.1007/s10669-015-9540-y

Dimmroth, K., & Schünemann, W. J. (2017). The ambiguous relation between privacy and security in German cyber politics. In *Springer eBooks* (pp. 97–112). https://doi.org/10.1007/978-3-319-53634-7_7

Djenna, A., Barka, E., Benchikh, A., & Khadir, K. (2023). Unmasking Cybercrime with Artificial-Intelligence-Driven Cybersecurity Analytics. *Sensors*, *23*(14), 6302. https://doi.org/10.3390/s23146302

Dogra, S., Singh, N., & Sahil, A. (2024). A REVIEW PAPER ON ETHICAL HACKING. *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, *08*(09), 1–5. https://doi.org/10.55041/ijsrem37588

Donnelly, J. (2000). *Realism and international relations*. https://doi.org/10.1017/cbo9780511612510

Doyle, M. W. (1986). Liberalism and world politics. *American Political Science Review*, *80*(4), 1151–1169. https://doi.org/10.2307/1960861

Dragomir, A. (2021). Cyber diplomacy. *International Journal of Information Security and Cybercrime*, *10*(2), 37–50. https://doi.org/10.19107/ijisc.2021.02.05

Drezner, D. (2020). Power and International Relations: a temporal view. *European Journal of International Relations*, *27*(1), 29–52. https://doi.org/10.1177/1354066120969800

Duan, T., & Dinavahi, V. (2021). Starlink Space Network-Enhanced Cyber–Physical Power System. *IEEE Transactions on Smart Grid*, *12*(4), 3673–3675. https://doi.org/10.1109/tsg.2021.3068046

Dunaj, K. (2023). EU STANDARDS FOR PROTECTING THE RIGHT TO PRIVACY IN THE AREA OF CYBERSECURITY. *Kwartalnik Prawa Międzynarodowego*, *III*(III), 1–19. https://doi.org/10.5604/01.3001.0053.8851

Duncombe, C. (2019). Digital Diplomacy: Emotion and identity in the public realm. *The Hague Journal of Diplomacy*, *14*(1–2), 102–116. https://doi.org/10.1163/1871191x-14101016

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity*, *5*(1). https://doi.org/10.1093/cybsec/tyz013

Durojaye, H., & Raji, O. (2022). Impact of state and state sponsored actors on the cyber environment and the future of critical infrastructure. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2212.08036

Dylan, H., Gioe, D. V., & Goodman, M. S. (2020). Entering the electoral fray: the CIA and Russian meddling in the 2016 election. In *Edinburgh University Press eBooks* (pp. 481–492). https://doi.org/10.3366/edinburgh/9781474428842.003.0024

Efrony, D., & Shany, Y. (2018). A rule book on the shelf? Tallinn Manual 2.0 on Cyber operations and subsequent state practice. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3172743

Eggenschwiler, J. (2020). Expert commissions and norms of responsible behaviour in cyberspace: a review of the activities of the GCSC. *Digital Policy Regulation and Governance*, *22*(2), 93–107. https://doi.org/10.1108/dprg-03-2019-0019

Ehsan, N. S. B., & Saquib, N. M. N. (2024). BALANCING CYBERSECURITY AND INDIVIDUAL RIGHTS: A CRITICAL ANALYSIS OF BANGLADESH'S CYBER SECURITY ACT 2023. *Journal of Creative Writing.*, *8*(1), 85–98. https://doi.org/10.70771/jocw.v8i1.109

Elliott, D. (2011). Deterring strategic cyberattack. *IEEE Security & Privacy*, *9*(5), 36–40. https://doi.org/10.1109/msp.2011.24

Embar-Seddon, A. (2002). Cyberterrorism. *American Behavioral Scientist*, *45*(6), 1033–1043. https://doi.org/10.1177/0002764202045006007

Eun, Y., & Aßmann, J. S. (2014). Cyberwar: Taking stock of security and warfare in the digital age. *International Studies Perspectives*, n/a. https://doi.org/10.1111/insp.12073

Falco, G., Viswanathan, A., Caldera, C., & Shrobe, H. (2018). A master attack methodology for an AI-Based automated attack planner for smart cities. *IEEE Access*, *6*, 48360–48373. https://doi.org/10.1109/access.2018.2867556

Fang, B. (2018). Main initiatives to safeguard cyberspace sovereignty. In *Springer eBooks* (pp. 439–478). https://doi.org/10.1007/978-981-13-0320-3_12

Farrell, H., & Newman, A. L. (2014). Domestic Institutions beyond the Nation-State: Charting the New Interdependence Approach. *World Politics*, *66*(2), 331–363. https://doi.org/10.1017/s0043887114000057

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber War. *Survival*, *53*(1), 23–40. https://doi.org/10.1080/00396338.2011.555586

Fernández-I-Marín, X., Knill, C., Steinbacher, C., & Steinebach, Y. (2023). Bureaucratic Quality and the Gap between Implementation Burden and Administrative Capacities. *American Political Science Review*, *118*(3), 1240–1260. https://doi.org/10.1017/s0003055423001090

Fernández, D. P. (2023). Restraining ICANN: An analysis of OFAC sanctions and their impact on the Internet Corporation for Assigned Names and Numbers. *Telecommunications Policy*, *47*(8), 102614. https://doi.org/10.1016/j.telpol.2023.102614

Fernback, J. (2007). Beyond the diluted community concept: a symbolic interactionist perspective on online social relations. *New Media & Society*, *9*(1), 49–69. https://doi.org/10.1177/1461444807072417

Finnemore, M., & Sikkink, K. (2001). TAKINGSTOCK: The Constructivist Research Program in International Relations and Comparative Politics. *Annual Review of Political Science*, *4*(1), 391–416. https://doi.org/10.1146/annurev.polisci.4.1.391

Fisher, B., Margolis, M., & Resnick, D. (1996). SURVEYING THE INTERNET: DEMOCRATIC THEORY AND CIVIC LIFE IN CYBERSPACE. *Southeastern Political Review*, *24*(3), 399–429. https://doi.org/10.1111/j.1747-1346.1996.tb00088.x

Flechais, I., & Chalhoub, G. (2023). Practical Cybersecurity Ethics: Mapping CYBOK to Ethical Concerns. *New Security Paradigms Workshop*, 62–75. https://doi.org/10.1145/3633500.3633505

Fletcher, N. (2007). Challenges for regulating financial fraud in cyberspace. *Journal of Financial Crime*, *14*(2), 190–207. https://doi.org/10.1108/13590790710742672

Fordham, B. O. (2011). Who wants to be a major power? Explaining the expansion of foreign policy ambition. *Journal of Peace Research*, *48*(5), 587–603. https://doi.org/10.1177/0022343311411959

Formosa, P., Wilson, M., & Richards, D. (2021). A principlist framework for cybersecurity ethics. *Computers & Security*, *109*, 102382. https://doi.org/10.1016/j.cose.2021.102382

Forsythe, D. P. (2012). Introduction: human rights in international relations. In *Cambridge University Press eBooks* (pp. 3–36). https://doi.org/10.1017/cbo9781139059114.005

Foulon, M., & Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. *Contemporary Security Policy*, *45*(3), 426–458. https://doi.org/10.1080/13523260.2024.2365062

Francois, C., & Lin, H. (2021). The strategic surprise of Russian information operations on social media in 2016 in the United States: mapping a blind spot. *Journal of Cyber Policy*, *6*(1), 9–30. https://doi.org/10.1080/23738871.2021.1950196

French, G. S. (2004). *Rethinking defensive information warfare*. https://doi.org/10.21236/ada465836

Friedberg, I., Skopik, F., Settanni, G., & Fiedler, R. (2014). Combating advanced persistent threats: From network event correlation to incident detection. *Computers & Security*, *48*, 35–57. https://doi.org/10.1016/j.cose.2014.09.006

Furtuna, P. (2021). THE DEMOCRATIC PEACE IN THE THEORY OF INTERNATIONAL RELATIONS. *Administrarea Publica*, *2 (110)*, 128–133. https://doi.org/10.52327/1813-8489.2021.2(110).10

Gao, C., Guo, Q., Jiang, D., Wang, Z., Fang, C., & Hao, M. (2019). Theoretical basis and technical methods of cyberspace geography. *Journal of Geographical Sciences*, *29*(12), 1949–1964. https://doi.org/10.1007/s11442-019-1698-7

Gao, X. (2022). An attractive alternative? China's approach to cyber governance and its implications for the Western model. *The International Spectator*, *57*(3), 15–30. https://doi.org/10.1080/03932729.2022.2074710

Gartzke, E. (2000). Preferences and the democratic peace. *International Studies Quarterly*, *44*(2), 191–212. https://doi.org/10.1111/0020-8833.00155

Gartzke, E., Li, Q., & Boehmer, C. (2001). Investing in the peace: economic interdependence and international conflict. *International Organization*, *55*(2), 391–438. https://doi.org/10.1162/00208180151140612

Geers, K. (2010). The challenge of cyber attack deterrence. *Computer Law & Security Review*, *26*(3), 298–303. https://doi.org/10.1016/j.clsr.2010.03.003

Gelvin, J. L. (2008). Al-Qaeda and anarchism: A Historian's reply to Terrorology. *Terrorism and Political Violence*, *20*(4), 563–581. https://doi.org/10.1080/09546550802257291

Gillard, S., David, D. P., Mermoud, A., & Maillart, T. (2023). Efficient collective action for tackling time-critical cybersecurity threats. *Journal of Cybersecurity*, *9*(1). https://doi.org/10.1093/cybsec/tyad021

Goldgeier, J. M., & McFaul, M. (1992). A tale of two worlds: core and periphery in the post-cold war era. *International Organization*, *46*(2), 467–491. https://doi.org/10.1017/s0020818300027788

Gondal, A. R. (2017). Cyber Warfare and International Humantarian Law. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2969778

González-Manzano, L., De Fuentes, J. M., Lombardi, F., & Ramos, C. (2023). A technical characterization of APTs by leveraging public resources. *International Journal of Information Security*, *22*(6), 1567–1584. https://doi.org/10.1007/s10207-023-00706-x

Gordon, W. J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R. J., Kadakia, J., Kufahl, J., Mazzone, C., Noga, J., Parkulo, M., Sanford, B., Scheib, P., & Landman, A. B. (2019). Assessment of employee susceptibility to phishing attacks at US health care institutions. *JAMA Network Open*, *2*(3), e190393. https://doi.org/10.1001/jamanetworkopen.2019.0393

Gould, D. (2019). Organizational resilience approaches to cyber security. *IGI Global eBooks*, 1189–1199. https://doi.org/10.4018/978-1-5225-8897-9.ch057

Government agencies and private companies undertake actions to limit the impact of foreign influence and interference in the 2020 U.S. election. (2021). *American Journal of International Law*, *115*(2), 309–317. https://doi.org/10.1017/ajil.2021.10

Granåsen, M., & Andersson, D. (2015). Measuring team effectiveness in cyber-defense exercises: a cross-disciplinary case study. *Cognition Technology & Work*, *18*(1), 121–143. https://doi.org/10.1007/s10111-015-0350-2

Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Penguin Random House.

Greenberg, A., & Excerpt. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history. *WIRED*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Guitton, M. J., & Fréchette, J. (2023). Facing cyberthreats in a crisis and post-crisis era: Rethinking security services response strategy. *Computers in Human Behavior Reports*, *10*, 100282. https://doi.org/10.1016/j.chbr.2023.100282

Gunnarson, R. S. (2011). Theorizing Fact-Based policy development at ICANN. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2809683

Gupta, N. M. P. R. S. (2023). Ethical Hacking and Penetration Testing: Securing digital assets and networks. *International Journal of Advanced Research in Science Communication and Technology*, 140–144. https://doi.org/10.48175/ijarsct-12422

Guzzini, S. (2004). The enduring dilemmas of realism in international relations. *European Journal of International Relations*, *10*(4), 533–568. https://doi.org/10.1177/1354066104047848

Haataja, S. (2022). Cyber operations against critical infrastructure under norms of responsible state behaviour and international law. *International Journal of Law and Information Technology*, *30*(4), 423–443. https://doi.org/10.1093/ijlit/eaad006

Habib, A. A., Hasan, M. K., Alkhayyat, A., Islam, S., Sharma, R., & Alkwai, L. M. (2023). False data injection attack in smart grid cyber physical system: Issues, challenges, and future direction. *Computers & Electrical Engineering*, *107*, 108638. https://doi.org/10.1016/j.compeleceng.2023.108638

Halliday, F. (1994). State and Society in International Relations. In *Rethinking International Relations* (pp. 74–93). Bloomsbury. https://doi.org/10.1007/978-1-349-23658-9_4

Han, R. (2018). Contesting cyberspace in China. In *Columbia University Press eBooks*. https://doi.org/10.7312/han-18474

Hani, U., Sohaib, O., Khan, K., Aleidi, A., & Islam, N. (2024). Psychological profiling of hackers via machine learning toward sustainable cybersecurity. *Frontiers in Computer Science*, *6*. https://doi.org/10.3389/fcomp.2024.1381351

Hansen, J. V., Lowry, P. B., Meservy, R. D., & McDonald, D. M. (2006). Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection. *Decision Support Systems*, *43*(4), 1362–1374. https://doi.org/10.1016/j.dss.2006.04.004

Harknett, R. J., & Nye, J. S. (2017). Is deterrence possible in cyberspace? *International Security*, *42*(2), 196–199. https://doi.org/10.1162/isec_c_00290

Harknett, R. J., & Smeets, M. (2020). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*, *45*(4), 534–567. https://doi.org/10.1080/01402390.2020.1732354

Hart, R. B. J. (2001). The governance of Cyberspace: politics, technology and global restructuring. *The Information Society*, *17*(2), 143–144. https://doi.org/10.1080/019722401750175702

He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2019). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital*, *21*(2), 203–213. https://doi.org/10.1108/jic-05-2019-0112

Healey, J. (2019). The implications of persistent (and permanent) engagement in cyberspace. *Journal of Cybersecurity*, *5*(1). https://doi.org/10.1093/cybsec/tyz008

Herbst, L., & Jakobi, A. P. (2024). Opening up or closing down? Non-state actors in UN cybersecurity governance. *Journal of Global Security Studies*, *9*(3). https://doi.org/10.1093/jogss/ogae026

Herrick, D., & Herr, T. (2016). Combating complexity: offensive cyber capabilities and integrated warfighting. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2845709

Herrmann, D. (2019). Cyber espionage and Cyber defence. In *Springer eBooks* (pp. 83–106). https://doi.org/10.1007/978-3-658-25652-4_5

Hirata, K. (2008). International norms and civil Society: New influences on Japanese security policy. In *Palgrave Macmillan US eBooks* (pp. 47–70). https://doi.org/10.1057/9780230615809_3

Hitchens, T., & Gallagher, N. W. (2019). Building confidence in the cybersphere: a path to multilateral progress. *Journal of Cyber Policy*, *4*(1), 4–21. https://doi.org/10.1080/23738871.2019.1599032

Hobson, C. (2011). Towards a critical theory of democratic peace. *Review of International Studies*, *37*(4), 1903–1922. https://doi.org/10.1017/s0260210510001634

Hobson, J. M., & Sharman, J. C. (2005). The enduring place of hierarchy in world politics: Tracing the social logics of hierarchy and political change. *European Journal of International Relations*, *11*(1), 63–98. https://doi.org/10.1177/1354066105050137

Hoffman, L., Burley, D., & Toregas, C. (2011). Holistically building the cybersecurity workforce. *IEEE Security & Privacy*, *10*(2), 33–39. https://doi.org/10.1109/msp.2011.181

Hofmann, J. (2016). Multi-stakeholderism in Internet governance: putting a fiction into practice. *Journal of Cyber Policy*, *1*(1), 29–49. https://doi.org/10.1080/23738871.2016.1158303

Holden, P. (2016). Eternal potential? Temporality, complexity and the incoherent power of the European Union. *Cooperation and Conflict*, *51*(4), 407–427. https://doi.org/10.1177/0010836716668786

Holsti, K. J. (1978). A new international politics? Diplomacy in complex interdependence. *International Organization*, *32*(2), 513–530. https://doi.org/10.1017/s002081830002662x

Hom, A. R. (2018). Silent Order: the Temporal Turn in Critical International Relations. *Millennium Journal of International Studies*, *46*(3), 303–330. https://doi.org/10.1177/0305829818771349

Hom, A. R. (2020). International relations and the problem of time. In *Oxford University Press eBooks*. https://doi.org/10.1093/oso/9780198850014.001.0001

Homburger, Z. (2019). The necessity and pitfall of Cybersecurity Capacity building for norm development in cyberspace. *Global Society*, *33*(2), 224–242. https://doi.org/10.1080/13600826.2019.1569502

Howie, E. (2017). Protecting the human right to freedom of expression in international law. *International Journal of Speech-Language Pathology*, *20*(1), 12–15. https://doi.org/10.1080/17549507.2018.1392612

Huang, L., & Zhu, Q. (2019). A dynamic games approach to proactive defense strategies against Advanced Persistent Threats in cyber-physical systems. *Computers & Security*, *89*, 101660. https://doi.org/10.1016/j.cose.2019.101660

Huang, Z. A., & Arceneaux, P. (2024). Ethical challenges in the digitalization of public diplomacy. In *Oxford University Press eBooks* (pp. 232–249). https://doi.org/10.1093/oxfordhb/9780192859198.013.13

Human *rights, digital society and the law*. (2019). https://doi.org/10.4324/9781351025386

Hunter, L. Y., Albert, C. D., Garrett, E., & Rutland, J. (2022). Democracy and cyberconflict: how regime type affects state-sponsored cyberattacks. *Journal of Cyber Policy*, *7*(1), 72–94. https://doi.org/10.1080/23738871.2022.2041060

Hurel, L. M., & Lobato, L. C. (2018). Unpacking Cyber Norms: Private companies as norm Entrepreneurs. *Journal of Cyber Policy*, *3*(1), 61–76. https://doi.org/10.1080/23738871.2018.1467942

Iasiello, E. (2014). Is cyber deterrence an illusory course of action? *Journal of Strategic Security*, *7*(1), 54–67. https://doi.org/10.5038/1944-0472.7.1.5

Iftikhar, S. (2024). Cyberterrorism as a global threat: a review on repercussions and countermeasures. *PeerJ Computer Science*, *10*, e1772. https://doi.org/10.7717/peerj-cs.1772

Ikenberry, G. J., Russett, B. M., & Oneal, J. R. (2001). Triangulating peace: democracy, interdependence, and international organizations. *Foreign Affairs*, *80*(3), 131. https://doi.org/10.2307/20050168

Ikwu, R. (2019). Identifying Data and Information Streams in Cyberspace: A Multi-Dimensional Perspective. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.1906.03757

Isnarti, R. (2016). A comparison of neorealism, liberalism, and constructivism in analysing cyber war. *Andalas Journal of International Studies (AJIS)*, *5*(2), 151. https://doi.org/10.25077/ajis.5.2.151-165.2016

Iswardhana, M. R. (2021). Cyber diplomacy and protection measures against threats of information communication technology in Indonesia. *Journal of Islamic World and Politics*, *5*(2), 343–367. https://doi.org/10.18196/jiwp.v5i2.12242

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Jayawardane, S., Larik, J., & Kaul, M. (2016). Governing cyberspace: building confidence, capacity and consensus. *Global Policy*, *7*(1), 66–68. https://doi.org/10.1111/1758-5899.12286

Jiang, B., You, X., Li, K., Li, T., Wang, X., & Si, D. (2024). Virtual geo-cyber environments: metaphorical visualization of virtual cyberspace with geographical knowledge. *International Journal of Digital Earth*, *17*(1). https://doi.org/10.1080/17538947.2024.2324959

Jiang, Y., Jeusfeld, M. A., Ding, J., & Sandahl, E. (2023). Model-Based Cybersecurity analysis. *Business & Information Systems Engineering*, *65*(6), 643–676. https://doi.org/10.1007/s12599-023-00811-0

Johnson, C. W. (2013). Anti-social networking: crowdsourcing and the cyber defence of national critical infrastructures. *Ergonomics*, *57*(3), 419–433. https://doi.org/10.1080/00140139.2013.812749

Johnson, D. E. (2019). Russian election interference and Race-Baiting. *Columbia Journal of Race and Law*, *9*(2), 191–264. https://doi.org/10.7916/cjrl.v9i2.3409

Jordan, T. (2002). Cyberpower: The culture and politics of cyberspace and the internet. *Contemporary Sociology a Journal of Reviews*, *31*(3), 290. https://doi.org/10.2307/3089671

Jovanovski, Z., Iliev, A., & Nikolovska, A. I. (2020). Historical perspectives and legal aspects of cyber warfare. *Annals of Disaster Risk Sciences*, *3*(2). https://doi.org/10.51381/adrs.v3i2.53

Joyner, C. C. (2001). Information Warfare as international Coercion: Elements of a legal framework. *European Journal of International Law*, *12*(5), 825–865. https://doi.org/10.1093/ejil/12.5.825

Junio, T. J. (2013). How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate. *Journal of Strategic Studies*, *36*(1), 125–133. https://doi.org/10.1080/01402390.2012.739561

Kaiser, P. (1995). State-Society relations in an international context: The case of Aga Khan Health-Care Initiatives in Tanzania. *International Journal of Comparative Sociology*, *36*(3–4), 184–197. https://doi.org/10.1177/002071529503600305

Kane, A. (2014). The Rocky Road to Consensus: The work of UN groups of governmental experts in the field of ICTs and in the context of international Security, 1998–2013. *American Foreign Policy Interests*, *36*(5), 314–321. https://doi.org/10.1080/10803920.2014.969175

Kanet, R. E. (2024). Moscow and the world: From Soviet active measures to Russian information warfare. *Applied Cybersecurity & Internet Governance*. https://doi.org/10.60097/acig/162742

Karakoç, J. (2010). The Impact of the Kurdish Identity on Turkey's Foreign Policy from the 1980s to 2008. *Middle Eastern Studies*, *46*(6), 919–942. https://doi.org/10.1080/00263206.2010.520423

Karakuş, M., & Ak, Ö. (2022). Pornification of the cyberspace during intrastate conflicts. In *Advances in religious and cultural studies (ARCS) book series* (pp. 189–210). https://doi.org/10.4018/978-1-6684-4964-6.ch011

Karnouskos, S. (2011). Stuxnet worm impact on industrial cyber-physical system security. *IECON 2020 the 46th Annual Conference of the IEEE Industrial Electronics Society*, 4490–4494. https://doi.org/10.1109/iecon.2011.6120048

Kasper, A., & Krasznay, C. (2019). Towards Pollution-Control in Cyberspace: problem structure and institutional design in international cybersecurity. *Mezinárodní a Srovnávací Právní Revue/International and Comparative Law Review*, *19*(2), 76–96. https://doi.org/10.2478/iclr-2019-0015

Katagiri, N. (2021). Why international law and norms do little in preventing non-state cyber attacks. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab009

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to theory and statecraft. *International Security*, *38*(2), 7–40. https://doi.org/10.1162/isec_a_00138

Kello, L. (2024). Digital diplomacy and cyber defence. In *Oxford University Press eBooks* (pp. 121–137). https://doi.org/10.1093/oxfordhb/9780192859198.013.7

Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., & Díaz-Castaño, N. (2021). Empty streets, busy internet: A Time-Series analysis of cybercrime and fraud trends during COVID-19. *Journal of Contemporary Criminal Justice*, *37*(4), 480–501. https://doi.org/10.1177/10439862211027986

Keohane, R. O. (2012). Twenty years of institutional liberalism. *International Relations*, *26*(2), 125–138. https://doi.org/10.1177/0047117812438451

Ketteman, M. C. (2017). Ensuring cybersecurity through international law. *Revista Española De Derecho Internacional*, *69*(2), 281–289. https://doi.org/10.17103/redi.69.2.2017.2.01

Khanna, P. (2018). STATE SOVEREIGNTY AND SELF-DEFENCE IN CYBERSPACE. *BRICS Law Journal*, *5*(4), 139–154. https://doi.org/10.21684/2412-2343-2018-5-4-139-154

Khasanova, L., & Tai, K. (2024). Shades of authoritarian digital sovereignty: divergences in Russian and Chinese data localisation regimes. *Journal of Cyber Policy*, 1–25. https://doi.org/10.1080/23738871.2024.2413938

Kim, M. (2022). North Korea's cyber capabilities and their implications for international security. *Sustainability, 14*(3), 1744. https://doi.org/10.3390/su14031744

Kitchin, R. M. (1998). Towards geographies of cyberspace. *Progress in Human Geography, 22*(3), 385–406. https://doi.org/10.1191/030913298668331585

Kittichaisaree, K. (2017). Jurisdiction and attribution of state responsibility in cyberspace. In *Law, governance and technology series* (pp. 23–44). https://doi.org/10.1007/978-3-319-54657-5_2

Klein, H. (2002). ICANN and Internet Governance: Leveraging technical coordination to realize global public policy. *The Information Society, 18*(3), 193–207. https://doi.org/10.1080/01972240290074959

Klimburg, A. (2011). Mobilising cyber power. *Survival, 53*(1), 41–60. https://doi.org/10.1080/00396338.2011.555595

Kobrin, S. J. (2001). Territoriality and the governance of cyberspace. *Journal of International Business Studies, 32*(4), 687–704. https://doi.org/10.1057/palgrave.jibs.8490990

Kohler, C. (2020). The EU Cybersecurity Act and European standards: an introduction to the role of European standardization. *International Cybersecurity Law Review, 1*(1–2), 7–12. https://doi.org/10.1365/s43439-020-00008-1

Kono, D. Y. (2007). Making anarchy work: international legal institutions and trade cooperation. *The Journal of Politics, 69*(3), 746–759. https://doi.org/10.1111/j.1468-2508.2007.00572.x

Kozub, M., & Mitręga, A. (2021). Strategic Thinking about Security in Cyberspace. *Rocznik Bezpieczeństwa Morskiego, XV-Wydanie specjalne*, 1–28. https://doi.org/10.5604/01.3001.0015.5893

Kraemer-Mbula, E., Tang, P., & Rush, H. (2012). The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change, 80*(3), 541–555. https://doi.org/10.1016/j.techfore.2012.07.002

Kramer, F. D. (2011). Cyberpower and National Security: In *University of Nebraska Press eBooks* (pp. 3–23). https://doi.org/10.2307/j.ctt1djmhj1.6

Kroll, J. A. (1993). The complexity of interdependence. *International Studies Quarterly, 37*(3), 321. https://doi.org/10.2307/2600811

Kshetri, N. (2015). India's cybersecurity landscape: the roles of the private sector and Public-Private Partnership. *IEEE Security & Privacy, 13*(3), 16–23. https://doi.org/10.1109/msp.2015.61

Kulikova, A. (2021). Cyber norms: technical extensions and technological challenges. *Journal of Cyber Policy, 6*(3), 340–359. https://doi.org/10.1080/23738871.2021.2020316

Kututung, R. M. N., & Triwahyuni, D. (2024). THE SETTLEMENT OF COMPETITION BETWEEN THE UNITED STATES AND CHINA IN CYBERSPACE IN THE PERSPECTIVE OF LIBERALISM. *Proceeding of International Conference on Business Economics Social Sciences and Humanities*, *7*(1), 1120–1130. https://doi.org/10.34010/icobest.v7i.625

Labazanova, S. L., Kaimova, F. A., & Isaeva, L. M. (2023). INTEGRATING CYBER SECURITY INTO STRATEGIC MANAGEMENT. *EKONOMIKA I UPRAVLENIE PROBLEMY RESHENIYA*, *10/6*(139), 23–30. https://doi.org/10.36871/ek.up.p.r.2023.10.06.003

Landman, T. (2005). The political science of human rights. *British Journal of Political Science*, *35*(3), 549–572. https://doi.org/10.1017/s0007123405000293

Lanoszka, A. (2018). Disinformation in international politics. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3172349

Lantis, J. S., & Bloomberg, D. J. (2018). Changing the code? Norm contestation and US antipreneurism in cyberspace. *International Relations*, *32*(2), 149–172. https://doi.org/10.1177/0047117818763006

Layne, C. (1994). Kant or Cant: The myth of the Democratic Peace. *International Security*, *19*(2), 5. https://doi.org/10.2307/2539195

Le, T. D., Le-Dinh, T., & Uwizeyemungu, S. (2024). Search engine optimization poisoning: A cybersecurity threat analysis and mitigation strategies for small and medium-sized enterprises. *Technology in Society*, *76*, 102470. https://doi.org/10.1016/j.techsoc.2024.102470

Leal, M. M., & Musgrave, P. (2023). Backwards from zero: How the U.S. public evaluates the use of zero-day vulnerabilities in cybersecurity. *Contemporary Security Policy*, *44*(3), 437–461. https://doi.org/10.1080/13523260.2023.2216112

Legro, J. W., & Moravcsik, A. (1999). Is anybody still a realist? *International Security*, *24*(2), 5–55. https://doi.org/10.1162/016228899560130

Leitner, M., Pahi, T., & Skopik, F. (2017). Situational awareness for strategic decision making on a national level. In *Auerbach Publications eBooks* (pp. 225–276). https://doi.org/10.4324/9781315397900-6

Levinson, N. S., & Marzouki, M. (2015). Internet Governance Institutionalization: Process and Trajectories. In *Palgrave Macmillan US eBooks* (pp. 17–35). https://doi.org/10.1057/9781137515209_2

Lewis, J. (2021). Shaping the ground for bilateral cybersecurity negotiations. *China International Strategy Review*, *3*(1), 115–122. https://doi.org/10.1007/s42533-021-00081-z

Li, M. (2024). A cross-platform comparison of China's confrontational diplomatic communication. *Journal of International Communication*, 1–22. https://doi.org/10.1080/13216597.2024.2335960

Li, Q. (2022). Network security management and protection in the context of emerging technologies. In *Lecture notes on data engineering and communications technologies* (pp. 192–198). https://doi.org/10.1007/978-3-030-96908-0_24

Li, Y., Dai, W., Bai, J., Gan, X., Wang, J., & Wang, X. (2018). An Intelligence-Driven Security-Aware defense mechanism for advanced persistent threats. *IEEE Transactions on Information Forensics and Security*, *14*(3), 646–661. https://doi.org/10.1109/tifs.2018.2847671

Liaropoulos, A. N. (2017). Cyberspace governance and state sovereignty. In *Springer eBooks* (pp. 25–35). https://doi.org/10.1007/978-3-319-52168-8_2

Libicki, M. (2017). It Takes More than Offensive Capability to Have an Effective Cyberdeterrence Posture. In *RAND Corporation eBooks*. https://doi.org/10.7249/ct465

Libicki, M. C. (2007). Hostile conquest as information warfare. In *Cambridge University Press eBooks* (pp. 15–49). https://doi.org/10.1017/cbo9780511804250.002

Liff, A. P. (2012). Cyberwar: a new 'Absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies*, *35*(3), 401–428. https://doi.org/10.1080/01402390.2012.663252

Lin, H. (2020). On the organization of the U.S. government for responding to adversarial information warfare and influence operations. In *Routledge eBooks* (pp. 166–185). https://doi.org/10.4324/9780429470509-11

Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., & Ebner, N. C. (2019). Susceptibility to Spear-Phishing emails. *ACM Transactions on Computer-Human Interaction*, *26*(5), 1–28. https://doi.org/10.1145/3336141

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, *22*(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

Lindsay, J. R. (2015). Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity*, tyv003. https://doi.org/10.1093/cybsec/tyv003

Linkov, I., Trump, B. D., Trump, J., Pescaroli, G., Hynes, W., Mavrodieva, A., & Panda, A. (2022). Resilience stress testing for critical infrastructure. *International Journal of Disaster Risk Reduction*, *82*, 103323. https://doi.org/10.1016/j.ijdrr.2022.103323

Liu, D., Wang, X., & Camp, J. (2008). Game-theoretic modeling and analysis of insider threats. *International Journal of Critical Infrastructure Protection*, *1*, 75–80. https://doi.org/10.1016/j.ijcip.2008.08.001

Liu, J. (2023). Cyber policies are needed. *Interdisciplinary Humanities and Communication Studies*, *1*(3). https://doi.org/10.61173/x97gh144

Liu, X., Qian, C., Hatcher, W. G., Xu, H., Liao, W., & Yu, W. (2019). Secure Internet of Things (IoT)-Based Smart-World Critical Infrastructures: Survey, case study and research opportunities. *IEEE Access*, *7*, 79523–79544. https://doi.org/10.1109/access.2019.2920763

Liu, Y., Hu, S., & Zomaya, A. Y. (2016). The hierarchical Smart home cyberattack detection considering power overloading and frequency disturbance. *IEEE Transactions on Industrial Informatics*, *12*(5), 1973–1983. https://doi.org/10.1109/tii.2016.2591911

Liu, Z., & Wang, L. (2020). Defense strategy against load redistribution attacks on power systems considering insider threats. *IEEE Transactions on Smart Grid*, *12*(2), 1529–1540. https://doi.org/10.1109/tsg.2020.3023426

Loader, B. (2003). The governance of cyberspace. In *Routledge eBooks* (1st ed.). Routledge. https://doi.org/10.4324/9780203360408

Lobell, S. E. (2018). A granular theory of balancing. *International Studies Quarterly*, *62*(3), 593–605. https://doi.org/10.1093/isq/sqy011

Loi, M., & Christen, M. (2020). Ethical frameworks for Cybersecurity. In *˜The œInternational library of ethics, law and technology* (pp. 73–95). https://doi.org/10.1007/978-3-030-29053-5_4

Lonsdale, D. J., & Kane, T. M. (2019). Cyber power. In *Routledge eBooks* (pp. 236–265). https://doi.org/10.4324/9781315163536-12

Loubet, G., Takacs, A., & Dragomirescu, D. (2019). Implementation of a Battery-Free wireless sensor for Cyber-Physical systems dedicated to structural health monitoring applications. *IEEE Access*, *7*, 24679–24690. https://doi.org/10.1109/access.2019.2900161

Macfadyen, L. P. (2006). The prospects for identity and community in cyberspace. In *IGI Global eBooks* (pp. 471–478). https://doi.org/10.4018/978-1-59140-562-7.ch071

Macnish, K., & Van Der Ham, J. (2020). Ethics in cybersecurity research and practice. *Technology in Society*, *63*, 101382. https://doi.org/10.1016/j.techsoc.2020.101382

Madnick, S., Choucri, N., & Ferwerda, J. (2011). Institutional Foundations for Cyber Security: current responses and new challenges. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2338649

Maillart, T., Zhao, M., Grossklags, J., & Chuang, J. (2017). Given enough eyeballs, all bugs are shallow? Revisiting Eric Raymond with bug bounty programs. *Journal of Cybersecurity*, *3*(2), 81–90. https://doi.org/10.1093/cybsec/tyx008

Maimó, L. F., Celdrán, A. H., Gómez, Á. L. P., Clemente, F. J. G., Weimer, J., & Lee, I. (2019). Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments. *Sensors*, *19*(5), 1114. https://doi.org/10.3390/s19051114

Mainwaring, S. (2020). Always in control? Sovereign states in cyberspace. *European Journal of International Security*, *5*(2), 215–232. https://doi.org/10.1017/eis.2020.4

Maiorca, D., Biggio, B., & Giacinto, G. (2019). Towards adversarial malware detection. *ACM Computing Surveys*, *52*(4), 1–36. https://doi.org/10.1145/3332184

Malcolm, J. (2015). Criteria of meaningful stakeholder inclusion in internet governance. *Internet Policy Review*, *4*(4). https://doi.org/10.14763/2015.4.391

Mammadrzali, S. (2020). Captain America protecting digital rights: "old school" national law vs. emerging internet complexities in Azerbaijan. *Vilnius University Open Series*, *6*, 132–145. https://doi.org/10.15388/os.law.2020.12

Manantan, M. B. F. (2021). Advancing cyber diplomacy in the Asia Pacific: Japan and Australia. *Australian Journal of International Affairs*, *75*(4), 432–459. https://doi.org/10.1080/10357718.2021.1926423

Manley, M. (2015). Cyberspace's dynamic duo: Forging a Cybersecurity Public-Private partnership. *Journal of Strategic Security*, *8*(3Suppl), 85–98. https://doi.org/10.5038/1944-0472.8.3s.1478

Manoilo, A., Borisova, A., Telichko, V., & Petrenko, A. (2019). Information warfare technologies and psychological operations within international relations and world politics. *˜the œEuropean Proceedings of Social & Behavioural Sciences*, 2128–2137. https://doi.org/10.15405/epsbs.2019.12.04.286

Mantelero, A., Vaciago, G., Esposito, M. S., & Monte, N. (2020). The common EU approach to personal data and cybersecurity regulation. *International Journal of Law and Information Technology*, *28*(4), 297–328. https://doi.org/10.1093/ijlit/eaaa021

Marcella, A. J. (2021). Cyber forensics. In *CRC Press eBooks* (pp. 87–144). https://doi.org/10.1201/9781003057888-3

Mareš, M., & Mlejnková, P. (2021). Propaganda and disinformation as a security threat. In *Political campaigning and communication* (pp. 75–103). https://doi.org/10.1007/978-3-030-58624-9_3

Martin, G., Kinross, J., & Hankin, C. (2017). Effective cybersecurity is fundamental to patient safety. *BMJ*, j2375. https://doi.org/10.1136/bmj.j2375

Martin, J. J. (2020). Hacks dangerous to human life: Using JASTA to overcome foreign state sovereign immunity in cyberattack cases. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3542617

Mastanduno, M., Lake, D. A., & Ikenberry, G. J. (1989). Toward a realist theory of state action. *International Studies Quarterly*, *33*(4), 457. https://doi.org/10.2307/2600522

Matei, G. I. (2024). Cross-Border Data Sharing and Sovereignty: Reactions of Non-EU Countries to Article 32 of the Budapest Convention. *Law And Economy*, *3*(9), 1–8. https://doi.org/10.56397/le.2024.09.01

Mathiesen, K. (2008). Access to information as a human right. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1264666

Matusitz, J. (2014). Intercultural Perspectives on Cyberspace: An updated Examination. *Journal of Human Behavior in the Social Environment*, *24*(7), 713–724. https://doi.org/10.1080/10911359.2013.849223

Maulana, Y. I., & Fajar, I. (2023). Analysis of Cyber Diplomacy and its Challenges for the Digital Era Community. *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, *4*(2), 169–177. https://doi.org/10.34306/itsdi.v4i2.587

McCourt, D. M. (2011). The roles states play: a Meadian interactionist approach. *Journal of International Relations and Development*, *15*(3), 370–392. https://doi.org/10.1057/jird.2011.26

McIlvenny, P. (1999). Avatars r US? Discourses of Community and Embodiment in Intercultural Cyberspace. *Journal of Intercultural Communication*, *1*(1), 1–11. https://doi.org/10.36923/jicc.v1i1.356

McIntosh, C. (2015). Theory across time: the privileging of time-less theory in international relations. *International Theory*, *7*(3), 464–500. https://doi.org/10.1017/s1752971915000147

Mearsheimer, J. J. (1995). A realist reply. *International Security*, *20*(1), 82. https://doi.org/10.2307/2539218

Melaku, H. M. (2023). A dynamic and adaptive cybersecurity governance framework. *Journal of Cybersecurity and Privacy*, *3*(3), 327–350. https://doi.org/10.3390/jcp3030017

Merlino, V., & Allegra, D. (2024). Energy-based approach for attack detection in IoT devices: A survey. *Internet of Things*, *27*, 101306. https://doi.org/10.1016/j.iot.2024.101306

Milewski, D. (2020). The analysis of narratives and Disinformation in the global information environment amid COVID-19 Pandemic. *EUROPEAN RESEARCH STUDIES JOURNAL*, *XXIII*(Special Issue 3), 3–17. https://doi.org/10.35808/ersj/1848

Milik, P. (2021). International legal regulations in the area of cybersecurity. *Cybersecurity and Law*, *1*(1), 115–141. https://doi.org/10.35467/cal/133774

Minchev, Z. (2023). On the Growing Transformational Role of AI Technologies for the Future Cyber Diplomacy in the Post-Information Age. *Proceedings of the. . . International Conference on Virtual Learning*, *4*, 29–41. https://doi.org/10.54852/ijcd.v4y202303

Ming, X. (2022). Understanding Cyberculture from Perspective of Intercultural Communication. *Advances in Social Science, Education and Humanities*

Research/Advances in Social Science, Education and Humanities Research. https://doi.org/10.2991/assehr.k.220105.023

Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security*, *120*, 102820. https://doi.org/10.1016/j.cose.2022.102820

Mishra, N., Islam, S. H., & Zeadally, S. (2023). A survey on security and cryptographic perspective of Industrial-Internet-of-Things. *Internet of Things*, *25*, 101037. https://doi.org/10.1016/j.iot.2023.101037

Mitrović, M. (2018). Genesis of propaganda as a strategic means of hybrid warfare concept. *Vojno Delo*, *70*(1), 34–49. https://doi.org/10.5937/vojdelo1801034m

Mohammed, A., Benson, V., & Saridakis, G. (2020). Understanding the relationship between cybercrime and human behavior through criminological theories and social networking sites. In *IGI Global eBooks* (pp. 979–989). https://doi.org/10.4018/978-1-5225-9715-5.ch066

Mois, G., Sanislav, T., & Folea, S. C. (2016). A Cyber-Physical system for environmental monitoring. *IEEE Transactions on Instrumentation and Measurement*, *65*(6), 1463–1471. https://doi.org/10.1109/tim.2016.2526669

Moneva, A., & Leukfeldt, R. (2023). Insider threats among Dutch SMEs: Nature and extent of incidents, and cyber security measures. *Journal of Criminology*, *56*(4), 416–440. https://doi.org/10.1177/26338076231161842

Montgomery, E. B. (2006). Breaking out of the security dilemma: realism, reassurance, and the problem of uncertainty. *International Security*, *31*(2), 151–185. https://doi.org/10.1162/isec.2006.31.2.151

Moore, D. (2022). Charting intangible warfare. In *Oxford University Press eBooks* (pp. 45–68). https://doi.org/10.1093/oso/9780197657553.003.0003

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, *3*(3–4), 103–117. https://doi.org/10.1016/j.ijcip.2010.10.002

Moravcsik, A. (1997). Taking Preferences seriously: A liberal theory of international politics. *International Organization*, *51*(4), 513–553. https://doi.org/10.1162/002081897550447

Morse, E. L. (1969). The politics of interdependence. *International Organization*, *23*(2), 311–326. https://doi.org/10.1017/s0020818300031611

Mowle, T. S. (2003a). Worldviews in Foreign Policy: realism, liberalism, and external conflict. *Political Psychology*, *24*(3), 561–592. https://doi.org/10.1111/0162-895x.00341

Mowle, T. S. (2003b). Worldviews in Foreign Policy: realism, liberalism, and external conflict. *Political Psychology*, *24*(3), 561–592. https://doi.org/10.1111/0162-895x.00341

Mueller, M. L. (2019). Against sovereignty in cyberspace. *International Studies Review*, *22*(4), 779–801. https://doi.org/10.1093/isr/viz044

Mugurtay, N., Duygu, U., & Varol, O. (2024). Politics and propaganda on social media: How Twitter and Meta moderate State-Linked Information Operations. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2401.02095

Mukherjee, S. (2019). Cyber warfare and implications. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3431676

Mukhopadhyay, A., & Jain, S. (2023). A framework for cyber-risk insurance against ransomware: A mixed-method approach. *International Journal of Information Management*, *74*, 102724. https://doi.org/10.1016/j.ijinfomgt.2023.102724

NATO CCDCOE. (2020). The Five eyes and offensive cyber capabilities: Building a 'Cyber Deterrence Initiative.' In *Tallinn*[Report]. https://www.ccdcoe.org/uploads/2020/10/2020-Josh-Gold-Five-Eyes-and-Offensive-Cyber-Capabilities.pdf

Netanel, N. W. (2000a). Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory. *California Law Review*, *88*(2), 395. https://doi.org/10.15779/z38kx56

Netanel, N. W. (2000b). Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory. *California Law Review*, *88*(2), 395. https://doi.org/10.2307/3481227

Neumann, I. B., & Welsh, J. M. (1991). The Other in European self-definition: an addendum to the literature on international society. *Review of International Studies*, *17*(4), 327–348. https://doi.org/10.1017/s0260210500112045

Nexon, D. H. (2009). The balance of power in the balance. *World Politics*, *61*(2), 330–359. https://doi.org/10.1017/s0043887109000124

Nica, C., & Tănase, T. (2020). Using weaponized machine learning in cyber offensive operations. *International Conference KNOWLEDGE-BASED ORGANIZATION*, *26*(1), 94–99. https://doi.org/10.2478/kbo-2020-0014

Nilsson, M., & Dalkmann, H. (2001). DECISION MAKING AND STRATEGIC ENVIRONMENTAL ASSESSMENT. *Journal of Environmental Assessment Policy and Management*, *03*(03), 305–327. https://doi.org/10.1142/s1464333201000728

Noh, J. (2022). The emotional underpinning of norms and identities in framing Korean aid. *Development in Practice*, *33*(3), 361–372. https://doi.org/10.1080/09614524.2022.2137104

Nonnecke, B. M., & Epstein, D. (2016). Crowdsourcing Internet Governance: The case of ICANN's Strategy Panel on Multistakeholder Innovation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2909353

Novanto, D. C., Putranti, I. R., & Dir, A. a. B. (2021). Cybernorms: Analysis of international norms in France's Paris call for trust and security in cyberspace. *Journal of Islamic World and Politics*, *5*(2), 326–342. https://doi.org/10.18196/jiwp.v5i2.11656

Nozhati, S., Rosenheim, N., Ellingwood, B. R., Mahmoud, H., & Perez, M. (2019). Probabilistic framework for evaluating food security of households in the aftermath of a disaster. *Structure and Infrastructure Engineering*, *15*(8), 1060–1074. https://doi.org/10.1080/15732479.2019.1584824

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security*, *41*(3), 44–71. https://doi.org/10.1162/isec_a_00266

Nye, J. S., & Keohane, R. O. (1971). Transnational Relations and World Politics: An Introduction. *International Organization*, *25*(3), 329–349. https://doi.org/10.1017/s0020818300026187

Oelsner, A. (2007). Friendship, mutual trust and the evolution of regional peace in the international system. *Critical Review of International Social and Political Philosophy*, *10*(2), 257–279. https://doi.org/10.1080/13698230701208061

Oh, S. H., Jeong, M. K., Kim, H. C., & Park, J. (2023). Applying Reinforcement Learning for Enhanced Cybersecurity against Adversarial Simulation. *Sensors*, *23*(6), 3000. https://doi.org/10.3390/s23063000

Ohonbamu, O., & Kutner, L. (1972). The human right to individual freedom. *University of Pennsylvania Law Review*, *120*(3), 574. https://doi.org/10.2307/3311364

Oikya, U. A. (2021). Az emberi Jogok beépítése a nemzetközi kapcsolatokba. *Belügyi Szemle*, *69*(4. ksz.), 85–92. https://doi.org/10.38146/bsz.spec.2021.4.6

Olesen, N. (2016). European Public-Private Partnerships on Cybersecurity - an instrument to support the fight against cybercrime and cyberterrorism. In *Advanced sciences and technologies for security applications* (pp. 259–278). https://doi.org/10.1007/978-3-319-38930-1_14

Omer, N., Samak, A. H., Taloba, A. I., & El-Aziz, R. M. A. (2023). A novel optimized probabilistic neural network approach for intrusion detection and categorization. *Alexandria Engineering Journal*, *72*, 351–361. https://doi.org/10.1016/j.aej.2023.03.093

Parent, J. M., & Rosato, S. (2015). Balancing in neorealism. *International Security*, *40*(2), 51–86. https://doi.org/10.1162/isec_a_00216

Parn, E. A., & Edwards, D. (2019). Cyber threats confronting the digital built environment. *Engineering Construction & Architectural Management*, *26*(2), 245–266. https://doi.org/10.1108/ecam-03-2018-0101

Parsola, J., & Professor, A. (2023). Cybersecurity Risk assessment and management for organizational
security. *NeuroQuantology*. https://doi.org/10.48047/nq.2022.20.5.nq22815

Pauletto, C. (2020). Information and telecommunications diplomacy in the context of international security at the United Nations. *Transforming Government People Process and Policy*, *14*(3), 351–380. https://doi.org/10.1108/tg-01-2020-0007

Percy, S. (2007). 1 Norms, their influence, and how they can be studied. In *Oxford University Press eBooks* (pp. 14–
48). https://doi.org/10.1093/acprof:oso/9780199214334.003.0002

Pernice, I. (2018). Global cybersecurity governance: A constitutionalist analysis. *Global Constitutionalism*, *7*(1), 112–141. https://doi.org/10.1017/s2045381718000023

Pohle, J. (2019). Verliert das Internet Governance Forum an Bedeutung? *Vereinte Nationen*, *67*(5), 201–206. https://doi.org/10.35998/vn-2019-0059

Ponnusamy, V., Jhanjhi, N. Z., & Humayun, M. (2019). Fostering Public-Private partnership. In *Advances in electronic government, digital divide, and regional development book series* (pp. 237–255). https://doi.org/10.4018/978-1-7998-1851-9.ch012

Poornima, B. (2022). Cyber threats and nuclear security in India. *Journal of Asian Security and International Affairs*, *9*(2), 183–206. https://doi.org/10.1177/23477970221099748

Potluri, S. R., Sridhar, V., & Rao, S. (2020). Effects of data localization on digital trade: An agent-based modeling approach. *Telecommunications Policy*, *44*(9), 102022. https://doi.org/10.1016/j.telpol.2020.102022

Powell, R. (1991). Absolute and relative gains in international relations theory. *American Political Science Review*, *85*(4), 1303–1320. https://doi.org/10.2307/1963947

Prince, C., Omrani, N., Maalaoui, A., Dabic, M., & Kraus, S. (2021). Are we living in surveillance societies and is privacy an illusion? An Empirical study on privacy literacy and privacy concerns. *IEEE Transactions on Engineering Management*, *70*(10), 3553–3570. https://doi.org/10.1109/tem.2021.3092702

Putnam, R. D. (1988). Diplomacy and domestic politics: the logic of two-level games. *International Organization*, *42*(3), 427–
460. https://doi.org/10.1017/s0020818300027697

Pym, D. J. (2021). The origins of Cyberspace. In *Oxford University Press eBooks* (pp. 7–
31). https://doi.org/10.1093/oxfordhb/9780198800682.013.1

Qian, X., & Zhang, J. (2020). Global Cyber Security Governance in the New Era: status, dilemma, and development. *DEStech Transactions on Engineering and Technology Research*. https://doi.org/10.12783/dtetr/mcaee2020/34989

Rascão, J. P. (2020). Freedom of expression, privacy, and ethical and social responsibility in democracy in the digital age. *International Journal of Business Strategy and Automation*, *1*(3), 1–23. https://doi.org/10.4018/ijbsa.2020070101

Rathbun, B. (2018). The Rarity of Realpolitik: What Bismarck's Rationality Reveals about International Politics. *International Security*, *43*(1), 7–55. https://doi.org/10.1162/isec_a_00323

Raymond, M. (2019). Rules for state conduct in the cyber domain. In *Oxford University Press eBooks* (pp. 203–235). https://doi.org/10.1093/oso/9780190913113.003.0006

Raymond, M. (2019). Rules for state conduct in the cyber domain. In *Oxford University Press eBooks* (pp. 203–235). https://doi.org/10.1093/oso/9780190913113.003.0006

Reddi, M., Kuo, R., & Kreiss, D. (2021). Identity propaganda: Racial narratives and disinformation. *New Media & Society*, *25*(8), 2201–2218. https://doi.org/10.1177/14614448211029293

Reiter, D. (2001). Does peace nurture democracy? *The Journal of Politics*, *63*(3), 935–948. https://doi.org/10.1111/0022-3816.00095

Ren, Y., Xiao, Y., Zhou, Y., Zhang, Z., & Tian, Z. (2022). CSKG4APT: A Cybersecurity Knowledge Graph for Advanced Persistent Threat Organization Attribution. *IEEE Transactions on Knowledge and Data Engineering*, 1–15. https://doi.org/10.1109/tkde.2022.3175719

Renard, T. (2018). EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain. *European Politics and Society*, *19*(3), 321–337. https://doi.org/10.1080/23745118.2018.1430720

Reuters. (2015, February 26). North Korean internet, 3G mobile network shut down for hours. *HuffPost*. Accssed att https://www.huffpost.com/entry/north-korean-internet-shut-down_n_6384546

Revizore, K., & Šļakota, M. (2017). FREEDOM OF EXPRESSION IN CYBERSPACE. *INDIVIDUAL SOCIETY STATE Proceedings of the International Student and Teacher Scientific and Practical Conference*, 163. https://doi.org/10.17770/iss2017.3021
Revizore, K., & Šļakota, M. (2017). FREEDOM OF EXPRESSION IN CYBERSPACE. *INDIVIDUAL SOCIETY STATE Proceedings of the International Student and Teacher Scientific and Practical Conference*, 163. https://doi.org/10.17770/iss2017.3021

Robins, K. (1995). Cyberspace and the World We Live in. *Body & Society*, *1*(3–4), 135–155. https://doi.org/10.1177/1357034x95001003008

Rodrigues, B., Scheid, E., Killer, C., Franco, M., & Stiller, B. (2020). Blockchain Signaling System (BLOSS): Cooperative signaling of Distributed Denial-of-Service Attacks. *Journal of Network and Systems Management*, *28*(4), 953–989. https://doi.org/10.1007/s10922-020-09559-4

Rose, G. (1998). Neoclassical realism and theories of foreign policy. *World Politics*, *51*(1), 144–172. https://doi.org/10.1017/s0043887100007814

Ross, R. S. (2006). Balance of power politics and the rise of China: accommodation and balancing in East Asia. *Security Studies*, *15*(3), 355–395. https://doi.org/10.1080/09636410601028206

Rudesill, D. S. (2020). Cyber operations, legal secrecy, and Civil-Military relations. In *Oxford University Press eBooks* (pp. 245–262). https://doi.org/10.1093/oso/9780197535493.003.0014

Ryan, N. J. (2017). Five kinds of cyber deterrence. *Philosophy & Technology*, *31*(3), 331–338. https://doi.org/10.1007/s13347-016-0251-1

Saaida, M. B. E. (2023). The role of culture and identity in international relations. *EAST AFRICAN JOURNAL OF EDUCATION AND SOCIAL SCIENCES, 4*(1), 49–57. https://doi.org/10.46606/eajess2023v04i01.0255

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. *Sensors*, *23*(16), 7273. https://doi.org/10.3390/s23167273

Sakr, H. A., Fouda, M. M., Ashour, A. F., Abdelhafeez, A., El-Afifi, M. I., & Abdellah, M. R. (2024). Machine learning-based detection of DDoS attacks on IoT devices in multi-energy systems. *Egyptian Informatics Journal*, *28*, 100540. https://doi.org/10.1016/j.eij.2024.100540

Salah, K., Elbadawi, K., & Boutaba, R. (2011). Performance modeling and analysis of network firewalls. *IEEE Transactions on Network and Service Management*, *9*(1), 12–21. https://doi.org/10.1109/tnsm.2011.122011.110151

Saleem, D., Sundararajan, A., Sanghvi, A., Rivera, J., Sarwat, A. I., & Kroposki, B. (2019). A multidimensional holistic framework for the security of distributed energy and control systems. *IEEE Systems Journal*, *14*(1), 17–27. https://doi.org/10.1109/jsyst.2019.2919464

Samtani, S., Chai, Y., & Chen, H. (2022). Linking Exploits from the Dark Web to Known Vulnerabilities for Proactive Cyber Threat Intelligence: An Attention-Based Deep Structured Semantic Model. *MIS Quarterly*, *46*(2), 911–946. https://doi.org/10.25300/misq/2022/15392

Samuelson, P. (2000). Privacy as intellectual property? *Stanford Law Review*, *52*(5), 1125. https://doi.org/10.2307/1229511

Sangarsu, R. R. (2023). Enhancing Cyber security using Artificial Intelligence: A Comprehensive approach. *International Journal of Science and Research (IJSR)*, *12*(11), 8–13. https://doi.org/10.21275/sr231029092527

Sari, M. N. (2024). Cybercrime in Association of Southeast Asian Nations: Regional effort and its effectiveness. *Journal of Information Policy*, *14*. https://doi.org/10.5325/jinfopoli.14.2024.0016

Schmidt, B. C. (2005). Competing realist conceptions of power. *Millennium Journal of International Studies*, *33*(3), 523–549. https://doi.org/10.1177/03058298050330031401

Schmidt, B. C., & Wight, C. (2023). Rationalism and the "rational actor assumption" in realist international relations theory. *Journal of International Political Theory*, *19*(2), 158–182. https://doi.org/10.1177/17550882221144643

Schmidt, E. (2022). AI, Great Power Competition & National Security. *Daedalus*, *151*(2), 288–298. https://doi.org/10.1162/daed_a_01916

Schmitt, M. N. (2016). The use of cyber force and international law. In *Oxford University Press eBooks* (pp. 1110–1130). https://doi.org/10.1093/law/9780199673049.003.0053

Schmitt, M. N. (2022). The law of Cyber Conflict. In *Oxford University Press eBooks* (pp. 103–122). https://doi.org/10.1093/oso/9780197626054.003.0007

Schmitt, M. N., & Vihul, L. (2017). Respect for Sovereignty in Cyberspace. *Texas Law Review*, *95*(7), 1639. https://centaur.reading.ac.uk/89703/

Schmitt, M. N., & Watts, S. (2016). Beyond State-Centrism: International law and non-state actors in cyberspace. *Journal of Conflict and Security Law*, *21*(3), 595–611. https://doi.org/10.1093/jcsl/krw019

Schulze, M. (2018). *From cyber-utopia to cyber-war: normative change in cyberspace*. https://doi.org/10.22032/dbt.35107

Segovia-Ferreira, M., Rubio-Hernan, J., Cavalli, A. R., & Garcia-alfaro, J. (2023). Cyber-Resilience approaches for Cyber-Physical systems. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2302.05402

Shackelford, S., Richards, E., Raymond, A., & Craig, A. (2013). Using BITs to protect bytes: Promoting cyber peace by safeguarding trade secrets through bilateral investment treaties. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2324619

Shaheen, S. (2013). Offense–Defense balance in cyber warfare. In *Springer eBooks* (pp. 77–93). https://doi.org/10.1007/978-3-642-37481-4_5

Shandler, R., Kostyuk, N., & Oppenheimer, H. (2023). Public opinion and cyberterrorism. *Public Opinion Quarterly*, *87*(1), 92–119. https://doi.org/10.1093/poq/nfad006

Sharma, A. (2023). Navigating the digital frontier: Safeguarding the right to privacy in cyberspace. *International Journal for Multidisciplinary Research*, *5*(6). https://doi.org/10.36948/ijfmr.2023.v05i06.10101

Sharma, I., & Afshar, M. (2016). Privacy and Freedom Issues in Cyberspace with Reference to Cyber Law. *International Journal of Computer Applications*, *145*(3), 11–18. https://doi.org/10.5120/ijca2016910185

Shea, J. (2017). NATO: Stepping up its game in cyber defence. *Cyber Security.*, *1*(2), 165. https://doi.org/10.69554/syug2137

Sheppard, K. (2014, December 21). McCain calls Sony Hack an "Act of war." *HuffPost*. https://www.huffpost.com/entry/sony-north-korea-war_n_6362454

Sheremet, O. S., Voluiko, O. M., Posmitna, V. V., Poda, T., & Bidzilya, Y. M. (2021). Political and legal aspects of the information warfare. *Revista Amazonia Investiga*, *10*(45), 31–41. https://doi.org/10.34069/ai/2021.45.09.3

Shibaev, D., & Uibo, N. (2016). State policy against information war. *Russian Law Journal*, *4*(3), 136–156. https://doi.org/10.17589/2309-8678-2016-4-3-136-156

Shoemaker, D., Kohnke, A., & Laidlaw, G. (2019). ETHICS AND CYBERSECURITY ARE NOT MUTUALLY EXCLUSIVE. *EDPACS*, *60*(1), 1–10. https://doi.org/10.1080/07366981.2019.1651516

Shrestha, M. (2023). Is cyber diplomacy essential in the present perspective? *Journal of Foreign Affairs*, *3*(01), 19–33. https://doi.org/10.3126/jofa.v3i01.56501

Siddiqui, S. Y., Farooqi, S., Rehman, W. U., & Zulfiqar, L. (2024). Human rights for the digital age. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2408.17302

Sigholm, J. (2013). Non-State Actors in cyberspace operations. *Journal of Military Studies*, *4*(1), 1–37. https://doi.org/10.1515/jms-2016-0184

Simcox, F. W. (2009). *Flexible options for cyber deterrence*. https://doi.org/10.21236/ada539892

Simmons, B. A., Dobbin, F., & Garrett, G. (2006). Introduction: The international diffusion of liberalism. *International Organization*, *60*(04). https://doi.org/10.1017/s0020818306060267

Simpson, G. (2012). International law in diplomatic history. In *Cambridge University Press eBooks* (pp. 25–46). https://doi.org/10.1017/cco9781139035651.004

Slaughter, A. (2000). A liberal theory of international law. *Proceedings of the ASIL Annual Meeting*, *94*, 240–249. https://doi.org/10.1017/s0272503700055919

Smeets, M. (2018). Integrating offensive cyber capabilities: meaning, dilemmas, and assessment. *Defence Studies*, *18*(4), 395–410. https://doi.org/10.1080/14702436.2018.1508349

Smith, N. R. (2018). Can Neoclassical Realism Become a Genuine Theory of International Relations? Squandered Opportunity: Neoclassical Realism and Iranian Foreign Policy, *The Journal of Politics*, *80*(2), 742–749. https://doi.org/10.1086/696882

Snidal, D. (1991). International Cooperation among Relative Gains Maximizers. *International Studies Quarterly*, *35*(4), 387. https://doi.org/10.2307/2600947

Solingen, E. (2001). Domestic coalitional analysis and the Democratic Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3274963

Solomon, T. (2013). Time and subjectivity in world politics. *International Studies Quarterly*, *58*(4), 671–681. https://doi.org/10.1111/isqu.12091

Soner, O., Kayisoglu, G., Bolat, P., & Tam, K. (2023). Risk sensitivity analysis of AIS cyber security through maritime cyber regulatory frameworks. *Applied Ocean Research*, *142*, 103855. https://doi.org/10.1016/j.apor.2023.103855

Song, X. (2018). Research on Security Protection Architecture of Energy Internet Information Communication. *MATEC Web of Conferences*, *228*, 02010. https://doi.org/10.1051/matecconf/201822802010

Spero, J. E. (2018). The politics of international economic relations. *International Journal of Political Science*, *4*(1).

Srinivas, J., Das, A. K., & Kumar, N. (2018). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178–188. https://doi.org/10.1016/j.future.2018.09.063

Staves, A., Anderson, T., Balderstone, H., Green, B., Gouglidis, A., & Hutchison, D. (2022). A Cyber Incident response and recovery framework to support operators of industrial control systems. *International Journal of Critical Infrastructure Protection*, *37*, 100505. https://doi.org/10.1016/j.ijcip.2021.100505

Stevens, T. (2012). A Cyberwar of Ideas? Deterrence and norms in Cyberspace. *Contemporary Security Policy*, *33*(1), 148–170. https://doi.org/10.1080/13523260.2012.659597

Stevens, T., & Kavanagh, C. (2021). Cyber power in international relations. In *Oxford University Press eBooks* (pp. 66–81). https://doi.org/10.1093/oxfordhb/9780198800682.013.4

Sudi, M., Suhada, K., Baharudin, M. Y. S., Irwan, I., & Sudianto, S. (2024). Ethical challenges in digital communications: online privacy, security, and responsibility. *Journal International Dakwah and Communication*, *4*(1), 212–224. https://doi.org/10.55849/jidc.v4i1.665

Sundelius, B. (1980). Interdependence and foreign policy. *Cooperation and Conflict*, *15*(4),187–208. https://doi.org/10.1177/001083678001500401

Swann, T. (2020). Anarchism and Cybernetics: A missed opportunity revisited. In *Policy Press eBooks* (pp. 35–60). https://doi.org/10.1332/policypress/9781529208788.003.0003

Taddeo, M. (2017). The Limits of Deterrence Theory in Cyberspace. *Philosophy & Technology*, *31*(3), 339–355. https://doi.org/10.1007/s13347-017-0290-2

Taha, N. L. M. (2023). Cyber threats and their impact on the U.S. national security. *Tikrit Journal for Political Science*, *2*(32), 178–229. https://doi.org/10.25130/tjfps.v2i32.195

Talpur, F., Korejo, I. A., Chandio, A. A., Ghulam, A., & Talpur, M. S. H. (2024). ML-Based detection of DDOS attacks using evolutionary Algorithms optimization. *Sensors*, *24*(5), 1672. https://doi.org/10.3390/s24051672

Tanodomdej, P. (2019). The Tallinn Manuals and the making of the International Law on Cyber Operations. *Masaryk University Journal of Law and Technology*, *13*(1), 67–86. https://doi.org/10.5817/mujlt2019-1-4

Terenteva, L. V. (2019). Territorial aspect of state jurisdiction and sovereignty in cyberspace. *Lex Russica*, *4*, 139–150. https://doi.org/10.17803/1729-5920.2019.149.4.139-150

Terentieva, L. (2021). The issue of state sovereignty in cyberspace. *Legal Issues in the Digital Age*, *2*(2), 49–69. https://doi.org/10.17323/2713-2749.2021.2.49.67

Thaw, D. (2013). The efficacy of cybersecurity regulation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2241838

Tikos, A., & Krasznay, C. (2022). Cybersecurity in the V4 Countries – A cross-border case study. *Central and Eastern European eDem and eGov Days*, *335*, 163–174. https://doi.org/10.24989/ocg.v335.13

Tran, H., Campos-Nanez, E., Fomin, P., & Wasek, J. (2016). Cyber resilience recovery model to combat zero-day malware attacks. *Computers & Security*, *61*, 19–31. https://doi.org/10.1016/j.cose.2016.05.001

Tsagourias, N. (2018). Law, borders and the territorialisation of cyberspace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3213511

Tsyrfa, I. (2020). INFLUENCE OF POWER NARRATIVES ON THE FORMATION OF THE US FOREIGN POLICY IDENTITY IN THE 21ST CENTURY. *Innovative Solutions in Modern Science*, *7*(43), 95. https://doi.org/10.26886/2414-634x.7(43)2020.7

Turner, S. (1998). Global Civil Society, Anarchy and Governance: Assessing an Emerging paradigm. *Journal of Peace Research*, *35*(1), 25–42. https://doi.org/10.1177/0022343398035001003

Turner, S., & Mazur, G. (2009). Morgenthau as a Weberian methodologist. *European Journal of International Relations*, *15*(3), 477–504. https://doi.org/10.1177/1354066109338242

Urgessa, W. G. (2019). Multilateral cybersecurity governance: Divergent conceptualizations and its origin. Computer Law & Security Review, 36, 105368. https://doi.org/10.1016/j.clsr.2019.105368

Van De Haar, E. (2009). Liberalism and international Relations theory. In *Palgrave Macmillan US eBooks* (pp. 125–150). https://doi.org/10.1057/9780230623972_7

Van Der Meer, S. (2015). Enhancing international cyber security. *Security and Human Rights, 26*(2–4), 193–205. https://doi.org/10.1163/18750230-02602004

Van Eeten, M. (2017). Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity. *Digital Policy Regulation and Governance, 19*(6), 429–448. https://doi.org/10.1108/dprg-05-2017-0029

Venables, A. (2021). Modelling cyberspace to determine cybersecurity training requirements. *Frontiers in Education*, *6*. https://doi.org/10.3389/feduc.2021.768037

Venables, A., Shaikh, S. A., & Shuttleworth, J. (2015). The projection and measurement of cyberpower. *Security Journal*, *30*(3), 1000–1011. https://doi.org/10.1057/sj.2015.35

Vićić, J., & Gartzke, E. (2024). Cyber-enabled influence operations as a 'center of gravity' in cyberconflict: The example of Russian foreign interference in the 2016 US federal election. *Journal of Peace Research*, *61*(1), 10–27. https://doi.org/10.1177/00223433231225814

Vincent, A. (2017). State-sponsored hackers: the new normal for business. *Network Security*, *2017*(9), 10–12. https://doi.org/10.1016/s1353-4858(17)30113-7

Von Heinegg, W. H. (2013). The Tallinn Manual and International Cyber Security Law. In *T.M.C. Asser Press eBooks* (pp. 3–18). https://doi.org/10.1007/978-90-6704-924-5_1

Vucetic, S. (2019). Identity and foreign policy. *International Relations*. https://doi.org/10.1093/obo/9780199743292-0250

Walker, T. C. (2000). The Forgotten Prophet: Tom Paine's Cosmopolitanism and International Relations. *International Studies Quarterly*, *44*(1), 51–72. https://doi.org/10.1111/0020-8833.00148

Waltz, K. N. (2000). Structural Realism after the Cold War. *International Security*, *25*(1), 5–41. https://doi.org/10.1162/016228800560372

Wang, L., Jajodia, S., Singhal, A., Cheng, P., & Noel, S. (2013). K-Zero Day Safety: a network security metric for measuring the risk of unknown vulnerabilities. *IEEE Transactions on Dependable and Secure Computing*, *11*(1), 30–44. https://doi.org/10.1109/tdsc.2013.24

Wang, R., & Xu, W. W. (2022). Hashtag framing and stakeholder targeting: An affordance perspective on China's digital public diplomacy campaign during COVID-19. *Journal of Information Technology & Politics*, *20*(3), 250–268. https://doi.org/10.1080/19331681.2022.2096742

Weiss, M., & Jankauskas, V. (2018). Securing cyberspace: How states design governance arrangements. *Governance*, *32*(2), 259–275. https://doi.org/10.1111/gove.12368

West, D. M. (2004). E-Government and the transformation of service delivery and citizen attitudes. *Public Administration Review*, *64*(1), 15–27. https://doi.org/10.1111/j.1540-6210.2004.00343.x

Whyte, C. (2020). Beyond tit-for-tat in cyberspace: Political warfare and lateral sources of escalation online. *European Journal of International Security*, *5*(2), 195–214. https://doi.org/10.1017/eis.2020.2

Wicki-Birchler, D. (2020). The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime? *International Cybersecurity Law Review*, *1*(1–2), 63–72. https://doi.org/10.1365/s43439-020-00012-5

Williams, M. C. (2004). Why ideas matter in international Relations: Hans Morgenthau, Classical realism, and the moral construction of power politics. *International Organization*, *58*(04). https://doi.org/10.1017/s0020818304040202

Williams, M. C. (2005). What is the National Interest? The Neoconservative Challenge in IR Theory. *European Journal of International Relations*, *11*(3), 307–337. https://doi.org/10.1177/1354066105055482

Wohlforth, W. C. (2011). Gilpinian realism and international Relations. *International Relations*, *25*(4), 499–511. https://doi.org/10.1177/0047117811411742

Wu, J., Li, J., & Ji, X. (2018). Security for cyberspace: challenges and opportunities. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), 1459–1461. https://doi.org/10.1631/fitee.1840000

Wu, Y., & Huang, Y. (2020). Will cyber warfare become a threat to contemporary international security? *Proceedings of the 2021 5th International Seminar on Education, Management and Social Sciences (ISEMSS 2021)*. https://doi.org/10.2991/assehr.k.200826.007

Xia, L., Baghaie, S., & Sajadi, S. M. (2023). The digital economy: Challenges and opportunities in the new era of technology and electronic communications. *Ain Shams Engineering Journal*, *15*(2), 102411. https://doi.org/10.1016/j.asej.2023.102411

Xuetong, Y. (2020). Bipolar rivalry in the early digital age. *The Chinese Journal of International Politics*, *13*(3), 313–341. https://doi.org/10.1093/cjip/poaa007

Yarchi, M. (2024). Digital diplomacy during wars and conflicts. In *Oxford University Press eBooks* (pp. 619–636). https://doi.org/10.1093/oxfordhb/9780192859198.013.34

Yau, H. (2018). Explaining Taiwan's cybersecurity policy prior to 2016: Effects of norms and identities. *Issues & Studies*, *54*(02), 1850004. https://doi.org/10.1142/s1013251118500042

Yongping, G. (2023). The past, conundrums, and future of international cybersecurity governance. *International Journal of Frontiers in Sociology, 5*(4). https://doi.org/10.25236/ijfs.2023.050411

Yusif, S., & Hafeez-Baig, A. (2021). A conceptual model for Cybersecurity governance. *Journal of Applied Security Research*, *16*(4), 490–513. https://doi.org/10.1080/19361610.2021.1918995

Zagare, F. C. (1996). Classical deterrence theory: A critical assessment. *International Interactions*, *21*(4), 365–387. https://doi.org/10.1080/03050629608434873

Zhang, F., Kodituwakku, H. a. D. E., Hines, J. W., & Coble, J. (2019). Multilayer Data-Driven Cyber-Attack Detection System for industrial control systems based on network, system, and process data. *IEEE Transactions on Industrial Informatics*, *15*(7), 4362–4369. https://doi.org/10.1109/tii.2019.2891261

Zhang, N. J., Zulkernine, M., & Haque, A. (2008). Random-Forests-Based network intrusion detection Systems. *IEEE Transactions on Systems Man and Cybernetics Part C (Applications and Reviews)*, *38*(5), 649–659. https://doi.org/10.1109/tsmcc.2008.923876

Zhang, Y., Li, Z., Gao, C., Bian, K., Song, L., Dong, S., & Li, X. (2018). Mobile social big data: WeChat Moments dataset, network applications, and opportunities. *IEEE Network*, *32*(3), 146–153. https://doi.org/10.1109/mnet.2018.1700282

Zhao, T., Tu, H., Jin, R., Xia, Y., & Wang, F. (2024). Improving resilience of cyber–physical power systems against cyber attacks through strategic energy storage deployment. *Reliability Engineering & System Safety*, *252*, 110438. https://doi.org/10.1016/j.ress.2024.110438

Zinovieva, E. S. (2022). Cyber Diplomacy under Increased Competition Between the Great Powers. *MGIMO Review of International Relations*, *17*(4), 27–47. https://doi.org/10.24833/2071-8160-2022-olf5

Zuech, R., Khoshgoftaar, T. M., & Wald, R. (2015). Intrusion detection and Big Heterogeneous Data: a Survey. *Journal of Big Data*, *2*(1). https://doi.org/10.1186/s40537-015-0013-4

Appendices

Appendix 1: Transcript of the Interview with Mr. Ammar Hussain Jaffri

Respondent's Name: Mr. Ammar Hussain Jaffri

Current Role: President of Pakistan Information Security Association (PISA) and Former Additional Director General Federal Investigation Agency, Islamabad

Research Purpose

This interview seeks to examine how the emergence and evolution of cyberspace have influenced the traditional theories of international relations (IR). Your responses will contribute to an academic study focused on theoretical innovation and adaptation in international relations theories in response to the rise of cyberspace.

Question 1

> **How do you see the influence of cyberspace on the traditional concepts of power, sovereignty, and borders in International Relations Theory**?

Response

We all see that the world around us is changing fast and cyberspace has further added to the speed with which events occur and the response time for states is shrinking fast. For instance, in this age of digital diplomacy we witness how a single tweet by world leaders significantly changes the world. Like the U.S. president Donald Trump tweets about trade tariffs and the global market responds to it instantly even before the tariffs and duties come into effect. So, this speed of change is irrefutable and nobody can dispute it. The traditional statecraft must come to terms with these new realities of cyberspace. In recent conflict between Pakistan and India we witnessed how cyberspace is crucially important for national security and defense too and it is encouraging to see that Pakistan has already took bold steps in the right direction.

Question 2

> **In your view, as an officer from the country's leading agency on cybercrimes and now as president of the Pakistan Information Security Association (PISA), is Pakistan ready for the era of supply chain attacks** and Advanced Persistent Threats (APTs)?

Response

Talking about the supply chain attacks all incoming equipment obviously has to go through physical screening for explosives to avoid sabotage attempts and to some extent Customs department Quality Control rules make sure all incoming technology related equipment meets the set standards but obviously Pakistan has no dedicated agency to audit the inbound technological equipment for use in critical infrastructures like national grid, power plants, aviation etc. for the backdoors to prevent sniffing and advanced persistent threats. Authorities should investigate this side too because security vulnerabilities are not just limited to hardware but software too. I want to add one more point here, Pakistan is an agricultural country and agriculture is changing fast. Modern agriculture heavily relies on the internet of things (IoT) to automate the process and reduce human labor, but these systems obviously come with their own vulnerabilities which should not be overlooked.

Question 3

> **How do you view the human resource aspect of the Pakistan's cybersecurity landscape?**

Response

I want to go a step backwards. With increasing out of school children we are even failing to impart traditional education let alone digital literacy. Human element is critically important in the cybersecurity chain, and a cyber-literate public significantly reduces the likelihood and damage from cyberattacks. This applies both in terms of general cyber hygiene practices and

then individuals specializing in offensive and defensive cyber operations. Even the most secure system in the hand of cyber illiterate users get compromised due to increasingly complex social engineering techniques. With the rise of artificial intelligence, the problem just got worse, deep fakes and AI powered voice replication can easily trick cyber illiterate users into allowing access to their devices and systems and compromise the whole networks. As a nation we are doing now what we should have done about a decade ago so technically we are almost a decade behind and it is not easy to catch up with the world, but not impossible either.

Question 4

How do you see the Public-Private partnership and Information Technology (IT) audit and compliance structures in Pakistan's case?

Response

This is one critical area that Pakistan has ignored for too long. Cybersecurity by default is a combined effort and nearly impossible with a good public-private partnership. But there are some encouraging cases too like the National Aerospace Science and Technology Park (NASTP) an initiative taken by the Pakistan Airforce to foster the public private partnership in critical technologies besides aviation. Similarly, the creation of Computer Emergency Response Team (CERT), security guidelines from State Bank of Pakistan (SBP) for commercial banking and Fintech sector signal a growing awareness and action in areas critical to the evolving cybersecurity landscape in Pakistan. Recently, the bifurcation of cyber wing of the Federal Investigation Agency (FIA) as National Cyber Crimes Investigation Agency (NCCIA) is another positive development. As an ADG FIA I was always pushing for a robust cybersecurity policy because without a carefully crafted policy cybercrimes are hard to curb.

Appendix 2: Transcript of the Interview with Dr. Salman Ali

Respondent's Name: Dr. Salman Ali

Current Role: Fudan University, China

Research Purpose

This interview seeks to examine how the emergence and evolution of cyberspace has influenced the traditional theories of international relations (IR). Your responses will contribute to an academic study focused on theoretical innovation and adaptation in international relations theories in response to the rise of cyberspace.

Question 1

How do you see the influence of cyberspace on the traditional concepts of power, sovereignty, and borders in International Relations Theory?

Response

The advent of cyberspace as a new arena has obviously changed the dynamics of world politics. As a new domain it transcends the Westphalian concept of statism that prevailed for centuries and relied mostly on material sources of power. This Westphalian strand of statism is now being tested by the emergence of a new domain which is highly fluid, entry to which doesn't need immigration screenings or visas like the physical world and actors can simultaneously exist and switch between different spaces, this fluidity and ubiquity is not possible in the physical domain. Secondly, determinants of state power have shifted beyond the material means and states are increasingly investing in cyberspace capabilities which is why international relations lexicon is also changing with terms and ideas like cyberwar, cyber army, cyber defense, and cyber operations are increasingly being used in the international relations literature. Recent conflicts have also validated the importance of cyberspace and cyber capabilities in all fields ranging from psychological operations, logistics, and offensive and

defensive operations etc. Similarly, the concept of sovereignty has also been influenced due to cyberspace's very transcending nature.

Question 2

> **In your view, what are the limitations of applying established International Relations theories (realism, liberalism, and constructivism) to cyberspace, and how can they be addressed?**

Response

The traditional theories rely on history dating back centuries and to an extent has identified patterns and answers to different questions like why wars happen in the international system. Traditional theories mostly have come up with answers to questions on such issues. Similarly, postmodern view talks mostly about perceptions, images, and constructs but these theories will have to theorize from the scratch and revisit their understanding of the events and phenomena because the cyber domain is highly fluid with a lax governance structure. Any effort in theorizing here requires both a good understanding of the architect of cyberspace and its implications and the working of world politics.

Question 3

> **How do you think international relations theories have adapted, if at all, to explain cyber conflict, cyber norms, and digital cooperation among states?**

Response

International relations theories, so far, are struggling to adapt to the cyberspace. Cyberspace has introduced a new structure which defies previous explanations. It is a matter of time too; new literature is being produced to explain these novel aspects introduced to international relations. But, overall, the international relations theory is struggling to come to terms and answer new questions arising from cyberspace.

Question 4

How do you view the cybersecurity landscape of Pakistan? What do you think are the shortcomings, and how can they be addressed?

Response

I think the realization is growing now in Pakistan on how to catch up and adapt to the challenges of this new domain and there is a visible push on the legislative side to address some difficult question regarding regulatory and oversight mechanisms and where cyberspace gets entangled with the justice system. So, we see an increasing acceptance of digital evidence and use of cutting-edge technologies and forensics being used by the prosecution and accepted by the courts. However, I think, as digital participation grows and the digital ecosystem within Pakistan evolve further, the frameworks will also adapt and this way gradually Pakistan will develop its own robust and extensive regulatory and legal frameworks for cyberspace. As more complex and perplexing questions arise from cyberspace, the frameworks will adapt to address the shortcomings.

Appendix 3: Transcript of the Interview with Dr. Yasir Masood

Respondent's Name: Dr. Yasir Masood

Current Role: Senior Research Fellow, Global Governance Institute, Beijing

Research Purpose

This interview seeks to examine how the emergence and evolution of cyberspace have influenced the traditional theories of international relations (IR). Your responses will contribute to an academic study focused on theoretical innovation and adaptation in international relations theories in response to the rise of cyberspace.

Question 1

How do you see the influence of cyberspace on the traditional concepts of power, sovereignty, and borders in International Relations Theory?

Response

Cyberspace has upended the old certainties of international politics. Power is no longer defined solely by armies or economies, but by the control of information flows, the ability to disrupt adversaries' networks, and the capacity to project influence instantly across borders. States and non-state actors alike deploy cyber tools to amplify their reach, creating new asymmetries that traditional military or economic metrics cannot capture.

Likewise, sovereignty in the digital age has become more fluid. When data and services float in a global cloud, the notion of exclusive state authority over territory frays. Governments scramble to assert cyber sovereignty by establishing domestic regulations or digital borders, but these measures often collide with the borderless nature of the Internet and the interests of multinational platforms.

Finally, physical borders matter less in cyberspace. While cables and servers remain rooted in geography, the virtual realm allows actors to bypass frontiers entirely. This has prompted a reimagining of borders as points of network control rather than lines on a map and

has lent urgency to international efforts to translate age-old principles of non-intervention and territorial integrity into rules suited for an interconnected world.

Question 2

> **In your view, what are the limitations of applying established International Relations theories (realism, liberalism, and constructivism) to cyberspace, and how can they be addressed?**

Response

Realism's state-centric model misses the stealth and ambiguity of cyber conflict, where non-state actors and data control often trump armies. It must broaden its idea of power to include digital tools.

Liberalism's reliance on institutions fails when states hoard cyber weapons and global bodies move slowly. Faster, public-private partnerships and shared threat intelligence are essential.

Constructivism captures cyber norms and identity but lacks precision and ignores diverse online cultures. Adding network analysis and digital ethnography can help map the spread of norms. Only a hybrid framework uniting power, cooperation, and digital culture can grasp cyberspace's challenges.

Question 3

> **How do you think international relations theories have adapted, if at all, to explain cyber conflict, cyber norms, and digital cooperation among states?**

Response

Realism has begun to treat cyberspace as a strategic domain, recognizing that denial, disruption, and deception can rival tanks and missiles. Liberalism has spawned new forums and coalitions for cyber diplomacy, with states and firms agreeing on incident response and

confidence-building measures. Constructivism has mapped how digital norms emerge through repeated interactions, from agreements on non-interference in electoral systems to voluntary data-sharing. While each tradition has expanded to encompass the digital realm, true insight now emerges from integrating power politics, institutional innovation, and norm evolution into a unified, cyber-aware framework.

Question 4

> **How do you view the cybersecurity landscape of Pakistan? What do you think are the shortcomings, and how can they be addressed**?

Response

Pakistan has taken steps to build its cyber defenses through a national cybersecurity policy and the establishment of a Computer Emergency Response Team. Yet these institutions remain underfunded and staffed by too few specialists to face increasingly sophisticated threats.

Wider gaps include outdated legislation that hinders rapid response to breaches and a lack of public awareness, leaving businesses and citizens vulnerable. Most critical infrastructure still relies on unpatched systems and foreign technology with opaque supply chains.

To address these flaws, Islamabad should prioritize hands-on training for a new generation of cyber professionals, modernize its legal framework to streamline incident reporting and enforcement, and foster genuine public-private collaboration. Regional intelligence sharing and partnerships with global CERT networks will also enhance resilience and help Pakistan stay ahead of emerging risks.

Appendix 4: Transcript of the Interview with Dr. Baqir Malik

Respondent's Name: Dr. Baqir Malik

Current Role: Assistant Professor, Quaid-i-Azam University Islamabad

Research Purpose

This interview seeks to examine how the emergence and evolution of cyberspace has influenced the traditional theories of international relations (IR). Your responses will contribute to an academic study focused on theoretical innovation and adaptation in international relations theories in response to the rise of cyberspace.

Question 1

How do you see the influence of cyberspace on the traditional concepts of power, sovereignty, and borders in International Relations Theory?

Response

Traditional conception of power is based primarily on material sources that are tangible, so it is easy to assess the power of different states on the traditional matrix but in cyberspace the power and capability is mostly intangible. Another important factor is the easy entry to cyberspace as an offensive or defensive actor; it does not take a lot of material resources to conduct offensive operations in cyberspace. Cyberspace is technically a pro-offense domain, and defense is usually more costly and difficult here than in the physical domain. For these reasons power in the cyber realm is elusive and hard to measure but to some extent it reflects a state's overall digital footprint and technological prowess. Perception too is central in cyberspace because technologically advanced nations, by default, have a good standing when it comes to capabilities in cyberspace.

The concept of sovereignty does not apply in the same way as in physical space, people can virtually exist in multiple places in real-time and they do not need any visa or immigration for it. Even offensive cyber operations are not generally seen as a breach of sovereignty unless critical assets or infrastructure is a target.

Although cyberspace defies the logic of borders due to its transnational nature and fluidity but to some extent firewalls and censorship techniques work as a border and enable states to regulate the flow and access of information.

Question 2

In your view, what are the limitations of applying established International Relations theories (realism, liberalism, and constructivism) to cyberspace, and how can they be addressed?

Response

These theories provide a framework for understanding international relations, but these theories need to adapt to the technological wave and there is a need for tailored approaches. Overall, these theories are central to understanding world politics and state is still central to the whole system. For instance, states regulate technological equipment and cyberspace through various means, so the role of state is still there. If we talk about liberal worldview that talks of cooperation in the international system and consolidating norms, this too is not possible without states because in case of any multistakeholder treaty or arrangement states will be party and signatory to it. Without state no treaty or agreement will hold in the world politics so the role of state is obviously important here too. However, the cyberspace has challenged the explanatory power of these theories and there is a need adaptation to address the new realities of cyberspace and their implications for world politics.

Question 3

How do you think international relations theories have adapted, if at all, to explain cyber conflict, cyber norms, and digital cooperation among states?

Response

International relations theories, so far, are struggling to adapt to the cyberspace. Cyberspace has introduced a new structure which defies previous explanations. It is a matter of time too; new literature is being produced to explain these novel aspects introduced to international relations. But, overall, the international relations theory is struggling to come to terms and answer new questions arising from cyberspace.

Talking about realism, state is still central to understanding international relations even in the cyberspace. Like United States and China both have their own cybercommands for both defensive and offensive cyberoperations. Similarly, about liberalist theory, GDPR in EU is an example of how states can agree to certain standards and norms.

Question 4

How do you view the cybersecurity landscape of Pakistan? What do you think are the shortcomings, and how can they be addressed?

Response

So far, we have seen that in Pakistan mostly cyber laws are used to curb dissent and has a partisan dynamic to it and missing an all-party consensus. Privacy laws and public private cooperation is still lagging and needs a major overhaul. Major data breaches go unpunished and there is a general sense of complacency when it comes to cyber vigilance even in the law enforcement sector that Pakistan is not a highly automated economy so focusing on high end equipment and skills is seen as an overstretch but in the future maybe we see greater realization.

We need a major overhaul of the entire criminal justice system too; cyber criminals mostly get away with their crimes because the judiciary and prosecution and still struggling to enforce the cyberlaws in true sense. The frequency of scams and social engineering attacks is a good indicator that without strict privacy and data protection laws cyber criminals will keep manipulating stolen data without any fear of punitive action.

Appendix 5: Transcript of the Interview with Dr. Muhammad Shoaib

Respondent's Name: Dr. Muhammad Shoaib

Current Role: Assistant Professor, Quaid-i-Azam University Islamabad

Research Purpose

This interview seeks to examine how the emergence and evolution of cyberspace has influenced the traditional theories of international relations (IR). Your responses will contribute to an academic study focused on theoretical innovation and adaptation in international relations theories in response to the rise of cyberspace.

Question 1

How do you see the influence of cyberspace on the traditional concepts of power, sovereignty, and borders in International Relations Theory?

Response

The debate on cyberspace is much different from those on traditional concepts of security and hence we see mainstream theories struggling in cyber domain. Traditional theories are based on the idea of sovereignty that cyberspace has seriously challenged over time. We see the response coming from the traditional theories of international relations as fragmented and struggling to account for the changing nature of world politics in and due to cyberspace. Theorizing is a slow process and in case of traditional theories it took centuries of theorizing to identify some broad strands that stood the test of time but in the fast-paced cyberspace theorizing is more challenging which is why International Relations theorists are yet to present some framework that can be validated across cases.

Question 2

In your view, what are the limitations of applying established International Relations theories (realism, liberalism, and constructivism) to cyberspace, and how can they be addressed?

Response

Applying theories is challenging because they were meant for something else and a different age when borders mattered & leaders could claim total control. What can be done? Instead of focusing on salient features, scholars can emphasize philosophical underpinnings of theories such as human nature, system-level, and functionalist logic to deal with the complex questions of today's world.

Question 3

How do you think international relations theories have adapted, if at all, to explain cyber conflict, cyber norms, and digital cooperation among states?

Response

So far, IR theories seem struggling to accommodate questions of cyber and related fields like AI. One reason can be the leading states' emphasis on their parochial interests, still dominated by 20th century mindset. Cold War history tells us that without the willingness of leading actors, new arrangements (like SALT in Cold War) can't be made.

Question 4

How do you view the cybersecurity landscape of Pakistan? What do you think are the shortcomings, and how can they be addressed?

Response

There's enough of talk on cyberspace in Pakistan. But the security apparatus has found it easier to curb access than managing it for good. Cyberspace is seen and treated more as a space that breeds and encourages dissent, so regulatory pushes are mostly made with the intent to curb dissent. Recent experiences of the country have shown that it's now beyond the state's capacity to curb & control, as such an approach negatively affects at both domestic and external level.