Ministry of Higher Education and Scientific Research
University of Abdelhamid Ibn Badis Mostaganem

Faculty of Law and Political Science

Department of Law

Reference:

Submitted in Partial Fulfillment of the Requirements for the Degree of Master

International Protection of Cyberspace

Field: Law and Political Science

Division: Public Law

Specialization: Public International Law

Prepared by the student: khaldi Imane

Supervised by: **Dr.** Benkara Mostefa Aicha

Thesis Committee Members

Professor Feninekh Abdelkader (Chair)

Professor Benkara Mostefa Aicha (Supervisor & Reporter)

Professor Ben Badra Afif (Examiner)

Academic Year: 2024/2025
Defended on: 03 / 07 / 2025

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
جامعة عبد الحميد بن باديس-مستغانم

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

كلية الحقوق و العلوم السياسية
مصلحة التربصات

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية
في إنجاز البحث

أنا الممضي أدناه،

السيد: حالدي اميرة الصفة: طالبة

الحامل لبطاقة التعريف الوطنية رقم: 210655678 والصادرة بتاريخ: 2024/06/24

المسجل بكلية: الحقوق و العلوم السياسية قسم: الحقوق

والمكلف بإنجاز مذكرة ماستر بعنوان:

international protection of cyberspace

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: 21 جويلية 2025

إمضاء المعني

* ملحق القرار الوزاري رقم 933 المؤرخ في 28 جويلية 2016 الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية و مكافحتها

Dedication

I thank **Allah SubḥānahuwaTaʿālā** for being my strength, my peace, and my constant guide.

To **myself**—you kept going, even when it was hard.

To my **mother, father, my beautiful aunt, and sisters**—your love carried me in ways you'll never fully know.

To **Marwa**, thank you for your quiet presence, your encouragement, and your heart.

Acknowledgments

I would like to express my sincere gratitude to **Dr. Benkara Mostefa Aicha**, my supervisor, for her trust, guidance, and consistent support throughout this research. Her thoughtful feedback and encouragement were essential in helping me complete this work with confidence.

I am also thankful to the **Faculty of Law** for the opportunity to write my thesis in English, and for providing an academic environment where I could grow and learn.

To all the professors who taught me during my master's studies—this year and last—thank you for your kindness, your knowledge, and the respect you showed me throughout.

I also wish to thank the **readers** of this thesis for your time and attention.

Finally, I'm grateful to my **family and friends** for your love, patience, and support during this journey. Your presence made this achievement possible.

List of Abbreviations

Art – Article

UN – United Nations

ICCPR - International Covenant on Civil and Political Rights

ICT – Information and Communication Technologies

ICJ – International Court of Justice

NATO – North Atlantic Treaty Organization

GDPR – General Data Protection Regulation

OEWG – Open-Ended Working Group

GGE – Group of Governmental Experts

US – United States

EU – European Union

ENISA – European Union Agency for Cybersecurity

Table of contents

General Introduction

The 21st century has ushered in a transformative era shaped by rapid advances in digital technologies. Cyberspace has evolved beyond a communication platform to become a critical strategic domain with significant social, economic, political, and military dimensions. Governments, corporations, civil society actors, and individuals alike now depend on cyberspace to store, exchange, and safeguard data, making cybersecurity an urgent priority for both national stability and international peace.

Characterized by its borderless, decentralized, and often anonymous nature, cyberspace enables global connectivity and innovation. However, these same features also present serious vulnerabilities. The proliferation of cybercrime, cyber espionage, state-sponsored attacks, and disinformation campaigns has revealed the fragility of digital infrastructure and highlighted the absence of clear regulatory frameworks. The implications of such threats extend well beyond individual or corporate interests—they challenge national sovereignty, democratic institutions, and the broader international legal order.

As cyberspace becomes increasingly integral to national power, global communication, and economic development, states are asserting stronger control over their digital infrastructure in the name of sovereignty. While such efforts aim to safeguard national interests, they also risk creating a fragmented Internet and undermining global cooperation.

Simultaneously, the lack of binding international legal norms leaves cyberspace open to exploitation by both state and non-state actors. Cyberattacks, disinformation campaigns, and cybercrime highlight the limitations of purely national responses in a globally interconnected domain.

This thesis addresses the central dilemma: How can the balance between protecting national sovereignty and ensuring international cybersecurity be achieved?

This question touches on the intersection of international law, state behavior, digital sovereignty, and global security, and raises critical issues about the future of international cooperation in cyberspace.

This study contributes to the emerging discourse on international cyber law by analyzing how legal frameworks, state practices, and diplomatic initiatives are responding to cybersecurity challenges. It examines the tension between national interests and collective responsibilities in the digital sphere. Particular attention is given to developments within the United Nations and other international forums that aim to establish shared principles for state behavior in cyberspace.

The relevance of this research extends to Algeria and other developing countries, which must simultaneously address domestic cybersecurity needs and engage in global norm-shaping efforts. As these states confront the dual pressures of digital vulnerability and sovereign autonomy, a clearer understanding of international legal processes becomes essential.

This thesis seeks to:

1. Define the conceptual and legal characteristics of cyberspace and cybersecurity under international law.

2. Identify the principal challenges posed by cyber threats to international peace and state sovereignty.

3. Evaluate the role of the United Nations and other multilateral bodies in promoting legal frameworks and norms of responsible state behavior in cyberspace.

4. Propose legal approaches for balancing state sovereignty with international cooperation and governance in the cyber domain.

This research is guided by the hypothesis that a balance between national sovereignty and international cybersecurity can be achieved by adapting existing international legal frameworks and fostering multilateral cooperation. Rather than presenting opposing goals, sovereignty and collective security can be harmonized through shared norms, trust-building measures, and inclusive dialogue, particularly within the institutional context of the United Nations and regional organizations.

This study adopts an analytical and descriptive methodology, drawing on legal instruments, multilateral agreements, case studies, academic literature, and official state practice. A comparative dimension is also applied, assessing how different legal systems and regional frameworks address cyber threats and engage with international cybersecurity norms.

The thesis is organized into two main chapters:

- **Chapter One** outlines the conceptual foundations of cyberspace and cybersecurity. It defines key terminology, traces the historical development of the Internet, and examines the strategic implications of cyber threats for state behavior and international relations.

- **Chapter Two** focuses on the international legal governance of cyberspace. It analyzes the role of the United Nations and other global bodies in

establishing legal norms, voluntary guidelines, and institutional mechanisms for promoting responsible state conduct in cyberspace.

The thesis concludes with a general conclusion summarizing the research findings and proposing directions for enhancing the international legal regulation of cyberspace.

Chapter One
Conceptual Framework for Cyberspace and Cybersecurity

Chapter One: Conceptual Framework for Cyberspace and Cyber security

In an era defined by digital interdependence, cyberspace has emerged as a critical domain of both opportunity and vulnerability. While it facilitates unprecedented connectivity, innovation, and economic integration, it also presents complex challenges to national sovereignty, individual privacy, and global stability. As states, corporations, and individuals increasingly rely on digital technologies to operate and communicate, the boundaries between physical and virtual security have blurred, giving rise to a new class of transnational threats.[1] Understanding cyberspace and the mechanisms for its protection has thus become a foundational concern in international relations and global security studies.

This chapter aims to establish a conceptual foundation for analyzing the evolving digital landscape and its implications for international security. Section One provides a theoretical and definitional overview of cyberspace and cyber security. It examines cyberspace as a socio-technical domain shaped by code, infrastructure, users, and governance frameworks. It also explores the evolution of cyber security as both a technical practice and a strategic imperative, addressing how diverse actors—state and non-state—navigate its operational, legal, and normative dimensions.[2]

Section Two turns to the proliferation of cyber threats and their growing influence on the architecture of international security. From state-sponsored cyber-espionage and infrastructure sabotage to criminal networks and hacktivist operations, this section analyzes the nature, sources, and consequences of cyber attacks. It investigates how such threats challenge traditional models of deterrence and conflict resolution

[1] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in Cyberpower and National Security, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 24–42, https://apps.dtic.mil/sti/citations/ADA503382.
[2] Milton Mueller, Networks and States: The Global Politics of Internet Governance (Cambridge, MA: MIT Press, 2010), 11–17.

and complicate international cooperation.[1] through this lens, the chapter interrogates the systemic vulnerabilities embedded in global digital infrastructure and their potential to destabilize political systems, economies, and intergovernmental trust.

Together, these sections offer a critical entry point for understanding cyberspace not simply as a technical environment but as a contested and politicized domain that demands comprehensive and cooperative approaches to security.

Section One: The Concept of Cyberspace and Cyber security

Cyberspace is a multifaceted and evolving digital environment formed by the global network of information and communication technologies (ICTs). It comprises not only the internet but also the infrastructures, hardware, software, and protocols that enable digital communication, data exchange, and remote interaction.[2] Unlike physical domains, cyberspace is not limited by geography or borders; it exists through the interconnectedness of devices, data centers, and transmission systems spread across sovereign territories. It is simultaneously virtual and real, governed by both code and policy, and shaped by human interaction as well as machine logic.

What distinguishes cyberspace as a unique domain is its socio-technical nature. It is a constructed space that reflects and amplifies human intentions, including communication, economic activity, innovation, control, and, increasingly, power projection.[3] Governments, corporations, individuals, and non-state actors all coexist and compete in cyberspace, using it as a platform for influence, conflict, and governance.

[1] Jason Healey, ed., A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 (Vienna, VA: Cyber Conflict Studies Association, 2013), 9–14.

[2] U.S. Department of Defense, Dictionary of Military and Associated Terms, Joint Publication 1-02 (2010), 69, https://irp.fas.org/doddir/dod/jp1_02.pdf

[3] Lawrence Lessig, Code: And Other Laws of Cyberspace (New York: Basic Books, 1999), 6–9.

As a result, cyberspace has become central to global political and economic systems, raising complex questions about jurisdiction, accountability, and sovereignty.[1]

Cybersecurity, in turn, refers to the practices, technologies, policies, and frameworks designed to protect cyberspace and the data, systems, and networks within it. It encompasses measures aimed at preventing, detecting, and responding to threats or unauthorized actions that may compromise the confidentiality, integrity, or availability of digital assets.[7] As digital technologies have become foundational to state functions, commerce, health, defense, and communication, cybersecurity has transitioned from a niche technical concern to a central component of national and international security strategies.[2]

Effective cybersecurity involves more than just technological defenses; it requires legal norms, institutional coordination, public-private partnerships, and international cooperation.[3] While states seek to protect critical infrastructure and digital sovereignty, private companies are often the gatekeepers of vast networks and sensitive data. This interplay has created a fragmented yet interdependent security environment, in which responsibility is dispersed across multiple actors and jurisdictions. Moreover, emerging technologies like artificial intelligence, quantum computing, and the Internet of Things (IoT) continue to reshape both the opportunities and vulnerabilities within cyberspace.

This section provides a comprehensive analysis of cyberspace as a socio-technical domain and explores how cybersecurity has emerged as an essential framework for managing the complexities of digital life. It

[1] Milton Mueller, *Networks and States* (MIT Press, 2010), 12–18.

[2] Jason Healey (ed.), *A Fierce Domain* (2013), 11–15..

[3] Joseph S. Nye Jr., "The Regime Complex for Managing Global Cyber Activities," Global Commission on Internet Governance, Paper Series No. 1 (May 2014), https://www.cigionline.org/static/documents/gcig_paper_no1.pdf.

critically examines the ways in which cyberspace challenges traditional legal and political structures, and how cybersecurity has evolved from a technical safeguard to a global policy imperative. Together, these concepts form the foundation for understanding the multidimensional governance and security issues that define the digital age.

1. Cyberspace

1.1 Historical Evolution of Cyberspace

The historical evolution of cyberspace is a complex interplay of technological innovation, military strategy, academic collaboration, and commercial expansion. Its development reflects both the ambitions and anxieties of the late 20th and early 21st centuries, and its history is essential to understanding its current structure and governance.

Cyberspace, as a term and a concept, emerged after the technology it describes was already in use. The foundations of cyberspace can be traced back to the **Cold War era**, particularly with the creation of the **ARPANET** (Advanced Research Projects Agency Network) in the late 1960s. Funded by the U.S. Department of Defense, ARPANET was designed to create a **decentralized communication network** that could survive a nuclear attack. The first successful message sent over ARPANET was between UCLA and Stanford Research Institute on October 29, 1969.[1]

Throughout the 1970s, ARPANET expanded, connecting more universities and research institutions. This era saw the development of key communication protocols, most importantly **TCP/IP (Transmission Control Protocol/Internet Protocol)**, proposed by Vinton Cerf and Robert Kahn in 1974 and adopted by ARPANET in 1983.[2] This marked a turning point, as TCP/IP allowed diverse networks to interconnect—a foundational step in the creation of the modern internet.

By the 1980s, the concept of a global information infrastructure began to take shape. The term **"cyberspace"** itself was popularized by

[1] Janet Abbate, Inventing the Internet (Cambridge: MIT Press, 1999), 52.
[2] Katie Hafner and Matthew Lyon, Where Wizards Stay Up Late: The Origins of the Internet (New York: Simon & Schuster, 1996), 212.

science fiction writer **William Gibson** in his 1984 novel *Neuromancer*, where it was described as a "consensual hallucination" experienced daily by billions. Gibson's vision was speculative, but it resonated with the growing digital connectivity of the real world.[1] His influence gave cyberspace a conceptual identity beyond its physical infrastructure, capturing the imagination of technologists and policymakers alike.

The late 1980s and early 1990s witnessed rapid expansion of networked systems. The **Domain Name System (DNS)** was introduced in 1984 to simplify the addressing of websites. In 1989, **Tim Berners-Lee**, a British scientist at CERN, proposed the **World Wide Web**, aiming to facilitate access and linkage to documents across the internet. By 1993, the launch of the **Mosaic** browser made the Web accessible to the general public, leading to a dramatic rise in usage.[2]

As commercial and individual users flocked to the internet in the 1990s, cyberspace became a domain of economic, social, and political importance. The **dot-com boom** fueled investment in online infrastructure, and by the end of the decade, the internet had become a global phenomenon. Governments began to recognize the strategic importance of cyberspace, not only for communication and commerce but also for national security.

The early 2000s marked a shift in the perception of cyberspace from a utopian domain of free expression to one increasingly associated with surveillance, crime, and geopolitical contestation. After the **9/11 attacks**, the U.S. and other states began heavily investing in cyber defense and surveillance capabilities. The revelations by **Edward Snowden** in 2013 showed the extent of state surveillance programs like **PRISM**, casting cyberspace as a contested and surveilled environment.[3]

Meanwhile, **cybercrime and cyberwarfare** emerged as major concerns. The **2007 cyberattacks on Estonia**, widely considered the

[1] William Gibson, Neuromancer (New York: Ace Books, 1984), 51.
[2] Tim Berners-Lee, Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web (New York: HarperCollins, 1999), 98.
[3] Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (New York: Metropolitan Books, 2014), 45.

first instance of state-level cyber aggression, marked a significant turning point. A series of coordinated Distributed Denial of Service (DDoS) attacks disrupted government, banking, and media websites. This incident revealed cyberspace as a potential domain of military and political conflict.[15] The **Stuxnet worm**, discovered in 2010, further illustrated this evolution. Believed to be a joint U.S.-Israeli operation, Stuxnet targeted Iran's nuclear program by sabotaging centrifuges—a landmark example of offensive cyber operations with real-world consequences.[1]

Throughout the 2010s and into the 2020s, cyberspace has become increasingly integrated into everyday life through the proliferation of **smartphones**, **cloud computing**, and the **Internet of Things (IoT)**. This era is marked by both remarkable digital innovation and rising cybersecurity threats. The **2016 U.S. presidential election interference**, attributed to Russian actors using cyber tools and information warfare, exemplifies how cyberspace can influence democratic processes.[2]

In recent years, **digital sovereignty**, **data protection**, and **cyber norms** have become central themes in global discourse. China's "Great Firewall," the European Union's **General Data Protection Regulation (GDPR)**, and increasing calls for internet fragmentation reflect the ongoing politicization and securitization of cyberspace. International debates around governance, digital rights, and the role of major tech companies such as Google, Amazon, and Meta highlight the challenges of regulating a space that transcends national borders but is deeply affected by national interests.[3]

The historical trajectory of cyberspace—from a Cold War defense project to a global, multidimensional domain—demonstrates its evolution as not merely a technical environment but a social, economic, legal, and geopolitical space. Its future will likely be shaped by

[1] Kim Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon (New York: Crown, 2014), 5.
[2] P.W. Singer and Emerson T. Brooking, LikeWar: The Weaponization of Social Media (New York: Houghton Mifflin Harcourt, 2018), 112.
[3] Milton Mueller, Will the Internet Fragment? Sovereignty, Globalization and Cyberspace (Cambridge: Polity Press, 2017), 64.

competing visions: one of openness and innovation, and another of control and competition.

1.2 Definition of Cyberspace

This concept can be approached from several angles:

A. Linguistic Definition of Cyber: The term "cyber" originates from "Cyber" which describes anything related to computer culture, information technology, or virtual reality. Cyber refers to "internet space" and is derived from the Greek word "Kybernetes" which first appeared in 1982 in the science-fiction novel Neuromancer by William Gibson, where it was used to mean "the control of a ship."

B. Terminological Definition of Cyber: In its modern sense, the term "cyber" was first used by American mathematician Norbert Weiner, a professor at the Massachusetts Institute of Technology (MIT), In 1948. Weiner coined the term to describe a feedback system in which the output of a system is used to regulate its inputs, thus maintaining control and stabilizing performance. Weiner believed that this system could be broadly applied across fields, not only in scientific domains but also in human and social context. Thus, in its modern technological sense, "cyber" relates to the "science of control and communication in living organism and machines."

Cyberspace itself is the "medium through which computer networks exist and facilitates electronic communication." More broadly, it is understood as a complex domain that encompasses both physical and non-physical elements, including computers, network systems and software, information computing, data transfer and storage, and all uses users of these components.

The International Telecommunication Union (ITU) defines cyberspace as a domain comprising both physical and non-physical elements, including computers, networks, software., information computing, transmitted content, control data, and users of These components.

Similarly, the U.S. Department of Defense's Military Dictionary describes cyberspace as an operational field within the informational environment, characterized by an interconnected network of data and IT infrastructure. This includes the internet, computers, communication networks, processing, and control systems.

The French National agency for the Security of Information System (ANSSI) defines cyberspace as "a communication space formed by global interconnection of digital data processing equipment."[1]

1.3 The Dimensions of Cyberspace

Cyberspace, often perceived as a purely technical realm, is in fact a multidimensional construct that encompasses technological, informational, social, legal, economic, and strategic aspects. Understanding these dimensions is essential to assess the scope and implications of cyber threats and formulate effective responses.

The **technical dimension** of cyberspace consists of the underlying physical and logical infrastructure that enables digital communication. This includes fiber-optic cables, data centers, satellites, internet exchange points, domain name systems (DNS), and routing protocols. At the logical level, protocols such as TCP/IP and encryption algorithms govern how data is formatted, transmitted, and secured. The physical and technical layers provide the foundation for the global information infrastructure, but they are also vulnerable to disruption. For instance, cable cuts or BGP (Border Gateway Protocol) hijacks can reroute or disable internet access across entire regions, as demonstrated by documented incidents in the Middle East and Central Asia.[2]

The **informational dimension** of cyberspace refers to the content that flows through the networks—emails, databases, multimedia, software code, and more. This dimension also includes metadata and behavioral data collected and analyzed to profile users. Control over information flow can influence political narratives, social behaviors, and

[1] Dr. Benkara Mostefa Aisha, International Law of Cyberspace, Jouda Editions, Algeria,2025, 20 –22.
[2] Tim Maurer, Cyber Mercenaries: The State, Hackers, and Power (Cambridge: Cambridge University Press, 2018), 45–46.

even economic trends. During election seasons, disinformation campaigns spread via social media platforms have shown how the manipulation of information in cyberspace can have far-reaching societal effects.[1] In response, both democratic and authoritarian regimes have invested heavily in content monitoring, censorship technologies, and narrative control.

The **social dimension** involves the interaction between users, institutions, and societies within cyberspace. It includes digital identities, online communities, and the formation of global civil society movements. Cyberspace enables decentralized communication and has redefined political engagement, activism, and even radicalization. For example, social media platforms have played a pivotal role in movements such as the Arab Spring and, conversely, in the recruitment strategies of terrorist organizations like ISIS.[2] These developments illustrate the dual-use nature of the social dimension in cyberspace—facilitating both democratization and destabilization.

The **legal and regulatory dimension** deals with the frameworks that govern behavior in cyberspace. Jurisdictional issues, cross-border data flows, digital sovereignty, and privacy rights are central concerns. Despite efforts to develop international cyber norms through platforms such as the United Nations' Group of Governmental Experts (GGE), cyberspace remains largely unregulated at the global level.[3] National regulations differ widely, from the General Data Protection Regulation (GDPR) in the European Union to more surveillance-oriented laws in countries like China and Russia. These discrepancies create legal grey zones exploited by cybercriminals and complicate international cooperation on cyber governance.

The **economic dimension** addresses the role of cyberspace in global commerce and development. Digital infrastructure supports a multitrillion-dollar economy that includes e-commerce, fintech, cloud

[1] P. W. Singer & Emerson T. Brooking, *LikeWar* (2018), 102–106.
[2] Gabriel Weimann, "Terrorist Migration to the Dark Web," Perspectives on Terrorism 10, no. 3 (2016): 40–44.
[3] United Nations, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," 2021, https://www.un.org/disarmament/ict-security/.

computing, and the gig economy. However, this dependency also exposes states and businesses to significant risks. According to Cybersecurity Ventures, the global cost of cybercrime is expected to reach $10.5 trillion annually by 2025, making it the third-largest economy if measured as a nation.[1] High-profile ransomware attacks on critical infrastructure, such as the 2021 Colonial Pipeline incident in the U.S., demonstrate how economic stability is directly tied to cyber resilience.[2]

The **political and sovereignty dimension** of cyberspace is shaped by the way states assert control and influence over digital territories. Concepts like "digital sovereignty" and "cyber borders" have emerged in response to concerns about foreign influence and dependency on global tech giants.[3] Some states, such as China and Russia, have implemented extensive national firewalls and data localization laws to ensure state control over domestic cyberspace. These strategies reflect a broader trend of digital nationalism and contestations over internet governance. At the international level, cyber diplomacy has become a critical component of foreign policy, with states engaging in cyber alliances, mutual defense treaties, and attribution coalitions.

Lastly, the **strategic and military dimension** highlights cyberspace as a domain of warfare. Military doctrines in countries such as the United States, Russia, China, and Iran now explicitly include offensive and defensive cyber operations as core capabilities.[4] Cyber tools are used for espionage, sabotage, psychological warfare, and in some cases, preemptive strikes. The 2010 Stuxnet worm, which targeted Iran's nuclear facilities, and the series of cyber operations linked to the Ukraine conflict, underscore the growing importance of cyberspace in geopolitical strategies.[5] Given the challenges of attribution and the

[1] Steve Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," Cybersecurity Ventures, November 13, 2020, https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/.
[2] Kim Zetter, *Countdown to Zero Day* (2014), 182–185
[3] Anu Bradford, The Brussels Effect: How the European Union Rules the World (Oxford: Oxford University Press, 2020), 215–220.
[4] U.S. Department of Defense, Summary of the Department of Defense Cyber Strategy (2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
[5] Kim Zetter, *Countdown to Zero Day* (2014).

asymmetry of cyber capabilities, cyberspace is also attractive to non-state actors and smaller powers seeking to project influence beyond conventional means.

Each of these dimensions is interconnected, and disruptions in one often have cascading effects on others. For example, a technical breach may lead to information leaks, social unrest, economic damage, legal disputes, and even military escalation. Therefore, understanding cyberspace requires a holistic approach that recognizes the complexity and interdependence of its various components.

1.4 Characteristics of Cyberspace

Cyberspace is a complex, multilayered environment composed of interconnected digital networks, data flows, users, and infrastructures. It differs significantly from physical domains due to its unique features, which define both its potential and its vulnerabilities. The characteristics of cyberspace influence not only how information is transmitted and secured, but also how states, non-state actors, and individuals engage with and within it.

One of the primary characteristics of cyberspace is its **borderless nature**. Unlike land, sea, or air, cyberspace is not limited by physical geography. Data and information can traverse the globe in milliseconds, challenging the traditional notions of sovereignty and jurisdiction. This transnational aspect makes it difficult for governments to enforce national laws across borders, especially when dealing with cybercrime or cyberattacks originating from foreign territories. For instance, a hacker operating from Eastern Europe can target institutions in the United States while routing their traffic through multiple countries, complicating efforts to trace and prosecute them.[1]

Another key characteristic is the **anonymity and pseudonymity** it offers. Users can interact, transact, and even attack without revealing their real identities. This capability can be beneficial for privacy, whistleblowing, or dissidence under oppressive regimes. However, it

[1] Thomas Rid, Cyber War Will Not Take Place (Oxford: Oxford University Press, 2013), 45.

also facilitates malicious activities such as identity theft, cyberbullying, and organized cybercrime. The structure of the internet, particularly with the use of tools like VPNs, Tor browsers, and cryptocurrencies, makes it easier for actors to conceal their identity and location, leading to challenges in attribution and accountability.[1]

Cyberspace is also defined by its **interconnectivity**. Billions of devices, ranging from traditional computers to smartphones and IoT (Internet of Things) gadgets, are connected in real time. This interconnectedness enables rapid communication, commerce, and innovation but also increases vulnerability. A single point of failure—such as a zero-day vulnerability in commonly used software—can cascade across interconnected systems, leading to large-scale disruptions. The 2017 WannaCry ransomware attack, which exploited vulnerabilities in Microsoft Windows, demonstrated how quickly a cyber incident could spread globally and cripple essential services like hospitals and transport systems.[2]

A further defining trait is the **asymmetry** in power and capability. In physical warfare, states usually have the upper hand due to their military capabilities. In cyberspace, however, small groups or even individuals can cause disproportionate damage to large institutions or governments. Cyber tools can be cheap, easily distributed, and repurposed. This asymmetry empowers non-state actors, hacktivist groups, and criminal organizations to operate with relative effectiveness against well-resourced targets.[3]

The **man-made and constantly evolving** nature of cyberspace distinguishes it from natural domains. Software, protocols, and systems are created, maintained, and modified by humans. As a result, cyberspace is in a perpetual state of flux, with new platforms, vulnerabilities, and trends emerging constantly. This dynamic nature requires continual adaptation by cybersecurity professionals, law

[1] Gabriella Coleman, Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous (London: Verso, 2014), 112.
[2] Andy Greenberg, *Sandworm* (2019), 89.
[3] Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," International Security 41, no. 3 (2017), 44.

enforcement, and policymakers. Moreover, software vulnerabilities are inherent in design and deployment, making perfect security virtually unattainable.[1]

Moreover, cyberspace has a unique **duality of use**. Technologies designed for benign or beneficial purposes can also be used maliciously. For example, machine learning algorithms can improve cybersecurity defense systems but also be weaponized for advanced phishing or deepfake campaigns. Similarly, remote access tools that enable IT support can be exploited by attackers to gain unauthorized entry. This dual-use nature complicates regulatory approaches, as outright bans may hinder technological progress.[2]

Another important characteristic is **speed and volume**. Information flows in cyberspace occur at lightning speed, and the volume of data exchanged is enormous. This pace challenges traditional decision-making and response times, especially in the context of cyber defense. Unlike traditional warfare, which may allow for mobilization or deliberation, cyberattacks can happen instantaneously and with devastating effect. Automated attacks, such as those launched by bots or worms, operate on timescales far shorter than human reaction can accommodate.[3]

The **lack of a centralized governing authority** is also a notable feature. While physical spaces are regulated by national and international laws, cyberspace lacks a single overarching body with enforcement powers. The internet's infrastructure is governed by a patchwork of public and private actors such as ICANN (Internet Corporation for Assigned Names and Numbers), ISPs, and regional internet registries. This decentralization leads to differing standards and regulations across countries and organizations, creating inconsistencies and regulatory gaps.[4]

[1] Bruce Schneier, Click Here to Kill Everybody: Security and Survival in a Hyper-connected World (New York: W. W. Norton & Company, 2018), 57.

[2] Ronald J. Deibert, Black Code: Inside the Battle for Cyberspace (Toronto: Signal, 2013), 163.

[3] Michael Warner, "Cybersecurity: A Pre-history," Intelligence and National Security 27, no. 5 (2012), 774.

[4] Milton Mueller, *Networks and States* (MIT Press, 2010), 774.

Finally, cyberspace facilitates **amplification and influence**. A single message, video, or post can go viral and reach millions, shaping public opinion and even political outcomes. This amplification power is leveraged in both positive campaigns and harmful activities like disinformation or cyber psychological operations. States and non-state actors alike use these techniques to sway elections, polarize societies, and undermine trust in institutions.[1]

Understanding these characteristics is essential for developing effective cybersecurity strategies, international cooperation mechanisms, and ethical frameworks for digital conduct. As cyberspace continues to expand and integrate deeper into daily life, its unique attributes will increasingly shape the security, legal, and political landscapes of the 21st century.

1.5 Architecture and Layers of Cyberspace

The architecture of cyberspace is not confined to a single form or framework but rather spans multiple interconnected layers—physical, logical, and social—that collectively enable the operation of the global digital environment. Understanding these layers is essential to grasp how cyberspace functions and how it is affected by political, legal, and economic forces.

At the **base of cyberspace architecture lies the physical layer**, which includes the tangible infrastructure that makes connectivity possible: undersea fiber-optic cables, data centers, satellites, mobile towers, routers, servers, and personal computing devices. This layer is geographically bound and unevenly distributed, with concentration of infrastructure in developed regions. Major Internet Exchange Points (IXPs), such as those in Frankfurt, Amsterdam, and Ashburn, Virginia, act as central nodes in the global internet backbone, reflecting both technical efficiency and geopolitical concentration. As such, the physical architecture of cyberspace reflects economic and strategic disparities between states and regions. Control over physical infrastructure can lead

[1] P. W. Singer & Emerson T. Brooking, *LikeWar* (2018), 3.

to digital hegemony or dependency, making this layer a key point of strategic concern for states and corporations alike.[1]

Above the physical layer exists the **logical layer**, often referred to as the code or protocol layer. This consists of the software and rules that govern how data is formatted, transmitted, routed, and accessed. Key components include the **Transmission Control Protocol/Internet Protocol (TCP/IP)**, which facilitates packet switching and end-to-end communication; the **Domain Name System (DNS)**, which translates human-readable web addresses into numerical IP addresses; and other protocols such as HTTP/HTTPS, FTP, and SMTP. These protocols are largely standardized by international bodies such as the **Internet Engineering Task Force (IETF)** and the **World Wide Web Consortium (W3C)**. The logical layer is integral to interoperability and scalability across diverse networks and devices.[2]

Control over the logical layer is both technical and political. For example, the U.S.-based **Internet Corporation for Assigned Names and Numbers (ICANN)** has historically played a central role in DNS coordination, which has led to international debates on governance and accountability. The transfer of IANA (Internet Assigned Numbers Authority) stewardship from the U.S. Department of Commerce to the global multistakeholder community in 2016 was a landmark moment in the politics of cyberspace architecture.[3] Even so, many nations continue to express concern over the concentration of protocol-setting power in Western, particularly American, institutions.

Overlaying the logical layer is the **content and application layer**, where digital services, platforms, and applications operate. This includes websites, social media platforms, e-commerce services, streaming platforms, and software applications—essentially the user-facing part of cyberspace. Here, entities like Google, Facebook (Meta), Amazon, and Alibaba dominate, creating a vertically integrated cyberspace in which the same companies often control infrastructure, data, and user

[1] Laura DeNardis, The Global War for Internet Governance (New Haven: Yale University Press, 2014), 14.
[2] Lawrence Lessig, Code and Other Laws of Cyberspace (New York: Basic Books, 1999), 34.
[3] Milton Mueller, *Networks and States* (MIT Press, 2010), 65.

experience. The application layer is where issues like content moderation, surveillance, disinformation, and data privacy play out, reflecting tensions between commercial interests and public good.[1]

Crucially, the content layer is not only shaped by technological protocols but also by **algorithmic architectures**. Algorithms determine what users see, how content is ranked or suppressed, and which data are collected. These mechanisms are typically proprietary and opaque, raising legal and ethical concerns. Algorithmic bias, echo chambers, and platform manipulation are increasingly central to discussions about the architecture of cyberspace.[2]

Beyond these technical layers lies the **social or human layer**, sometimes referred to as the "user layer." This includes the individuals, communities, organizations, and states that engage with and shape cyberspace. It encompasses the behaviors, norms, and power relations of cyberspace as a lived experience. The social layer reflects how people use cyberspace for communication, identity formation, economic activity, activism, or even criminal behavior. It is also the layer most directly affected by regulations, digital rights, and cultural practices.[3]

These layers—physical, logical, application, and social—are **deeply interdependent**. A change or disruption in one can have cascading effects on the others. For instance, a cable cut in the physical layer can disrupt access to services in the application layer. Likewise, changes to DNS protocol rules in the logical layer can affect domain accessibility, censorship, or surveillance policies at the content layer. The layered nature of cyberspace architecture thus poses challenges for governance, cybersecurity, and legal jurisdiction.

Additionally, **cloud computing** and **edge computing** have introduced a degree of fluidity to these layers. Cloud services abstract the physical infrastructure into virtualized environments, making data and processing location-agnostic. Edge computing, conversely,

[1] Shoshana Zuboff, The Age of Surveillance Capitalism (New York: PublicAffairs, 2019), 65.
[2] Safiya Umoja Noble, Algorithms of Oppression: How Search Engines Reinforce Racism (New York: NYU Press, 2018), 25.
[3] Manuel Castells, The Rise of the Network Society, 2nd ed. (Oxford: Wiley-Blackwell, 2010), 390.

decentralizes data processing by bringing it closer to users, increasing responsiveness and reducing latency. These developments further complicate questions of jurisdiction, security, and accountability.[1]

It is also essential to note the emerging **cyber-physical convergence**, particularly through the Internet of Things (IoT). The integration of cyberspace with physical systems—such as transportation, healthcare, and energy infrastructure—blurs the boundaries between digital and physical realms. A cyberattack on an IoT device can now cause real-world harm, making the architecture of cyberspace not just a technical issue but a matter of public safety and national security.[2]

In sum, the architecture of cyberspace is not monolithic but multilayered, dynamic, and contested. Its components are designed for efficiency and scalability but often lead to centralization and asymmetry in power and control. Understanding this architecture is critical for addressing legal, ethical, and strategic challenges in the digital age.

1.6 Governance of Cyberspace

Governance of cyberspace refers to the complex systems, principles, and institutions that shape how the internet and its infrastructure are managed, accessed, and regulated across different jurisdictions and sectors. Unlike traditional domains, cyberspace is not governed by a single centralized authority. Instead, it is managed through a decentralized and contested web of actors—including states, international organizations, private corporations, technical communities, and civil society groups—each asserting varying degrees of influence over different aspects of digital life.

The governance of cyberspace can be broadly categorized into **technical governance**, **legal and policy governance**, and **normative or ethical governance**. Each operates across global, regional, and national levels, often overlapping or conflicting with one another. The most prominent example of technical governance is the **Internet Corporation**

[1] Niels ten Oever and Stefania Milan, "The Politics of Internet Infrastructure: Shaping the Expanse of the Internet," Internet Policy Review 8, no. 2 (2019).
[2] Kim Zetter, *Countdown to Zero Day* (2014), 8.

for Assigned Names and Numbers (ICANN), a California-based nonprofit organization that manages the **Domain Name System (DNS)**, coordinates IP addresses, and ensures the stability of the internet's naming infrastructure. Though originally overseen by the U.S. Department of Commerce, ICANN transitioned to a multistakeholder governance model in 2016, sparking debates over digital sovereignty and the continued dominance of U.S.-based institutions in cyberspace governance.[1]

The **multistakeholder model** promoted by ICANN and the **Internet Governance Forum (IGF)** is rooted in the idea that internet governance should involve a broad coalition of actors rather than being controlled by governments alone. This model emerged as a response to the growing role of private companies and civil society in shaping digital spaces and reflects the decentralized nature of the internet. However, critics argue that the multistakeholder approach disproportionately favors technologically advanced countries and multinational corporations, limiting meaningful participation from the Global South.[2]

In contrast, some states advocate for a **multilateral model**, where governments play the leading role in internet governance. This perspective is most strongly advanced by countries such as **China**, **Russia**, and **Iran**, who argue for the primacy of state sovereignty in managing domestic internet spaces. These countries promote cyber sovereignty—a principle asserting that states have the right to regulate their own cyberspace without external interference.[3] The **Shanghai Cooperation Organization (SCO)** and forums like the **World Internet Conference** in China support this model, proposing state-centered alternatives to Western-led internet institutions.[4]

One of the most contested areas of cyberspace governance involves the regulation of **content and data flows**. Governments and international organizations attempt to manage issues such as hate speech,

[1] Laura DeNardis, *The Global War for Internet Governance*, 36.
[2] Milton Mueller, *Networks and States* (MIT Press, 2010), 112.
[3] Adam Segal, The Hacked World Order (New York: PublicAffairs, 2016), 139.
[4] Tim Maurer, *Cyber Mercenaries.*

misinformation, digital surveillance, and data protection. The **European Union's General Data Protection Regulation (GDPR)**, enacted in 2018, represents one of the most influential legal frameworks in this regard. GDPR sets strict rules on data privacy and user consent, with global ramifications due to its extraterritorial application.[1] In contrast, the United States maintains a fragmented, sector-specific approach to data regulation, with stronger protections in areas like healthcare and finance but limited general oversight.[2]

Another critical aspect of cyberspace governance is **cybersecurity and international law**. The increasing frequency of state-sponsored cyberattacks and transnational cybercrime has prompted efforts to develop international norms and legal frameworks. The **United Nations Group of Governmental Experts (UNGGE)** and the **Open-Ended Working Group (OEWG)** have been central to negotiating norms for responsible state behavior in cyberspace, including prohibitions on attacking critical infrastructure during peacetime.[3] However, consensus remains fragile, as powerful nations often interpret cyber norms according to their strategic interests.

Non-state actors also play significant roles in cyberspace governance. Companies like **Google**, **Meta (Facebook)**, and **Amazon** have unparalleled power in determining how information flows online, moderating content, and collecting user data. These firms operate transnationally and are often criticized for lacking transparency and accountability. The growing influence of these digital giants has led some scholars to describe them as "digital sovereigns" due to their control over key parts of the online ecosystem.[4] Their decisions—whether algorithmic, economic, or policy-driven—can have global implications, yet they remain subject to limited external oversight.

[1] Paul De Hert and Vagelis Papakonstantinou, "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?" Computer Law & Security Review 32, no. 2 (2016): 179–194.
[2] Daniel J. Solove and Woodrow Hartzog, Breached!: Why Data Security Law Fails and How to Improve It (New York: Oxford University Press, 2022), 67.

[3] United Nations Group of Governmental Experts, Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174 (2015).

[4] Shoshana Zuboff, The Age of Surveillance Capitalism (New York: PublicAffairs, 2019), 132.

Civil society organizations, including NGOs and academic institutions, contribute to cyberspace governance by advocating for digital rights, promoting open-source development, and ensuring representation for marginalized groups. Initiatives such as the **Electronic Frontier Foundation (EFF)**, **Access Now**, and **Global Voices** work to protect online freedom, privacy, and inclusion, especially in contexts where state or corporate actors may act in abusive or discriminatory ways.[1]

Despite these numerous players and frameworks, cyberspace governance remains highly **fragmented**. No binding international treaty currently exists to regulate state behavior in cyberspace. Attempts to develop such instruments—like the proposed **UN Cybercrime Convention**—have been met with skepticism from digital rights advocates, who fear that authoritarian regimes may exploit legal frameworks to suppress dissent.[2] The lack of consensus has led to a "normative vacuum" in which powerful states and corporations exert disproportionate influence, leaving weaker states and users vulnerable to abuse or exclusion.

In response, some scholars and policymakers have proposed the concept of a **"polycentric governance model"**, where authority is distributed among multiple centers that coordinate through rules, norms, and mutual recognition. This model acknowledges the diversity of actors and interests in cyberspace and aims to balance innovation, security, and human rights in a more inclusive manner.[3]

In conclusion, the governance of cyberspace is a dynamic and contested field shaped by shifting power relations between states, corporations, and civil society. As cyberspace continues to permeate every aspect of human activity, its governance will remain a central issue

[1] Ronald J. Deibert, *Black Code*, 187.
[2] Human Rights Watch, "Proposed UN Cybercrime Treaty Could Harm Rights," last modified August 2021. https://www.hrw.org/news/2021/08/11/proposed-un-cybercrime-treaty-could-harm-rights.
[3] Stefania Milan and Niels ten Oever, "Internet Governance as a Decentralized, Polycentric Order," Internet Policy Review 6, no. 3 (2017).

in debates over digital rights, global justice, and the future of international order.

1.7 Key Actors in Cyberspace

The governance, evolution, and security of cyberspace are influenced by a diverse range of actors operating across public, private, and civil society domains. These key actors shape policies, norms, infrastructure, and user experiences, often in overlapping or conflicting ways. Their roles are dynamic and reflect the decentralized, global, and multi-stakeholder nature of cyberspace.

Nation-states are among the most powerful actors in cyberspace. States use digital technologies for governance, surveillance, diplomacy, intelligence gathering, and warfare. They also play a central role in establishing legal frameworks, enforcing cybersecurity standards, and negotiating international norms. For instance, the United States maintains significant influence due to its historical role in the development of the internet and its control over critical infrastructure such as the Internet Assigned Numbers Authority (IANA) and root name servers.[1] On the other hand, countries like China and Russia emphasize digital sovereignty and tightly regulate their domestic internet space, advocating for multilateral governance models through platforms like the Shanghai Cooperation Organization (SCO).[2]

State actors also invest heavily in cyber capabilities for both defense and offense. Cyber units such as the U.S. Cyber Command, Russia's GRU Unit 74455, and China's PLA Unit 61398 have been linked to sophisticated cyber operations ranging from espionage and intellectual property theft to attacks on critical infrastructure.[3] These activities often blur the line between national security and international aggression, raising concerns over escalation and norm violations.

Private sector corporations, particularly technology companies, are equally influential in shaping cyberspace. Corporations such as

[1] Laura DeNardis, *The Global War for Internet Governance*, 42.
[2] Adam Segal, The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (New York: PublicAffairs, 2016), 147.
[3] Kim Zetter, *Countdown to Zero Day* (2014), 56.

Google, Microsoft, Amazon, Meta (formerly Facebook), Apple, and Alibaba own vast portions of the digital infrastructure and dominate software, data storage, and communication services. These firms influence the architecture of cyberspace, set de facto standards, and often act as arbiters of online speech and conduct.[1] For example, content moderation policies and algorithmic decisions by platforms like YouTube or Facebook can impact billions of users and influence political discourse globally.

Moreover, private companies frequently collaborate with governments on issues like national security, data requests, and counterterrorism. However, this collaboration also raises privacy and human rights concerns, particularly in authoritarian contexts where governments may compel companies to censor content or share user data.[2] Tech giants also engage in global lobbying to shape regulations in ways that align with their interests, making them powerful political actors beyond the commercial realm.

The **technical and standards-setting communities** form another vital pillar of cyberspace governance. Organizations such as the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), and the Internet Corporation for Assigned Names and Numbers (ICANN) develop and maintain the protocols and standards that enable the global internet to function.[3] These groups typically operate through open, consensus-based processes and are composed of engineers, academics, and other stakeholders. While formally non-political, their decisions can have significant geopolitical implications, especially when they intersect with national interests or global conflicts.

International organizations and multilateral institutions also play key roles in shaping cyberspace norms and cooperation. The United Nations, through the Group of Governmental Experts (UNGGE) and the Open-Ended Working Group (OEWG), seeks to establish norms for responsible state behavior in cyberspace and promote confidence-

[1] Shoshana Zuboff, The Age of Surveillance Capitalism (New York: PublicAffairs, 2019), 129.
[2] Ronald J. Deibert, Reset: Reclaiming the Internet for Civil Society (Toronto: House of Anansi, 2020), 85.
[3] Milton Mueller, *Networks and States* (MIT Press, 2010), 63.

building measures among states.[1] Similarly, regional organizations such as the European Union (EU), African Union (AU), and the Organization for Security and Co-operation in Europe (OSCE) have developed strategies and policies related to cybersecurity, digital rights, and cybercrime. The EU, in particular, has emerged as a normative power in cyberspace, especially through the enforcement of the General Data Protection Regulation (GDPR).[2]

Civil society organizations advocate for the protection of digital rights, open access, and inclusivity in cyberspace. These include non-governmental organizations (NGOs), academia, journalists, and activist groups that monitor corporate practices, state surveillance, and censorship. Groups like the Electronic Frontier Foundation (EFF), Access Now, Reporters Without Borders, and the Association for Progressive Communications work to ensure that digital technologies serve the public interest.[3] Civil society actors also participate in multistakeholder forums such as the Internet Governance Forum (IGF), promoting transparency, accountability, and human rights in cyberspace policy-making.

Hackers and hacktivists represent another unconventional yet significant group. While their actions are often outside formal institutions, they have played major roles in exposing surveillance programs, highlighting corporate or governmental vulnerabilities, and resisting censorship. The Anonymous collective, for instance, has conducted digital operations to protest against perceived injustices, while whistleblowers like Edward Snowden have had a profound impact on public awareness regarding state surveillance practices.[4] At the same time, some hacker groups act as proxies for state interests, further complicating attribution and accountability in cyberspace.

[1] United Nations, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174 (2015).
[2] Paul De Hert and Vagelis Papakonstantinou, "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?" Computer Law & Security Review 32, no. 2 (2016): 179–194.
[3] Electronic Frontier Foundation, "Our Work," accessed June 2025, https://www.eff.org/about.
[4] Gabriella Coleman, Hacker, Hoaxer, Whistleblower, Spy, 241.

Criminal organizations exploit the anonymity and global reach of cyberspace to conduct illicit activities such as ransomware attacks, phishing scams, identity theft, and the operation of darknet markets. These groups are often transnational and agile, making them difficult to track and prosecute. The rise of ransomware-as-a-service (RaaS) models and cryptocurrency payments has made cybercrime more accessible and profitable, posing severe threats to financial systems, hospitals, and public infrastructure.[1]

Finally, **individual users** are both the most numerous and the most vulnerable actors in cyberspace. Users generate data, shape digital cultures, and are often the targets of manipulation, surveillance, or exploitation. While individual influence may be limited compared to institutional actors, user behavior—ranging from voting with clicks to participating in online movements—can drive broader changes in governance and platform policies. The rise of user-led advocacy, such as net neutrality protests or privacy campaigns, reflects the potential power of collective user action.[2]

The interplay among these actors is complex, often adversarial, and constantly evolving. As cyberspace becomes more deeply integrated into political, economic, and social life, understanding the roles and interactions of its key actors is essential for shaping fair, secure, and inclusive digital futures.

1.8 Cyberspace as a Domain of Conflict

Cyberspace has rapidly evolved into a distinct domain of conflict, akin to traditional theaters such as land, sea, air, and outer space. This transformation reflects the growing reliance of military, governmental, and civilian infrastructures on interconnected digital networks and the capacity of cyberspace to serve as both a battlefield and a strategic tool. Unlike conventional domains, cyberspace is characterized by low

[1] Europol, "Internet Organised Crime Threat Assessment (IOCTA) 2022," accessed June 2025, https://www.europol.europa.eu.
[2] Ethan Zuckerman, Mistrust: Why Losing Faith in Institutions Provides the Tools to Transform Them (New York: W. W. Norton & Company, 2020), 168.

barriers to entry, attribution challenges, asymmetrical advantages, and a blurring of lines between peacetime and wartime activities.

State-sponsored cyber operations have become a primary tool in geopolitical rivalries. These operations include espionage, sabotage, influence campaigns, and the pre-positioning of malware within critical infrastructure. For example, the Stuxnet worm—discovered in 2010—was allegedly developed jointly by the United States and Israel to target Iran's nuclear enrichment facilities. It is widely regarded as the first digital weapon to cause physical damage to real-world infrastructure, setting a precedent for cyberwarfare.[1] Since then, states have integrated cyber capabilities into their military doctrines. The United States officially recognized cyberspace as a warfighting domain in 2011, followed by the establishment of U.S. Cyber Command.[2] Similarly, NATO declared cyberspace as an operational domain in 2016, asserting that a cyberattack could trigger Article 5, the alliance's collective defense clause.[3]

Cyber conflicts differ from conventional warfare in several key ways. First, they often unfold in the grey zone between war and peace. Covert cyber operations such as election interference, disinformation campaigns, or the theft of state secrets do not cross the traditional threshold of armed attack under international law, but they may still generate strategic effects. For instance, Russia's interference in the 2016 U.S. presidential election involved coordinated cyber intrusions, leaks, and social media manipulation designed to undermine trust in democratic institutions.[4] These operations have been categorized as "information warfare," highlighting the strategic use of digital tools to influence perception and behavior without firing a single shot.[5]

[1] Kim Zetter, *Countdown to Zero Day* (2014), 6–9.
[2] Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," July 2011.
[3] NATO, "Warsaw Summit Communiqué," July 9, 2016.
[4] Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," January 6, 2017.
[5] Thomas Rid, Active Measures: The Secret History of Disinformation and Political Warfare (New York: Farrar, Straus and Giroux, 2020), 295.

Second, cyberattacks are difficult to attribute with certainty. Sophisticated threat actors often employ obfuscation techniques such as proxy servers, false flags, and malware reuse to hide their identities or shift blame. This lack of clear attribution complicates response options and weakens deterrence, as victims may hesitate to retaliate without incontrovertible proof.[1] In many cases, governments are reluctant to disclose attribution findings due to intelligence sensitivities, further reducing transparency and accountability.

Third, the cyber domain empowers non-state actors—such as hacktivists, criminal groups, and private contractors—who can disrupt national and international security. Groups like Anonymous or LulzSec have launched attacks on government websites and corporations, often in the name of political causes. Meanwhile, ransomware gangs have increasingly targeted critical infrastructure, exemplified by the 2021 attack on Colonial Pipeline in the United States, which led to fuel shortages across the East Coast.[2] Though some of these groups operate independently, others have been linked to state intelligence services or tolerated by host governments, blurring the line between state and non-state actors.

Critical infrastructure—such as energy grids, water systems, hospitals, and financial institutions—is especially vulnerable in cyberspace. These systems often rely on legacy technologies with inadequate cybersecurity measures. The 2015 and 2016 cyberattacks on Ukraine's power grid, attributed to the Russian-linked group Sandworm, demonstrated the real-world consequences of cyberattacks on civilian infrastructure.[3] As digitalization expands, the potential impact of cyberattacks on public safety, economic stability, and societal trust becomes increasingly severe.

International efforts to regulate conflict in cyberspace have struggled to keep pace. There is no comprehensive treaty on

[1] Michael Schmitt and Liis Vihul, eds., Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge: Cambridge University Press, 2013), 43.
[2] Cybersecurity and Infrastructure Security Agency (CISA), "DarkSide Ransomware: Best Practices for Preventing Business Disruption," May 2021.
[3] Andy Greenberg, *Sandworm* (2019), 102.

cyberwarfare akin to the Geneva Conventions. However, the Tallinn Manual—an academic, non-binding study led by NATO's Cooperative Cyber Defence Centre of Excellence—has attempted to apply existing international law to cyber operations. It argues that principles such as sovereignty, proportionality, and necessity apply in cyberspace, but implementation remains inconsistent.[1] Furthermore, major powers disagree on the application of international law to cyberspace. Western countries advocate for the applicability of existing law, while others, like China and Russia, push for new treaties emphasizing state control and digital sovereignty.[2]

Efforts by the United Nations through the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) have yielded some progress. Both bodies have produced consensus reports affirming that international law applies in cyberspace and calling for responsible state behavior. However, enforcement mechanisms are lacking, and political divisions hinder deeper cooperation.[3] Additionally, cyberspace's transnational nature makes unilateral regulation insufficient, necessitating international collaboration among governments, private entities, and civil society.

Cyber conflict also has economic and psychological dimensions. Cyber operations can be designed to sow panic, erode trust in institutions, or exert economic pressure without conventional military engagement. For example, the NotPetya malware, initially disguised as ransomware, inflicted billions of dollars in damages to multinational companies and government agencies in 2017. Though it targeted Ukrainian infrastructure, its indiscriminate spread affected organizations across the globe, including Maersk, Merck, and FedEx. The U.S. and UK later attributed the attack to the Russian military.[4] This case illustrated how a single cyberattack can generate unintended, global collateral

[1] Schmitt and Vihul, Tallinn Manual, 185.
[2] Tim Maurer, *Cyber Mercenaries.*

[3] United Nations, "Report of the Group of Governmental Experts (2021)," A/76/135.

[4] Andy Greenberg, *Sandworm* (2019), 186–193.

damage—raising serious concerns about cyberweapons' unpredictability.

As cyber capabilities become more integrated into hybrid warfare strategies, the line between civilian and military targets continues to erode. Modern military doctrines now include cyber tools for intelligence gathering, battlefield disruption, and psychological operations. At the same time, most of cyberspace is owned and operated by the private sector, making coordination with non-governmental actors essential for national defense. Public-private partnerships, information sharing, and joint response exercises are increasingly common components of cyber readiness.[1]

2. Cybersecurity

2.1 Distinctions Among Digital Security, Cybersecurity, and others

The distinction between digital security and information security is often blurred in both academic discourse and practical application. However, understanding their differences is critical to designing effective policies, strategies, and technical frameworks for modern security needs. Digital security refers broadly to the protection of all digital assets, systems, and users from unauthorized access, disruption, or modification. It encompasses a wide range of practices and technologies that safeguard not only data but also digital identities, devices, and online behaviors. Information security, by contrast, is a narrower concept focused specifically on the **confidentiality, integrity, and availability (CIA)** of information, regardless of its form—digital, physical, or verbal.[2]

One of the clearest distinctions lies in scope. Information security covers both digital and non-digital forms of information, such as printed documents or verbal communication in a secure environment. For example, a locked file cabinet containing confidential personnel records

[1] National Institute of Standards and Technology (NIST), "Cybersecurity Framework," 2018.
[2] ISO/IEC 27000:2018, Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary (Geneva: International Organization for Standardization, 2018).

is a matter of information security but not digital security. In contrast, digital security involves technologies such as encryption, two-factor authentication, and device management, which are tailored to protect digital interactions and assets.[1]

Another important difference lies in the focus on **user behavior and identity**. Digital security often addresses threats posed through user interactions with technology, such as phishing scams, malware downloads, and poor password hygiene.[2] In contrast, information security may not always consider user-centric threats; it focuses more on data governance and access control mechanisms that apply to both human and machine interactions. For instance, an organization's access management policy designed to protect sensitive files from unauthorized employees is part of information security, whereas user training on avoiding phishing emails is more aligned with digital security.[3]

These differences become even more apparent when we examine adjacent concepts like **cybersecurity**. While digital security and cybersecurity are often used interchangeably, some frameworks draw distinctions. Cybersecurity traditionally focuses on protecting systems and networks against external threats, particularly those arising from cyberspace—such as nation-state attacks, ransomware, or distributed denial-of-service (DDoS) attacks.[4] Digital security, meanwhile, extends to include the individual and behavioral dimensions of security, such as protecting personal digital identities, online communications, and mobile applications.[5]

Data security and **data protection** are two additional terms that overlap with both digital and information security but focus more specifically on safeguarding data from loss, corruption, theft, or unauthorized access. Data protection is also often used in the context of compliance with privacy regulations like the **General Data Protection**

[1] ENISA, Digital Security.
[2] Cybersecurity and Infrastructure Security Agency (CISA), "Cyber Essentials," https://www.cisa.gov/cyber-essentials.
[3] NIST, Framework for Improving Critical Infrastructure Cybersecurity.
[4] United Nations GA Report, *A/76/135 (2021).*
[5] Microsoft, "Digital Geneva Convention".

Regulation (GDPR) in the European Union.[1] Information security policies will typically include data protection provisions, but not all data protection practices are necessarily digital—for example, secure storage of printed health records.[2]

Similarly, **network security** refers to the practices and technologies that secure a computer network infrastructure. It includes firewalls, intrusion detection systems, and VPNs. While network security is a subset of cybersecurity, it does not encompass the broader human-centric and digital identity issues addressed by digital security. For example, a firewall might block unauthorized traffic from entering a system (network security), while digital security would also include user behavior monitoring to prevent internal breaches.[3]

Understanding these distinctions is particularly important in the public sector and critical infrastructure industries, where terms like "digital security" and "cybersecurity" appear in national strategies. For instance, the **European Union's Cybersecurity Strategy** emphasizes resilience against cyber threats to digital services and infrastructure but also references broader concerns such as digital autonomy and trust in digital services, which align more closely with digital security.[4] Similarly, the **National Institute of Standards and Technology (NIST)** provides distinct guidelines for cybersecurity risk management and information security controls, highlighting that they serve overlapping but not identical goals.[5]

Finally, the **cultural and legal context** also shapes how these terms are used. In countries with strong digital sovereignty agendas, digital security includes not just the technical protection of assets but also strategic goals like data localization, digital independence, and online

[1] European Commission, "General Data Protection Regulation (GDPR)," https://ec.europa.eu/info/law/law-topic/data-protection_en.
[2] OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.
[3] IBM, "What is Network Security?," https://www.ibm.com/topics/network-security.
[4] European Commission, "EU Cybersecurity Strategy."
[5] NIST, Framework for Improving Critical Infrastructure Cybersecurity.

censorship.[1] In such cases, digital security becomes a political concept as much as a technical one, expanding far beyond traditional information security practices.

In sum, digital security is a broader, more inclusive term that integrates behavioral, technical, and identity-based protections in the digital environment. Information security remains crucial for protecting data across all mediums, but it does not fully address the unique challenges of our increasingly interconnected digital world. Awareness of these differences allows for more targeted, efficient, and adaptive security frameworks across sectors and disciplines.

2.2 Defining Digital Security and Its Global Significance

Digital security, often called cybersecurity, refers to the protection of internet-connected systems—including hardware, software, and data—from cyber threats. It aims to prevent unauthorized access, data breaches, and disruptions to services. Digital security ensures the **confidentiality, integrity, and availability** of data, commonly known as the CIA triad in cybersecurity frameworks.[2] With the rise of the internet, cloud computing, smart devices, and critical infrastructure automation, digital security has evolved into a central component of national and international security strategies.

The need for cybersecurity emerged as digital networks grew in complexity and became targets for malicious activity. In its early stages, cybersecurity focused primarily on antivirus protection and securing personal computers. Today, it encompasses a much wider field: **threat intelligence, encryption, identity management, network monitoring, incident response, and cybercrime investigation**. Modern cyberattacks are often conducted by organized criminal groups, hacktivists, or state-

[1] Krapiva, "Russia's Sovereign Internet".
[2] National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (Gaithersburg, MD: NIST, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

sponsored actors using sophisticated techniques such as ransomware, phishing, denial-of-service attacks, and zero-day exploits.[1]

Digital security has become essential not just for protecting individual users but also for defending **critical national infrastructure**. Power grids, hospitals, banking systems, airports, and water treatment facilities are increasingly managed by digital systems that, if compromised, could cause catastrophic damage. The 2015 cyberattack on Ukraine's power grid, which resulted in widespread blackouts, is a prominent example of how cyber operations can impact physical infrastructure and national security.[2]

International cooperation on cybersecurity has accelerated in response to such threats. The **United Nations** has taken steps to develop a common understanding of responsible state behavior in cyberspace. Through the **UN Group of Governmental Experts (GGE)**, member states have agreed that international law—including the **UN Charter and principles of sovereignty and non-intervention**—applies to cyber activities.[3] However, disagreements remain over how exactly these principles are interpreted and enforced in the digital realm.

The **European Union** has also taken a leadership role in cybersecurity regulation. The **General Data Protection Regulation (GDPR)** and the **NIS Directive (Network and Information Security Directive)** set legal obligations on data protection and network security for both public and private organizations within the EU. These regulations also have extraterritorial effects, influencing how international firms handle data and protect digital assets.[4]

Meanwhile, the **United States** has adopted a multi-agency approach to cybersecurity, involving the **Cybersecurity and Infrastructure**

[1] ENISA, Threat Landscape Report 2022: Interconnected Threats, European Union Agency for Cybersecurity, 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.
[2] Andy Greenberg, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.
[3] United Nations General Assembly, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace, A/76/135, July 14, 2021, https://undocs.org/A/76/135.
[4] European Commission, "EU Cybersecurity Strategy for the Digital Decade," 2020, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

Security Agency (CISA), **Federal Bureau of Investigation (FBI)**, and **National Security Agency (NSA)**, among others. CISA, in particular, plays a central role in coordinating the defense of critical infrastructure and issuing advisories on threats such as ransomware and foreign cyber espionage.[1]

Another major cybersecurity issue is **cyber sovereignty**—the idea that states should have control over their digital infrastructure and the flow of data within their borders. Countries such as **China** and **Russia** advocate for a more state-centric internet, where governments tightly regulate and monitor domestic cyberspace. In contrast, Western democracies generally support an open, global internet with multi-stakeholder governance involving civil society, academia, the private sector, and governments.[2] These competing models influence how international law, human rights, and commerce operate in cyberspace.

Data privacy and **surveillance** are closely linked to digital security debates. Mass data collection by governments and corporations poses risks to civil liberties, especially when conducted without proper oversight. Whistleblower Edward Snowden's 2013 revelations about global surveillance by the NSA sparked widespread concern about the lack of transparency in intelligence operations and the vulnerabilities of digital communications.[3] Balancing the need for security with respect for privacy and human rights remains one of the core challenges in the cybersecurity field.

Additionally, **cybersecurity education and workforce development** are key components of national resilience. As cyber threats increase, so does the demand for skilled professionals. According to a report by (ISC)², the global cybersecurity workforce gap reached over 3 million in 2023, underscoring the need for investment in training and

[1] Cybersecurity and Infrastructure Security Agency (CISA), "Cybersecurity Guidance and Resources," https://www.cisa.gov/cybersecurity.
[2] Adam Segal, The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (New York: PublicAffairs, 2016), 121–134.
[3] Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (New York: Metropolitan Books, 2014).

education.[1] Governments and universities are launching new programs in cybersecurity law, digital forensics, and ethical hacking to address this shortfall.

In summary, cybersecurity has grown from a technical concern to a multifaceted issue that touches on national defense, international law, human rights, and global commerce. It requires constant adaptation to emerging threats and a collaborative approach between governments, the private sector, and civil society to ensure a secure and open digital future.

2.3 The Evolution of International Approaches to Cybersecurity

The field of international cybersecurity has undergone significant transformation since the early days of the internet. Initially centered around the protection of isolated networks, the concept has expanded to include global governance, state responsibility, digital sovereignty, and the norms of behavior in cyberspace. As cyber threats have evolved, so too have the responses of states and international organizations attempting to establish frameworks for cooperation, deterrence, and regulation.

In the 1990s, cybersecurity was primarily a domestic issue, concerned with viruses, worms, and unauthorized access to systems. At that time, international legal instruments addressing cybercrime were limited. The **Council of Europe's Budapest Convention on Cybercrime (2001)** marked the first international treaty to focus on crimes committed via the internet and other computer networks. It remains the only binding international agreement in this domain, establishing common definitions for cybercrime and fostering international cooperation on criminal justice matters in cyberspace.[2]

By the early 2000s, cyberattacks began to gain strategic significance. The 2007 **cyberattacks against Estonia**, widely attributed

[1] (ISC)², Cybersecurity Workforce Study 2023, https://www.isc2.org/Research/Workforce-Study.
[2] Council of Europe, Convention on Cybercrime (ETS No. 185), November 23, 2001, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

to Russian hackers, marked a turning point in the global understanding of cybersecurity as a national and international security concern. The attacks paralyzed government and financial services and demonstrated the potential for cyber operations to disrupt critical infrastructure.[1] In response, NATO launched the **Cooperative Cyber Defence Centre of Excellence (CCDCOE)** in Tallinn, Estonia, to study and coordinate cyber defense strategies among member states.[2]

The attacks on Estonia spurred conversations around the **application of international law to cyberspace**. The **UN Group of Governmental Experts (GGE)** on Developments in the Field of Information and Telecommunications in the Context of International Security began convening in 2004. Over several sessions, the GGE affirmed that **international law, particularly the UN Charter, applies to cyberspace**, including norms of sovereignty, non-intervention, and the prohibition of the use of force.[3] However, states remain divided on how to operationalize these principles, especially when attributing responsibility for cyberattacks.

In 2013 and 2015, the GGE produced consensus reports that were widely praised for establishing a baseline of acceptable behavior in cyberspace. They emphasized voluntary norms, such as not attacking critical infrastructure during peacetime and cooperating on cyber incident responses.[4] Yet by 2017, geopolitical tensions—particularly between Western states and Russia and China—prevented the GGE from reaching further consensus.

These divisions gave rise to **competing visions of cyber governance**. The **United States and European Union** advocate for a multistakeholder model that includes civil society, the private sector, and governments, supporting a global, open internet. In contrast, **China and**

[1] Damien McGuinness, "How a Cyber Attack Transformed Estonia," BBC News, April 27, 2017, https://www.bbc.com/news/39655415.
[2] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), "About Us," https://ccdcoe.org/about-us/.
[3] United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, June 24, 2013, https://undocs.org/A/68/98.
[4] Elaine Korzak, "Norms in Cyberspace: The GGE's Muted Report," Lawfare, July 18, 2015, https://www.lawfaremedia.org/article/norms-cyberspace-gges-muted-report.

Russia promote a state-centric model where each country controls its own digital territory, advocating for a new international treaty on cybersecurity under the UN framework to regulate content and infrastructure.[1]

To supplement diplomatic efforts, **regional organizations** have also developed cybersecurity strategies. The **European Union** adopted its **Cybersecurity Strategy for the Digital Decade** in 2020, aiming to bolster collective cyber defense and establish digital operational resilience frameworks for sectors like energy, finance, and healthcare.[2] Meanwhile, the **African Union's Convention on Cyber Security and Personal Data Protection (Malabo Convention)**, signed in 2014, addresses data privacy, e-commerce, and cybercrime but has yet to be widely ratified.[3]

The **Tallinn Manual on the International Law Applicable to Cyber Warfare**, developed by legal scholars under the auspices of NATO's CCDCOE, provides a comprehensive analysis of how existing international law applies to cyber conflicts. Although non-binding, the manual is an important resource for legal interpretation and academic debate.[4]

More recently, the UN launched the **Open-Ended Working Group (OEWG)** to continue discussions on responsible state behavior in cyberspace. Unlike the GGE, the OEWG includes all UN member states and has focused on building trust and confidence through capacity-building and dialogue. The group's final report in 2021 reaffirmed the applicability of international law and called for further development of cyber norms.[5]

[1] Segal, The Hacked World Order, 145–163.
[2] European Commission, "EU Cybersecurity Strategy."
[3] African Union, Convention on Cyber Security and Personal Data Protection (Malabo Convention), 2014, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.
[4] Michael N. Schmitt, ed., Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge: Cambridge University Press, 2013).
[5] United Nations General Assembly, Final Substantive Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, A/76/135, July 14, 2021, https://undocs.org/A/76/135.

In parallel, the **private sector and civil society** have assumed growing roles in international cybersecurity. Initiatives like **Microsoft's Digital Geneva Convention proposal** and the **Paris Call for Trust and Security in Cyberspace**—supported by over 70 states—advocate for new rules to protect civilians and infrastructure during cyber conflicts.[1] These efforts highlight the complexity of modern cyberspace governance, where governments no longer act alone but must engage with a wide range of actors.

In conclusion, the evolution of international cybersecurity reflects the growing interdependence of states in a digitized world. While legal frameworks and norms have made significant strides, persistent disagreements over sovereignty, jurisdiction, and attribution continue to pose challenges. The international community must navigate these issues to establish a secure, stable, and rights-respecting cyberspace.

2.4 Cybersecurity and National Sovereignty

Cybersecurity has become a fundamental pillar in maintaining national sovereignty. In the age of digital interdependence, a state's ability to control and defend its cyberspace has become as vital as controlling its physical territory. The concept of cyber sovereignty is rooted in a state's right to govern activities within its digital borders, including data regulation, content management, and protection of critical infrastructure. While globalization initially promoted a borderless internet, the rise of cyber threats has compelled nations to reclaim control over digital domains.

China offers the most prominent example of this approach. Its Cybersecurity Law of 2017, along with subsequent legislation, mandates that data collected within China be stored locally and gives authorities significant power to monitor and restrict online activity. This legal framework exemplifies how Beijing uses cybersecurity to reinforce political authority, enforce ideological conformity, and safeguard national interests.[2] Such measures are consistent with China's broader

[1] Microsoft Blog, *Digital Geneva Convention.*
[2] Segal, Hacked World Order, 52–53.

vision of cyber sovereignty, which seeks to counter Western dominance of global internet governance and preserve state-centric control.[1]

Russia has followed a similar path. In 2019, it passed the "sovereign internet" law, designed to enable the country to disconnect from the global internet during emergencies.[2] This includes the creation of a national domain name system and the rerouting of internet traffic through domestic exchange points. Although the Russian government frames this as a protective measure, critics argue it undermines digital freedoms and enables extensive state surveillance.[3] The Russian model, like China's, emphasizes a cybersecurity policy rooted in territorial sovereignty, where the internet is not a global commons but a space divided by national jurisdictions.

Western democracies have approached the issue differently. The European Union (EU), while upholding the principle of a free and open internet, has introduced stringent data protection and cybersecurity regulations to assert its digital autonomy. The General Data Protection Regulation (GDPR) and the EU Cybersecurity Strategy for the Digital Decade are examples of how the EU balances individual rights with collective security.[4] These frameworks affirm the EU's commitment to democratic values while recognizing the need for cyber resilience in the face of rising threats. Cyber sovereignty here is not about isolating national cyberspaces but about ensuring that digital infrastructures are secure, transparent, and subject to democratic oversight.

The strategic importance of cybersecurity for sovereignty is most visible in the realm of critical infrastructure. Energy grids, financial systems, communication networks, and health services are increasingly digitized, making them vulnerable to cyberattacks. The 2007 cyberattacks on Estonia, widely attributed to Russian actors, marked a

[1] Segal, Hacked World Order, 72.
[2] Andrei Soldatov and Irina Borogan, "Russia's Sovereign Internet Law," Carnegie Endowment for International Peace, October 24, 2019, https://carnegieendowment.org/2019/10/24/russia-s-sovereign-internet-law-pub-80131.
[3] Natalia Krapiva, "Russia's Sovereign Internet Is a Model for Censorship," Access Now, April 7, 2021, https://www.accessnow.org/russia-sovereign-internet-censorship/.
[4] European Commission, "EU Cybersecurity Strategy."

turning point.[1] They targeted banks, media outlets, and government servers, demonstrating how cyber warfare can disrupt national stability without a single shot being fired. In 2024, another alarming example emerged when hackers linked to the Russian state targeted water facilities in Texas, exploiting outdated software and insufficient federal oversight.[2] Such incidents highlight how cybersecurity is no longer just a technical concern but a matter of national defense.

This shift has made attribution—a key challenge in cyber warfare—a central issue in sovereignty debates. Unlike traditional military attacks, cyber operations are difficult to trace with certainty, allowing aggressors plausible deniability. This complicates international legal responses and often leaves victim states with limited recourse. The absence of binding global norms for cyberspace governance exacerbates the problem, as existing international law struggles to address non-kinetic, transnational threats.[3] While some efforts have been made to develop confidence-building measures and establish international norms—such as the UN Group of Governmental Experts on Cybersecurity—they remain voluntary and under-enforced.[4]

The assertion of cyber sovereignty also carries risks. The trend toward digital nationalism threatens to fragment the internet into isolated networks, or a "splinternet," where access to information and digital services varies depending on geography. This balkanization of cyberspace could hinder economic innovation, restrict freedom of expression, and reduce global cooperation on shared challenges like cybercrime and misinformation.[5] It is therefore essential to find a

[1] Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," Proceedings of the 7th European Conference on Information Warfare and Security (2008), 163–168.
[2] Frank Bajak, "Cyberattacks on US Infrastructure Highlight Local Vulnerabilities," AP News, March 18, 2024, https://apnews.com/article/cybersecurity-texas-water-hack.
[3] Duncan B. Hollis, "Re-thinking the Boundaries of Law in Cyberspace: A Duty to Hack?" Temple Law Review 100, no. 3 (2021): 543–567.
[4] United Nations GA Report, *A/76/135 (2021)*.
[5] Emily Taylor, "The Splinternet: How Geopolitics and Commerce Are Fragmenting the World Wide Web," Chatham House, November 2020, https://www.chathamhouse.org/2020/11/splinternet-how-geopolitics-are-fragmenting-web.

balance between protecting sovereignty and preserving the global nature of the internet.

Ultimately, cybersecurity and national sovereignty are intertwined. As states navigate this complex terrain, they must reconcile the need for control with the benefits of openness. A pragmatic approach—anchored in robust cybersecurity infrastructure, international collaboration, and respect for democratic norms—offers the best path forward in a digitally sovereign but globally connected world.

2.5 Cybersecurity in International Law: Norms, Rules, and Legal Gaps

The rapid evolution of cyberspace has exposed significant challenges for international law, which was originally developed for a predominantly physical world. As state and non-state actors increasingly operate in the cyber domain, international law has been compelled to respond—though often reactively—by attempting to apply existing legal frameworks to novel digital phenomena. Central to this emerging legal discourse are the principles of sovereignty, non-intervention, due diligence, and the prohibition of the use of force, all of which must now contend with the intangibility and cross-border nature of cyber operations.

One of the most important normative contributions to international cybersecurity has come through the work of the United Nations. Since 2004, various Groups of Governmental Experts (GGE) and Open-Ended Working Groups (OEWG) have convened under the UN to address the security implications of information and communication technologies (ICTs). The 2013 and 2015 GGE reports marked key milestones by affirming that **existing international law applies to cyberspace**, including the UN Charter's provisions on the use of force and non-intervention in the internal affairs of states.[1] These reports also outlined voluntary norms of responsible state behavior, such as the duty not to

[1] United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98 (24 June 2013), 8–10.

damage critical infrastructure during peacetime, and the importance of cooperative mechanisms for investigating malicious cyber incidents.

However, while the recognition of international law's applicability is a foundational step, it has not resolved interpretive ambiguities. For instance, **the threshold at which a cyber operation constitutes a "use of force" under Article 2(4) of the UN Charter** remains disputed. Scholars and states differ on whether cyberattacks causing significant economic harm or disruption—such as the 2017 NotPetya attack—can amount to unlawful uses of force in the absence of kinetic damage.[1] The Tallinn Manual 2.0, developed by an independent group of experts, suggests that severity, immediacy, directness, invasiveness, and military character are among the factors to consider when assessing a cyber operation's legality under Article 2(4).[2] Nonetheless, this interpretation is non-binding and lacks universal acceptance.

Closely related is the issue of **state sovereignty in cyberspace**, which continues to generate divergent views. The principle of sovereignty implies that states have the right to control cyber infrastructure within their territory and to be free from unwanted foreign intrusion. However, there is no consensus on whether mere cyber intrusions—such as espionage or data exfiltration that do not cause physical damage—constitute violations of sovereignty. While some states, like the United Kingdom and the Netherlands, have taken a restrictive view of sovereignty's role in cyberspace, others, such as Iran and China, adopt broader interpretations that encompass a wider range of cyber operations.[3]

Moreover, **the principle of non-intervention** prohibits coercive interference in a state's internal or external affairs. Yet the definition of "coercion" in cyberspace remains fluid. For instance, a cyber campaign designed to manipulate another state's electoral outcomes may arguably

[1] Jack Goldsmith, "How NotPetya Has Changed the Landscape of Cybersecurity," Lawfare, February 20, 2018, https://www.lawfareblog.com/how-notpetya-has-changed-landscape-cybersecurity.
[2] Michael N. Schmitt, ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press, 2017), 345–58.
[3] Harriet Moynihan, The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention (Chatham House, 2019), https://www.chathamhouse.org/sites/default/files/2019-11-28-Application-of-International-Law-to-Cyberattacks.pdf.

amount to a violation of this principle, but establishing intent, coercion, and attribution simultaneously is legally and technically complex.[1]

The **principle of due diligence**, which obliges a state not to knowingly allow its territory to be used for acts that harm other states, is also under strain in the cyber context. Because cyber operations are often routed through multiple jurisdictions using compromised infrastructure, states may genuinely be unaware of hostile activities occurring through their networks. Nonetheless, calls have been made for greater clarity on what constitutes "reasonable" measures for monitoring and mitigating malicious cyber activity emanating from national networks.[2]

The issue of **attribution** is a central legal and practical obstacle in holding actors accountable for cyber operations. States are hesitant to publicly attribute cyberattacks due to the evidentiary burden and fear of escalation. Yet under the **law of state responsibility**, a state can be held accountable only when an act is attributable to it and constitutes a breach of an international obligation.[3] The challenge of securing reliable, publicly verifiable attribution hinders the effective enforcement of international legal norms in cyberspace.

Despite these gaps, states and organizations continue to develop frameworks to enhance normative clarity. For instance, the 2021 Final Report of the OEWG reaffirmed the voluntary, non-binding norms proposed by previous UN processes and emphasized the importance of capacity building, transparency, and confidence-building measures.[4] Meanwhile, regional efforts such as the European Union's **Cyber Diplomacy Toolbox** and the African Union's **Malabo Convention** seek

[1] Duncan B. Hollis, "An e-SOS for Cyberspace," Harvard International Law Journal 52, no. 2 (2011): 374–75.
[2] International Committee of the Red Cross, International Humanitarian Law and Cyber Operations During Armed Conflicts (November 2019), https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts.
[3] International Committee of the Red Cross, International Humanitarian Law and Cyber Operations During Armed Conflicts (November 2019), https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts.
[4] United Nations, Final Substantive Report of the Open-Ended Working Group on Developments in the Field of ICTs, A/AC.290/2021/CRP.2 (10 March 2021), https://documents.unoda.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

to complement global legal initiatives by providing mechanisms for joint response and legal harmonization.

In sum, while **international law provides a general framework for state behavior in cyberspace**, numerous legal uncertainties persist. These include the thresholds for the use of force, the scope of sovereignty, the standard of due diligence, and mechanisms for lawful attribution and enforcement. Bridging these gaps will require not only doctrinal development but also enhanced multilateral cooperation and shared interpretations of legal norms across diverse geopolitical contexts.

Section Two: Cyber threats and their impact on international security

In the 21st century, cyberspace has emerged as a critical domain of international security, alongside land, sea, air, and space. The global dependence on digital infrastructure has opened new vulnerabilities exploited by a growing range of cyber threats. These threats include state-sponsored espionage, ransomware campaigns, infrastructure sabotage, and misinformation operations, all of which can undermine national sovereignty, economic stability, and global peace. As the digital sphere expands, so too does the threat landscape, with malicious cyber activities now recognized as major strategic and political risks by governments and international organizations alike[1].

Cyber threats can be broadly defined as malicious actions that target computer systems, networks, and data to disrupt, damage, or gain unauthorized access, often for political, economic, or ideological purposes[2]. These threats are not limited to conventional cybercrime; they extend to acts of cyberterrorism, cyberwarfare, and cyberespionage. While some cyber incidents are driven by profit, others are orchestrated by nation-states or ideologically motivated actors to influence foreign

[1] Joseph S. Nye Jr., *The Regime Complex for Managing Global Cyber Activities.*
[2] U.S. Department of Homeland Security. “Cyber Threats.” https://www.dhs.gov/cisa/cyber-threats

policy, election outcomes, or national security decisions. The anonymity and transnational nature of the internet make it difficult to detect, attribute, and respond effectively to such attacks.

The impact of cyber threats on international security is profound and multifaceted. At the state level, cyber operations can degrade military capabilities, paralyze infrastructure, or manipulate public opinion—consequences that once required kinetic warfare to achieve. For example, cyberattacks targeting electrical grids, healthcare systems, and financial institutions can generate widespread disruption without physical confrontation, blurring the lines between war and peace[1]. The 2007 cyberattacks on Estonia, widely attributed to Russian actors, disrupted government and banking systems and were seen as one of the first examples of cyberwarfare affecting national stability[2].

Moreover, the strategic use of cyber operations has triggered a shift in power dynamics and global threat perceptions. States such as the United States, Russia, China, Iran, and North Korea have integrated cyber capabilities into their military and foreign policy doctrines, using them as tools of coercion, deterrence, or asymmetric warfare[3]. This growing militarization of cyberspace increases the risk of escalation and miscalculation, especially when attribution is unclear or when norms of responsible behavior are absent.

In addition, the rise of hybrid threats—where cyber tools are combined with disinformation campaigns, economic pressure, and diplomatic coercion—has complicated traditional approaches to security. These tactics are often used to destabilize societies from within, erode trust in democratic institutions, and weaken international alliances[4]. The COVID-19 pandemic, for instance, was accompanied by a surge in state-sponsored cyber intrusions and disinformation campaigns, revealing how crises can be exploited in the cyber domain to advance geopolitical agendas.

[1] Jason Healey (ed.), *A Fierce Domain* (2013).
[2] Tikk, Kaska, and Vihul, International Cyber Incidents.
[3] Thomas Rid, *Cyber War Will Not Take Place.*
[4] European External Action Service (EEAS). “Hybrid Threats.” https://www.eeas.europa.eu/eeas/hybrid-threats_en

As a result, cybersecurity has become an essential component of national defense and international diplomacy. Multilateral institutions, including NATO, the United Nations, and the European Union, have recognized the need to establish norms, build resilience, and coordinate responses to cyber threats. However, the lack of a universal legal framework governing state behavior in cyberspace continues to pose challenges to accountability and collective action[1]. In this context, understanding the nature of cyber threats and their implications is vital to shaping future strategies for peace and stability in the digital age. **This section provides a comprehensive analysis of the evolving landscape of cyber threats, examining their nature, sources, and operational methods, while also exploring their significant implications for global political stability and the structure of international security.**

1.2 Related Key Concepts: Definitions and Distinctions between Cybercrime, Cyberterrorism, Cyberespionage, and Traditional Terrorism

Cybercrime refers to illegal activities that are carried out using computers or networks. It encompasses a wide range of offenses, including identity theft, phishing, financial fraud, cyberstalking, and the distribution of malware. These acts are typically motivated by financial gain, personal revenge, or political agendas. Unlike traditional crimes, cybercrime can be committed remotely, often across national boundaries, making attribution and prosecution difficult. The perpetrators range from individual hackers to organized criminal syndicates. A key characteristic of cybercrime is its violation of confidentiality, integrity, or availability of data, often targeting both individuals and institutions alike[2].

Cyberterrorism, while sharing technological tools with cybercrime, differs in intent and target. It is defined as the use of computer systems to cause disruption or fear for political or ideological reasons. Cyberterrorist acts might include attacks on critical infrastructure, such as power grids, hospitals, and transportation systems, aiming to create

[1] United Nations, Group of Governmental Experts on ICT Security.
[2] Brenner, Susan W. Cybercrime: Criminal Threats from Cyberspace. Praeger, 2010.

mass panic or destabilize governments. What distinguishes cyberterrorism from other cyber threats is its purpose: to instill terror or coerce societies and governments into adopting specific political positions. Unlike cybercriminals, whose primary motive is profit, cyberterrorists seek ideological outcomes[1].

Espionage in cyberspace, or cyber espionage, involves the unauthorized access to confidential or sensitive information, typically for political, economic, or military advantage. Governments, corporations, and individuals can be both perpetrators and victims. State-sponsored hackers often infiltrate foreign networks to gather intelligence on military capabilities, trade secrets, or diplomatic strategies. While espionage has existed for centuries, cyberspace offers unprecedented opportunities for surveillance and data exfiltration. Importantly, cyber espionage is generally covert and not meant to be publicly known, unlike cyberterrorism, which is often designed to be visible and fear-inducing[2].

Terrorism, in the broader sense, involves the use of violence or threats to intimidate or coerce, especially for political purposes. It is not confined to the digital realm and often includes bombings, shootings, kidnappings, and other forms of physical violence. However, with the growth of digital technology, terrorists now often use the internet to recruit, fundraise, and coordinate attacks. Thus, while traditional terrorism and cyberterrorism may overlap in goals, they differ significantly in methods and immediacy of threat. The former generally causes physical harm, whereas the latter targets digital systems, though both aim to disrupt and influence societies[3].

Distinguishing between these concepts lies primarily in the actors, motives, and outcomes. Cybercrime is profit-driven and can be both opportunistic and organized. Cyberterrorism seeks to create fear for ideological or political ends, often targeting public safety or critical infrastructure. Cyber espionage focuses on gathering intelligence,

[1] Conway, Maura. "Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet." First Monday 7, no. 11 (2002). https://firstmonday.org/ojs/index.php/fm/article/view/1001
[2] Thomas Rid, *Cyber War Will Not Take Place.*
[3] Hoffman, Bruce. Inside Terrorism. Columbia University Press, 2017.

typically covertly, with no immediate public disruption. Traditional terrorism, in contrast, usually involves physical violence and direct human casualties. While cyberterrorism and cyber espionage may be state-sponsored, cybercrime is often perpetrated by non-state actors, though the lines can blur when cybercriminals are co-opted by state interests. Understanding these distinctions is critical for developing targeted cyber defense strategies and international legal responses[1].

1.3 Cyber threat categorization

Cyber threat categorization is essential for understanding and mitigating the wide array of risks that emerge from cyberspace. These threats can be broadly classified into several categories based on origin, motivation, method, and target. The primary categories include nation-state threats, cybercriminal threats, hacktivist threats, insider threats, and advanced persistent threats (APTs).

Nation-state threats originate from governments or state-sponsored entities and are often motivated by political, military, or economic objectives. These threats typically involve sophisticated operations targeting other states' critical infrastructure, intelligence systems, or commercial secrets. Cyber espionage, sabotage, and disinformation campaigns are frequently deployed tools. For example, the Stuxnet worm, allegedly developed by the United States and Israel, was used to sabotage Iran's nuclear program and is a key illustration of state-sponsored cyber operations[2]. Nation-state threats are marked by high technical complexity, extensive resources, and long-term strategic planning.

Cybercriminal threats are financially motivated and are typically perpetrated by individuals or organized criminal groups. These include activities such as ransomware attacks, identity theft, phishing, and credit card fraud. Ransomware attacks like WannaCry and REvil exemplify this category, where malicious software encrypts a victim's data and demands payment in exchange for the decryption key[3]. Cybercriminals

[1] Carr, Jeffrey. Inside Cyber Warfare: Mapping the Cyber Underworld. O'Reilly Media, 2011.
[2] Kim Zetter, *Countdown to Zero Day* (2014).
[3] Andy Greenberg, *Sandworm* (2019).

often exploit vulnerabilities in software, human behavior, or weak security protocols to gain access to valuable information or financial assets. This category is characterized by opportunism, speed, and a high level of adaptability to changing technological environments.

Hacktivist threats are ideologically motivated and involve unauthorized digital actions aimed at promoting political agendas or social causes. Unlike nation-state actors, hacktivists operate independently or in loosely affiliated collectives, such as Anonymous. Their methods often include website defacements, data leaks, or distributed denial-of-service (DDoS) attacks aimed at drawing attention to specific issues. Although hacktivist actions may not always cause lasting damage, they can be disruptive and embarrassing to targets, including governments and corporations[1].

Insider threats involve individuals within an organization—such as employees, contractors, or business partners—who exploit their access to data or systems to cause harm. These threats can be either malicious, where the insider intends to damage or steal information, or negligent, resulting from careless or poorly trained employees. Edward Snowden's disclosure of classified NSA documents represents a significant insider threat that had broad national security implications[2]. This category is particularly challenging to detect because insiders often operate with legitimate access credentials.

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. APTs are commonly associated with nation-state actors but may also involve highly organized cybercriminal groups. The objective is often data exfiltration, surveillance, or sabotage. APTs utilize sophisticated techniques such as spear-phishing, zero-day vulnerabilities, and lateral movement across systems. APT1, attributed to

[1] [1] Gabriella Coleman, Hacker, Hoaxer, Whistleblower, Spy.
[2] Gellman, Barton, and Laura Poitras. "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program." The Washington Post, June 6, 2013. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06

China's People's Liberation Army Unit 61398, is a notable example of such activity targeting U.S. corporations and government entities[1].

Each category of cyber threat poses distinct challenges to cybersecurity professionals. A nuanced understanding of their characteristics and motivations is essential for developing effective defenses, crafting relevant policies, and fostering international cooperation in the digital domain.

1.4 Cyber Threat Actors: States, Groups, and Individuals

Cyber threat actors encompass a broad range of entities—states, organized groups, and individuals—each with varying motivations, capabilities, and methods. Understanding the profiles and behaviors of these actors is essential for developing effective cybersecurity policies and response strategies.

State-sponsored threat actors are among the most sophisticated and well-resourced. These actors operate under the directives of national governments and are often motivated by geopolitical objectives such as espionage, disruption of critical infrastructure, and strategic advantage. For example, Russia's APT29 (also known as "Cozy Bear") and China's APT10 have been linked to numerous cyber espionage campaigns against governmental and private sector targets worldwide[2]. These groups employ advanced persistent threats (APTs), leveraging zero-day vulnerabilities, customized malware, and long-term infiltration strategies to steal sensitive data or destabilize systems. State actors often use cyber tools as part of broader hybrid warfare tactics, blurring the lines between peace and conflict.

Cybercriminal organizations operate with profit as their primary goal. These actors can range from loosely affiliated hackers to highly structured international syndicates. Ransomware-as-a-Service (RaaS) models have enabled the commodification of cybercrime, lowering the technical barrier for entry and increasing the frequency of attacks.

[1] Mandiant. APT1: Exposing One of China's Cyber Espionage Units. Mandiant Intelligence Center Report, 2013. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
[2] Thomas Rid, *Cyber War Will Not Take Place.*

Groups such as REvil and Conti have targeted hospitals, municipalities, and corporations, demanding cryptocurrency ransoms in exchange for data decryption[1]. Unlike state actors, these groups prioritize financial gain over political or strategic outcomes, though some may collaborate with state entities when interests align.

Hacktivist groups engage in cyber operations to advance ideological, political, or social causes. They are typically decentralized and operate under collective banners such as Anonymous or LulzSec. Hacktivist activities include website defacements, data leaks, and denial-of-service attacks, aiming to raise awareness or retaliate against perceived injustices. While less technically advanced than nation-state actors, hacktivists can cause reputational and operational damage to their targets[2]. Their motivations often intersect with civil disobedience and protest, creating legal and ethical ambiguities.

Insider threats come from individuals within an organization who have authorized access to sensitive systems and data. These actors can be either malicious—intentionally leaking or sabotaging information—or negligent, resulting in accidental data breaches. The 2013 disclosures by Edward Snowden, a former NSA contractor, exemplify how insiders can expose vast amounts of classified data[3]. Insider threats are particularly challenging to mitigate because they exploit legitimate credentials and bypass traditional perimeter defenses.

Individual hackers can act independently or as part of broader communities. Their motivations vary widely—from curiosity and notoriety to personal grievances or financial gain. While some "black hat" hackers engage in illegal activities, others may be "white hat" or "gray hat" hackers who help identify vulnerabilities without malicious intent. The line between ethical and criminal behavior in this space can be blurred, especially when legal protections for ethical hacking are unclear.

[1] Greenberg, Sandworm.
[2] Gabriella Coleman, Hacker, Hoaxer, Whistleblower, Spy.
[3] Gellman, Barton. Dark Mirror: Edward Snowden and the American Surveillance State. Penguin Press, 2020.

Script kiddies represent a subset of individual actors who use pre-existing tools or scripts to carry out attacks, often without fully understanding the underlying code. Though typically less skilled, they can still cause disruption, particularly when targeting poorly secured systems[1].

Cyber threat actors continue to evolve, exploiting technological advances and global interconnectivity. Differentiating between these actors based on intent, capability, and affiliation is critical for attribution and response in the cybersecurity domain.

1.5 Cyber Threat Vectors and Techniques

Cyber threat vectors and techniques refer to the methods and pathways used by malicious actors to infiltrate, disrupt, damage, or exploit digital systems and data. As the threat landscape evolves, attackers adopt increasingly sophisticated tools and tactics to bypass security mechanisms and achieve their objectives. Understanding these vectors is vital for building resilient cybersecurity frameworks.

One of the most common and damaging cyber threat techniques is **malware**, a general term for malicious software designed to harm or exploit systems. Malware includes viruses, worms, Trojans, ransomware, spyware, and rootkits. For instance, ransomware encrypts victims' data and demands payment for decryption keys, with high-profile cases such as WannaCry (2017) affecting hospitals and companies worldwide[2]. Trojans masquerade as legitimate software to trick users into installing them, granting attackers backdoor access to systems.

Phishing is another prevalent vector, involving deceptive emails or messages that lure users into divulging sensitive information or downloading malicious attachments. Advanced phishing techniques, such as **spear phishing**, are highly targeted, often customized using social engineering to increase their success rate. These attacks are

[1] Skoudis, Ed, and Tom Liston. Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses. Prentice Hall, 2006.
[2] Andy Greenberg, *Sandworm* (2019).

frequently the initial step in larger campaigns, including credential theft and espionage[1].

Denial-of-Service (DoS) and **Distributed Denial-of-Service (DDoS)** attacks are used to overwhelm systems, networks, or services, rendering them unavailable to users. DDoS attacks employ multiple compromised systems—often part of a botnet—to generate massive volumes of traffic. These attacks can disrupt essential services, as seen in the 2016 Mirai botnet attack, which targeted DNS provider Dyn and affected major websites like Twitter and Netflix[2].

Zero-day exploits are attacks that leverage previously unknown vulnerabilities in software or hardware. Because vendors have no prior knowledge of the flaw, there are no patches or fixes at the time of the attack, making zero-days extremely dangerous. Nation-state actors often use zero-days in advanced persistent threats (APTs) to conduct long-term, stealthy operations[3].

Insider threats occur when individuals within an organization abuse their access for malicious purposes or through negligence. This vector is particularly challenging because insiders typically bypass perimeter defenses. For example, Edward Snowden's unauthorized disclosure of classified information from the NSA illustrates how insiders can pose national security risks[4].

Man-in-the-middle (MITM) attacks occur when an attacker intercepts communication between two parties to steal or manipulate data. These attacks often exploit unsecured networks, such as public Wi-Fi, and may involve tactics like session hijacking or SSL stripping.

SQL injection is a technique used to exploit vulnerabilities in web applications by inserting malicious SQL code into query fields. If

[1] Hadnagy, Christopher. Social Engineering: The Science of Human Hacking. Wiley, 2018.
[2] Krebs, Brian. "KrebsOnSecurity Hit with Record DDoS." Krebs on Security, September 21, 2016. https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/.
[3] Kim Zetter, *Countdown to Zero Day* (2014).
[4] Gellman, *Dark Mirror*.

successful, attackers can access or manipulate databases, potentially retrieving sensitive information like user credentials or payment data[1].

Supply chain attacks target third-party software or service providers to compromise their clients. The SolarWinds attack in 2020 demonstrated the dangers of this vector, as attackers inserted malicious code into a legitimate software update, granting them access to U.S. government agencies and major corporations[2].

Credential stuffing involves the use of automated tools to try stolen usernames and passwords from one breach across multiple sites. This technique capitalizes on users' tendency to reuse credentials across platforms, making it effective even with basic tools.

Social engineering underpins many of these vectors, as it manipulates human psychology to bypass technical defenses. Whether through phishing, pretexting, or baiting, these methods rely on trust, fear, or urgency to prompt user action.

Together, these vectors and techniques represent a dynamic and growing array of threats in the cyber domain. Effective defense strategies require not only technological solutions but also user awareness and continuous adaptation to emerging tactics.

1.6 Ethical and Human Rights Implications of Cyber Threats

Cyber threats not only jeopardize data and systems but also raise serious ethical and human rights concerns. As cyberspace becomes increasingly entangled with all aspects of modern life—communication, governance, finance, and national security—the ethical dimensions of cyber operations and their potential to violate fundamental rights demand critical attention.

One of the primary human rights at risk in the cyber domain is the **right to privacy**, enshrined in Article 17 of the *International Covenant*

[1] Halfond, William G. J., Jeremy Viegas, and Alessandro Orso. "A Classification of SQL Injection Attacks and Countermeasures." In Proceedings of the IEEE International Symposium on Secure Software Engineering, 2006.
[2] Sanger, David E., Nicole Perlroth, and Julian E. Barnes. "As Understanding of Russian Hacking Grows, So Does Alarm." The New York Times, December 20, 2020. https://www.nytimes.com/2020/12/20/us/politics/russian-hacking-government.html.

on Civil and Political Rights (ICCPR). Cyber surveillance technologies—often justified as national security tools—can infringe upon individuals' right to be free from arbitrary or unlawful interference in their private lives[1]. The deployment of spyware, such as the Israeli NSO Group's Pegasus software, exemplifies this threat. Investigations revealed that Pegasus was used to monitor journalists, human rights defenders, and political dissidents across multiple countries, raising alarms about the unchecked use of cyber tools by state and non-state actors[2].

Closely related is the issue of **mass surveillance**, as exposed by whistleblowers such as Edward Snowden in 2013. The revelation of widespread monitoring by the U.S. National Security Agency (NSA) and its allies under programs like PRISM sparked global debates on the balance between national security and individual freedoms[3]. The lack of transparency and accountability mechanisms in such surveillance programs underscores the ethical tensions in cyberspace governance.

Freedom of expression, another core right, is also at risk. Governments and corporations may restrict online content, filter information, or shut down internet access altogether. For example, during political unrest, regimes in Myanmar, Iran, and Sudan have implemented **internet shutdowns**, denying entire populations access to information and communication tools[4]. These measures often aim to suppress dissent and are in direct violation of Article 19 of the ICCPR, which guarantees the right to seek, receive, and impart information and ideas of all kinds[5].

The ethical implications of **cyberattacks on critical infrastructure** are equally troubling. Attacks on hospitals, power grids, and water systems—especially during armed conflicts—may violate international

[1] United Nations. International Covenant on Civil and Political Rights, 1966. Article 17.
[2] Amnesty International. "Forensic Methodology Report: How to Catch Pegasus." July 18, 2021. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-pegasus/.
[3] Gellman, *Dark Mirror*.
[4] Access Now. "The Return of Digital Authoritarianism: Internet Shutdowns in 2022." March 2023. https://www.accessnow.org/keepiton-report-2022/.
[5] United Nations. International Covenant on Civil and Political Rights, 1966. Article 19.

humanitarian law principles such as distinction and proportionality. The 2017 WannaCry ransomware attack severely impacted the UK's National Health Service, delaying surgeries and threatening lives[1]. When civilian life is endangered through cyber means, it raises both legal and moral red flags.

Algorithmic bias and digital discrimination present further concerns. AI systems used for security screening, facial recognition, or predictive policing may reflect and amplify societal prejudices if trained on biased data. This creates unequal treatment and violates the principle of non-discrimination embedded in international human rights law[2].

Moreover, the **ethical responsibilities of corporations** in safeguarding user data are frequently questioned. Data breaches at companies like Facebook (now Meta) and Equifax exposed millions of users' personal information due to poor cybersecurity practices or opaque data-sharing policies. These incidents not only erode trust but also violate data protection principles enshrined in regulations like the **EU General Data Protection Regulation (GDPR)**[3].

Lastly, the **weaponization of disinformation**, especially during elections and pandemics, has profound implications for democratic processes and public health. State-sponsored and automated campaigns manipulate public discourse, spreading falsehoods that influence political outcomes or hinder vaccine acceptance[4]. Combating such threats raises complex ethical questions about content moderation, censorship, and the line between free speech and harmful misinformation.

In sum, cyber threats are not only technical and security challenges but also raise profound questions of ethics and human dignity. Legal

[1] Andy Greenberg, *Sandworm* (2019).
[2] Eubanks, Virginia. Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. St. Martin's Press, 2018.
[3] European Parliament and Council. General Data Protection Regulation, Regulation (EU) 2016/679
[4] Wardle, Claire, and Hossein Derakhshan. "Information Disorder: Toward an Interdisciplinary Framework." Council of Europe Report DGI(2017)09, September 2017. https://rm.coe.int/information-disorder-report/1680764666.

systems, technology developers, and civil society must work together to ensure that cyberspace remains a domain where rights are respected and protected.

2. The impact of cyber threats on international security

2.1 Models of Cyber Threats (Iran, USA, Russia)

Cyber threat models vary significantly based on national strategies, capabilities, and geopolitical interests. Countries like Iran, the United States, and Russia exhibit distinct patterns in how they develop, deploy, and justify their cyber operations. Each model reflects their technological capacity, security doctrines, and strategic objectives in the global cyber domain.

The **Iranian cyber threat model** is characterized by asymmetric warfare tactics and strong reliance on proxy hacking groups. Lacking the advanced technological infrastructure of Western nations, Iran leverages cyber capabilities to compensate for conventional military limitations and exert regional influence. Iranian threat actors such as APT33, APT34 (OilRig), and APT35 (Charming Kitten) have conducted operations targeting critical infrastructure, government institutions, and private companies, particularly in the Middle East and North America[1]. These groups often use spear-phishing and credential-harvesting techniques, aiming to steal sensitive information or disrupt operations. For instance, APT33 is linked to attacks on Saudi Arabian energy firms, reflecting Iran's strategic focus on destabilizing regional rivals[2]. Iran also uses cyber tools for internal repression and censorship, targeting dissidents and activists both domestically and abroad[3].

In contrast, the **United States' cyber threat model** is rooted in advanced technological capability, legal frameworks, and a global security outlook. The U.S. Department of Defense views cyberspace as a warfighting domain, as articulated in the 2018 DoD Cyber Strategy[173].

[1] FireEye. "APT33: Cyber Espionage Group Linked to Iran." September 2017. https://www.fireeye.com/blog/threat-research/2017/09/apt33-cyber-espionage-group.html
[2] Sanger, David E. The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age. Crown Publishing, 2018.
[3] Freedom House. "Iran." Freedom on the Net 2022. https://freedomhouse.org/country/iran/freedom-net/2022

American cyber operations range from defensive measures to proactive "hunt forward" missions, where cyber teams deploy in allied nations to counter adversary malware in real-time. The United States Cyber Command (USCYBERCOM) exemplifies the operationalization of cyber power, as seen in the deployment of persistent engagement strategies against actors such as ISIS and Russian state-sponsored groups[1]. A high-profile example of U.S. offensive cyber capability is **Stuxnet**, a joint U.S.-Israeli operation that sabotaged Iran's nuclear centrifuges in 2010—widely recognized as the first known use of a cyberweapon to cause physical damage[2].

The **Russian model of cyber threats** is deeply integrated into the country's broader information warfare doctrine. Unlike the United States' open strategy or Iran's reactive posture, Russia employs cyber operations as part of a larger hybrid warfare strategy that combines hacking with disinformation, political interference, and psychological operations. Russian threat actors such as APT28 (Fancy Bear) and APT29 (Cozy Bear), believed to be affiliated with the GRU and FSB, respectively, have been implicated in high-profile cyberattacks, including the 2016 U.S. election interference and the SolarWinds supply chain attack[3]. Russia uses its cyber capabilities to undermine democratic institutions, exploit social divisions, and weaken NATO cohesion. Moreover, its activities in Ukraine—both before and during the ongoing war—illustrate the offensive use of cyber tools to disrupt critical infrastructure, media, and military systems[4].

Each country's model reflects its national priorities and strategic culture. Iran adopts cyber operations as tools of survival and deterrence. The United States treats cyberspace as a critical domain of military superiority and collective security. Russia weaponizes information and cyber tools to challenge Western norms, amplify authoritarian influence,

[1] U.S. Cyber Command. "Persistent Engagement." https://www.cybercom.mil/About/Persistent-Engagement/
[2] Kim Zetter, *Countdown to Zero Day* (2014).
[3] Office of the Director of National Intelligence. Foreign Threats to the 2020 U.S. Federal Elections. March 2021. https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf
[4] Center for Strategic and International Studies. "Significant Cyber Incidents." Updated 2024. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

and pursue regional ambitions. Understanding these models is essential for crafting effective international cybersecurity policies and anticipating state-sponsored cyber threats.

2.2 Case Studies of Major Cyber Conflicts or Incidents

The evolving landscape of cyber conflict has been shaped by a series of landmark incidents that demonstrate the destructive potential of cyber capabilities. These case studies—Stuxnet, the 2007 cyberattacks on Estonia, the NotPetya malware campaign, and the SolarWinds breach—illustrate different motivations, techniques, and geopolitical implications of cyber operations.

One of the earliest and most impactful cyber weapons was **Stuxnet**, a highly sophisticated malware discovered in 2010. It is widely attributed to a joint effort by the United States and Israel targeting Iran's nuclear enrichment facilities at Natanz[1]. Unlike traditional cyberattacks, Stuxnet was designed to cause physical destruction by sabotaging industrial control systems. The worm exploited multiple zero-day vulnerabilities in Microsoft Windows and spread via USB drives to reach air-gapped systems. Once inside the targeted network, it altered the speeds of centrifuges used for uranium enrichment, causing them to degrade over time while reporting normal operations to monitoring systems[2]. Stuxnet marked a pivotal moment in cyber warfare, demonstrating that cyber tools could be used to deliver precise, kinetic effects without launching a conventional military attack.

In contrast to Stuxnet's targeted and covert nature, the **2007 cyberattacks on Estonia** represented a broader, politically motivated disruption campaign. Following a diplomatic dispute with Russia over the relocation of a Soviet-era war memorial, Estonia experienced a wave of distributed denial-of-service (DDoS) attacks that crippled government websites, financial institutions, media outlets, and telecommunications

[1] Sanger, David E. Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power. New York: Crown, 2012.
[2] Kim Zetter, *Countdown to Zero Day* (2014).

services[1]. Although the attackers were never conclusively identified, the scale and coordination of the attacks pointed to the involvement or support of Russian actors. Estonia, one of the most digitally integrated countries in Europe, faced significant disruption, prompting NATO and the EU to recognize the need for collective cybersecurity strategies[2]. This incident was a watershed for international security communities, catalyzing the establishment of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn.

Another major cyber conflict with global ramifications was the **NotPetya malware attack** in 2017. Initially targeting Ukrainian organizations through a compromised tax software update, the malware spread rapidly across international networks, affecting companies such as Maersk, Merck, FedEx, and many others[3]. Though masquerading as ransomware, NotPetya was in fact a destructive wiper, rendering systems unusable and causing an estimated $10 billion in damages[4]. The attack was attributed to the Russian military intelligence agency GRU and viewed as part of ongoing Russian aggression against Ukraine following the annexation of Crimea[5]. NotPetya demonstrated how cyber operations intended for regional disruption could have far-reaching and indiscriminate consequences, especially when they exploit widely used software platforms.

Most recently, the **SolarWinds supply chain attack**, discovered in late 2020, exemplified a long-term cyber espionage operation that compromised U.S. federal agencies and private sector entities. The attackers inserted malicious code into a routine software update for the Orion network management platform, used by over 18,000

[1] Tikk, Eneken, Kadri Kaska, and Liis Vihul. International Cyber Incidents: Legal Considerations. Tallinn: NATO CCDCOE, 2010.
[2] NATO CCDCOE. “About Us.” https://ccdcoe.org/about-us/
[3] Greenberg, Andy. “The Untold Story of NotPetya, the Most Devastating Cyberattack in History.” Wired, August 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[4] Office of the Director of National Intelligence. Annual Threat Assessment of the U.S. Intelligence Community, April 2021. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf
[5] U.K. Foreign, Commonwealth & Development Office. “Russia: UK condemns GRU over NotPetya cyber-attack.” February 2018. https://www.gov.uk/government/news/russia-uk-condemns-gru-over-notpetya-cyber-attack

organizations[1]. This allowed the attackers—believed to be Russian intelligence—to gain persistent access to sensitive networks and exfiltrate data without detection for months. What set SolarWinds apart was the sophistication of the supply chain compromise, the scale of infiltration, and the stealth with which the attackers operated[2]. It raised serious concerns about software trust, vulnerability disclosure, and the cybersecurity of government contractors.

These case studies illustrate the breadth of cyber conflict: from the militarized precision of Stuxnet and the politically driven DDoS campaign in Estonia to the economically devastating NotPetya attack and the covert surveillance of SolarWinds. Each incident contributed to shaping international discourse on cyber norms, deterrence, and collective security. They underscore the strategic value of cyber capabilities and the urgent need for robust international cooperation and resilience-building to confront future threats.

2.3 The Impact of Cyber Threats on Political Stability and International Relations

Cyber threats have significantly reshaped the geopolitical landscape, undermining political stability and complicating international relations. These threats—ranging from cyber espionage and election interference to large-scale infrastructure attacks—have blurred the lines between war and peace, challenging traditional understandings of sovereignty and conflict. Governments worldwide increasingly recognize cyberspace as a critical arena for strategic competition, with cyber incidents often acting as flashpoints for diplomatic tensions and security concerns.

One of the most direct impacts of cyber threats on political stability is their role in undermining democratic processes. State-sponsored cyber operations targeting elections are among the most visible and disruptive

[1] U.S. Cybersecurity and Infrastructure Security Agency (CISA). “Emergency Directive 21-01.” December 2020. https://cyber.dhs.gov/ed/21-01/

[2] Sanger, David E., Nicole Perlroth, and Julian E. Barnes. “As Understanding of Russian Hacking Grows, So Does Alarm.” New York Times, January 2021. https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html

forms of interference. A prominent example is the 2016 U.S. presidential election, during which Russian state-affiliated actors conducted widespread disinformation campaigns, hacked into political party servers, and leaked sensitive information[1]. These efforts, attributed to groups like APT28 (Fancy Bear), sought to erode trust in democratic institutions, polarize public discourse, and influence electoral outcomes. Similar tactics have been observed in European countries, including Germany and France, where cyber operations have targeted politicians, parties, and media outlets[2]. Such actions not only destabilize domestic politics but also create long-term challenges to electoral integrity and public confidence in governance.

Cyber threats also disrupt international relations by increasing mistrust and complicating diplomatic engagement. When attribution of cyberattacks is difficult or disputed, states may resort to unilateral accusations and retaliatory measures, exacerbating geopolitical rivalries. For instance, the 2020 SolarWinds cyber espionage campaign, which compromised multiple U.S. government agencies and private firms, was widely attributed to Russian intelligence services[3]. Although the operation appeared to be espionage rather than sabotage, its scale and sophistication prompted widespread concern and led to U.S. sanctions and diplomatic expulsions[4]. These responses deepened tensions between Washington and Moscow, showcasing how cyber operations can provoke real-world geopolitical consequences even without physical violence.

Similarly, Chinese cyber activities—particularly those aimed at intellectual property theft and economic espionage—have strained

[1] Office of the Director of National Intelligence. Assessing Russian Activities and Intentions in Recent U.S. Elections. January 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf
[2] European Commission. "Tackling Online Disinformation." 2021. https://digital-strategy.ec.europa.eu/en/policies/online-disinformation
[3] Sanger, David E., Nicole Perlroth, and Julian E. Barnes. "Russian Hackers Broke Into Federal Agencies." New York Times, December 13, 2020. https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html
[4] U.S. Department of State. "Russia Sanctions." April 15, 2021. https://www.state.gov/russia-sanctions/
191 FireEye. "APT10: Operation Cloud Hopper." April 2017. https://www.fireeye.com/blog/threat-research/2017/04/operation-cloud-hopper.html

relations with the United States and other Western nations. Operations attributed to Chinese groups such as APT10 (Cloud Hopper) have targeted managed service providers and multinational corporations, facilitating long-term access to valuable proprietary information[1]. The U.S. Department of Justice has indicted several Chinese hackers in connection with these operations, framing them as violations of international norms and a threat to fair economic competition[2]. These actions not only disrupt economic relations but also challenge the prospects for international cyber norms and cooperation.

Beyond bilateral disputes, cyber threats affect collective security arrangements and multilateral diplomacy. NATO, for example, has recognized cyberattacks as potential triggers for Article 5 collective defense commitments, thereby incorporating cyber defense into its strategic framework[3]. However, differing national cyber capabilities and threat perceptions among member states complicate coordinated responses. The European Union, likewise, has adopted cyber diplomacy tools—including attribution frameworks and sanctions regimes—to address malicious cyber behavior, yet internal divisions over attribution and proportionality persist[4].

Moreover, cyber threats often intersect with broader geopolitical crises, further destabilizing fragile regions or exacerbating existing conflicts. In Ukraine, Russian cyber operations have accompanied kinetic military aggression, targeting power grids, government agencies, and communication networks[5]. These attacks aim to weaken Ukraine's ability to resist militarily while signaling Russia's technological reach and intent. Such hybrid warfare strategies highlight how cyber capabilities can serve as force multipliers in conventional conflicts, altering the dynamics of war and deterrence.

[1] OSCE CBMs 2016.
[2] U.S. Department of Justice. "Two Chinese Hackers Associated With the Ministry of State Security Charged." December 20, 2018. https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion
[3] NATO. "Cyber Defence." March 2024. https://www.nato.int/cps/en/natohq/topics_78170.htm
[4] Council of the European Union. "EU Cyber Diplomacy Toolbox." https://www.consilium.europa.eu/en/policies/cybersecurity/
[5] Andy Greenberg, *Sandworm* (2019).

Efforts to build international norms and agreements around responsible state behavior in cyberspace remain ongoing but fragile. The United Nations' Open-Ended Working Group and the Group of Governmental Experts have made some progress in identifying voluntary norms, such as protecting critical infrastructure and refraining from cyberattacks on civilian targets[1]. However, enforcement remains elusive, and divergent views among major powers impede the development of binding international law in cyberspace.

In sum, cyber threats have profound and multifaceted impacts on political stability and international relations. They weaken democratic institutions, intensify geopolitical rivalries, and complicate international law and diplomacy. As states continue to invest in cyber capabilities, the risk of escalation, miscalculation, and broader destabilization remains high, underscoring the need for robust cyber governance mechanisms and renewed diplomatic engagement.

2.4 Responses and Countermeasures to Cyber Threats

As cyber threats grow in scale, complexity, and geopolitical relevance, states, international organizations, and private actors have developed a range of responses and countermeasures. These efforts encompass legal frameworks, military doctrines, cybersecurity strategies, multilateral cooperation, and public-private partnerships. Although the global community still lacks a unified approach to governing cyberspace, significant initiatives have emerged to bolster resilience and deter adversaries.

One of the earliest formal responses came from the military sector. The United States established **U.S. Cyber Command (USCYBERCOM)** in 2009 as a unified command responsible for defending military networks and conducting offensive cyber operations when authorized[2]. In 2018, the Department of Defense adopted a new cyber strategy emphasizing "defend forward" and "persistent

[1] United Nations. "Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security." https://www.un.org/disarmament/open-ended-working-group/

[2] U.S. Cyber Command. "About." https://www.cybercom.mil/About/

engagement," allowing the U.S. to disrupt malicious cyber activities at their source, even before they reach American systems[1]. Other countries followed suit: Russia's military doctrine incorporates cyber warfare as a key strategic tool, while China's Strategic Support Force (PLASSF) oversees cyber, electronic, and space operations[2].

Beyond national military responses, governments have implemented comprehensive cybersecurity strategies. The **European Union**, for example, developed the **EU Cybersecurity Strategy** and the **NIS Directive** (Directive on Security of Network and Information Systems) to enhance the cybersecurity capabilities of member states and ensure coordination[3]. In 2020, the EU proposed the **Cybersecurity Act**, which granted the EU Agency for Cybersecurity (ENISA) a permanent mandate and established a cybersecurity certification framework for digital products[4].

International cooperation has also grown through initiatives like the **Budapest Convention on Cybercrime** (2001), the first binding international treaty to address Internet and computer crime by harmonizing national laws and fostering cross-border collaboration[5]. Despite its success, major powers like Russia and China have criticized it for being Western-centric and have proposed alternatives, including a new cybercrime convention under the United Nations framework.

NATO has acknowledged cyberspace as a domain of operations since 2016, pledging to defend allies in the event of a significant cyberattack under Article 5 of its founding treaty[6]. The **NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)** in Tallinn plays a crucial role in research, training, and simulations like the

[1] U.S. Department of Defense, Summary of the Department of Defense Cyber Strategy
[2] Heginbotham, Eric, et al. China's Evolving Nuclear Deterrent. RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1040.html
[3] European Commission. "Cybersecurity Strategy of the European Union." https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy
[4] European Union Agency for Cybersecurity (ENISA). "Cybersecurity Act." https://www.enisa.europa.eu/topics/csirt-cert-services/cybersecurity-act
[5] Council of Europe. "Convention on Cybercrime." https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
[6] NATO, "Cyber Defence."

annual "Locked Shields" cyber defense exercise. NATO's collective approach has strengthened the capacity of member states to respond to state-sponsored cyber threats.

The **private sector** also plays a central role. Technology companies like Microsoft, Google, and CrowdStrike provide frontline defense against cyber threats, often detecting and disclosing major breaches. Microsoft's **Digital Crimes Unit** and **Cyber Defense Operations Center** collaborate with law enforcement agencies worldwide to combat cybercrime and nation-state threats[1]. In 2017, Microsoft proposed the **"Digital Geneva Convention"**, advocating international norms to protect civilians from cyberattacks and restrict the development of cyber weapons[2].

Public-private partnerships are increasingly essential. For example, the U.S. **Cybersecurity and Infrastructure Security Agency (CISA)** works closely with private industry to secure critical infrastructure. CISA's **Cyber Information Sharing and Collaboration Program (CISCP)** enables real-time threat intelligence sharing between the government and private stakeholders[3].

Another key countermeasure is **cyber diplomacy**. Countries have participated in the United Nations' **Group of Governmental Experts (GGE)** and the **Open-Ended Working Group (OEWG)** on developments in the field of information and telecommunications in the context of international security. These bodies have produced consensus reports recognizing that international law, including the UN Charter, applies to cyberspace and affirming the importance of voluntary norms[4].

norms[4].

Despite these measures, challenges persist. Disparities in capacity between developed and developing countries, the lack of consensus on

[1] Microsoft. "Cyber Defense Operations Center." https://www.microsoft.com/en-us/security/business/cyberdefense
[2] Microsoft Blog, *Digital Geneva Convention.*
[3] Cybersecurity and Infrastructure Security Agency (CISA). "Cyber Information Sharing and Collaboration Program (CISCP)." https://www.cisa.gov/cyber-information-sharing-collaboration-program
[4] United Nations. Reports of the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security. https://www.un.org/disarmament/ict-security/

cyber norms, attribution difficulties, and conflicting views on sovereignty in cyberspace hinder progress. Nonetheless, responses to cyber threats continue to evolve, with increasing recognition that multi-layered, multistakeholder approaches are essential for global cyber stability.

2.5 Cyber Deterrence and Attribution

In the realm of international security, cyber deterrence and attribution stand as two of the most complex and controversial challenges. Deterrence—the ability to prevent an adversary from taking an undesired action through the threat of retaliation or denial—and attribution—the ability to identify the perpetrator of a cyberattack with confidence—are foundational concepts in conventional security strategies. Yet in cyberspace, these concepts are far harder to implement due to the technical and political nature of digital operations. Despite their difficulties, both deterrence and attribution are critical to building a credible international cyber security architecture.

Cyber deterrence borrows from traditional theories of nuclear and military deterrence but must be adapted to the unique attributes of cyberspace: the low cost of entry, anonymity, proliferation of actors, and blurred lines between peace and conflict. Cyber deterrence typically takes three main forms: **deterrence by denial**, **deterrence by punishment**, and **norm-based deterrence**[1]. Deterrence by denial involves hardening systems and improving cyber resilience to make attacks ineffective. This includes adopting robust cybersecurity measures, patching vulnerabilities, conducting regular audits, and segmenting networks to reduce damage in the event of a breach.

Deterrence by punishment involves the threat or implementation of retaliatory actions—either in cyberspace or through other means—against those who perpetrate cyberattacks. For instance, the United States has stated in several defense and cybersecurity strategies that it reserves the right to respond to cyberattacks using conventional military

[1] Joseph S. Nye Jr., *Deterrence and Dissuasion in Cyberspace*, 44–71. https://doi.org/10.1162/ISEC_a_00266

force if necessary[1]. In 2020, the U.S. Department of Justice indicted members of the Russian military intelligence agency GRU for their role in global cyberattacks such as NotPetya and attacks on the 2018 Winter Olympics, demonstrating a form of legal and diplomatic punishment[2].

However, for punishment to work as a deterrent, **credible attribution** is essential. Unlike conventional attacks, cyber operations can be routed through numerous global servers, anonymized using encryption, or carried out via proxy actors, making it difficult to trace their origin definitively. Attribution in cyberspace involves technical forensics—such as malware signatures, IP traces, time zones, language usage in code—as well as **intelligence gathering**, including human sources, intercepted communications, and satellite data[3]. Attribution is rarely based on a single indicator but on a mosaic of evidence, often termed "confidence levels."

The difficulties in attribution have led to the development of **attribution frameworks** and cooperative mechanisms. The United States, the United Kingdom, and allied countries often **publicly attribute** major cyberattacks to state actors, as seen in the coordinated attributions of the SolarWinds and WannaCry attacks to Russia and North Korea, respectively[4]. These attributions are part of a broader **naming-and-shaming strategy** meant to isolate the perpetrators diplomatically and signal resolve.

Still, public attribution carries risks. If states incorrectly assign blame or act without conclusive evidence, they risk escalating conflicts or damaging diplomatic relations. As a result, some countries prefer to **keep attribution classified** or respond covertly through counter-cyber operations, sanctions, or economic measures.

[1] U.S. Department of Defense, Summary of the Department of Defense Cyber Strategy.

[2] U.S. Department of Justice. "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware." October 19, 2020. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

[3] Rid, Thomas, and Ben Buchanan. "Attributing Cyber Attacks." Journal of Strategic Studies 38, nos. 1–2 (2015): 4–37. https://doi.org/10.1080/01402390.2014.977382

[4] UK Foreign, Commonwealth & Development Office. "UK Blames Russia for SolarWinds Attack." April 2021. https://www.gov.uk/government/news/uk-blames-russia-for-solarwinds-attack

International cooperation plays a key role in improving attribution. Organizations such as **NATO**, the **European Union**, and the **Five Eyes intelligence alliance** have developed **cyber threat intelligence sharing platforms** to enhance joint attribution capabilities[1]. The **Paris Call for Trust and Security in Cyberspace**, supported by over 1,200 entities including governments and tech companies, also promotes transparency and responsible behavior in attribution processes[2].

Cyber deterrence is further complicated by **non-state actors** who may not be deterred by traditional means. Hacktivist groups, criminal syndicates, and proxies may act for ideological, financial, or personal motives and may not fear conventional retaliation. In such cases, **law enforcement cooperation**, cybercrime treaties like the **Budapest Convention**, and targeted financial sanctions become more effective deterrence mechanisms[3].

Another emerging area is **cyber signaling**—sending clear and credible messages about a state's cyber capabilities and willingness to act. For example, in 2018, the U.S. Cyber Command publicly announced its strategy of "persistent engagement," and reports emerged of cyber operations against Iran and Russia intended to signal deterrent intent[4]. Likewise, offensive cyber exercises and controlled disclosures of cyber capabilities serve as indirect methods of deterrence, mirroring the concept of military drills during the Cold War.

The theoretical foundation for cyber deterrence remains contested. Some scholars argue that cyber deterrence is inherently weak due to the **asymmetry** of capabilities and low entry barriers, while others assert that it can work if supported by strong **norms**, credible attribution, and multilateral cooperation[5]. Deterrence must also be adapted for **gray zone**

[1] NATO, "Cyber Defence."
[2] French Ministry for Europe and Foreign Affairs. "Paris Call for Trust and Security in Cyberspace." https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/paris-call-for-trust-and-security-in-cyberspace/
[3] Council of Europe, "Budapest Convention on Cybercrime."
[4] David E. Sanger, *The Perfect Weapon.*
[5] Gartzke, Erik, and Jon R. Lindsay. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." Security Studies 24, no. 2 (2015): 316–348. https://doi.org/10.1080/09636412.2015.1038188.

conflict, where cyber operations fall below the threshold of war but still aim to weaken adversaries.

In conclusion, cyber deterrence and attribution are pivotal yet fragile pillars of international cybersecurity. As cyber threats increase in frequency and sophistication, advancing attribution capabilities and refining deterrent strategies—through resilience, threat of retaliation, and norm enforcement—remain vital for preserving global security and preventing escalation.

Chapter Two
International Legal Framework for Cyberspace

Chapter Two: International Legal Framework for Cyberspace

As cyberspace becomes increasingly integral to national security, economic stability, and societal cohesion, the demand for a coherent international legal framework to regulate state behavior in this domain has grown significantly. However, unlike traditional domains such as land, sea, and air, cyberspace remains legally ambiguous and politically contested. While international law—particularly the UN Charter, the law of armed conflict, and international human rights law—is widely acknowledged as applicable to cyberspace, its interpretation and enforcement in the digital realm remain subject to debate and fragmentation. In this evolving context, multilateral institutions, regional organizations, and informal coalitions have taken diverse approaches to norm development and legal interpretation in cyberspace governance.

Section One of this chapter explores the role of the **United Nations and regional organizations** in shaping the foundational principles of international cybersecurity. The UN, primarily through its **Group of Governmental Experts (GGE)** and **Open-Ended Working Group (OEWG)**, has fostered consensus on key normative principles such as the applicability of international law, respect for state sovereignty, and the prohibition of coercive intervention in the cyber domain.[1] These forums have also promoted voluntary, non-binding norms and confidence-building measures, often endorsed by the UN General Assembly.[2] In parallel,

[1] United Nations GA Report, *A/70/174 (2015)*, https://undocs.org/A/70/174.
[2] United Nations General Assembly, Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, A/75/816 (2021),

regional organizations such as the **Organization for Security and Co-operation in Europe (OSCE)**, the **European Union (EU)**, the **African Union (AU)**, and the **Organization of American States (OAS)** have translated these norms into region-specific instruments and operational mechanisms, contributing to a multi-layered governance model.[1] These initiatives reflect both the UN's global mandate and the importance of localized implementation through regional bodies.

Section Two shifts focus to the development of **alternative normative frameworks** outside the formal structures of the United Nations. These include influential interpretative efforts such as the **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**,[2] as well as **state-driven declarations** like the **Paris Call for Trust and Security in Cyberspace (2018)** and the **Shanghai Cooperation Organisation's Code of Conduct (2015)**.[3] While the Tallinn Manual offers a Western academic interpretation of how existing international law applies to cyber operations, the Paris and Shanghai frameworks represent competing geopolitical visions: the former promotes a liberal, multistakeholder approach, while the latter emphasizes sovereignty, state control of information, and the creation of new legal instruments.[4] These competing approaches underscore the challenges of achieving legal harmonization in cyberspace and illustrate the ongoing contest over who defines the rules of the digital age.

---

https://undocs.org/A/75/816.

[1] Organization for Security and Co-operation in Europe (OSCE), Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of ICTs, 2016, https://www.osce.org/pc/227281.

[2] Tallinn Manual 2.0 (Schmitt, ed.), 543–567.

[3] Government of France, Paris Call for Trust and Security in Cyberspace, 2018, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/paris-call/; Shanghai Cooperation Organisation, International Code of Conduct for Information Security, 2015, https://ccdcoe.org/uploads/2018/10/SCO-CyberCode.pdf.

[4] Elaine Korzak, "Norms in Cyberspace: The SCO Code of Conduct," in Global Cybersecurity Norms, ed. Patryk Pawlak (EU Institute for Security Studies, 2017), 48–52.

Taken together, these two sections trace the architecture of international cyber law as it currently stands: a fragmented but evolving system marked by both institutional cooperation and normative divergence. They also reflect the strategic interests that shape cyber governance and the persistent struggle between global convergence and regional autonomy in defining lawful state behavior in the cyber domain.

Section One: The role of the United Nations and regional organizations in achieving international cybersecurity

In the face of growing cyber threats that transcend national borders and pose risks to international peace, security, and development, the global community has increasingly turned to multilateral institutions for guidance and coordination. As cyberspace evolves into a strategic and contested domain, questions of sovereignty, responsible state behavior, and international cooperation have become central to international law and diplomacy. In this context, both the **United Nations (UN)** and **regional organizations** have emerged as key actors in shaping international cybersecurity frameworks, albeit through different mandates and mechanisms.

The **United Nations** plays a pivotal role in developing norms, principles, and voluntary frameworks to guide state conduct in cyberspace. Through mechanisms such as the **Group of Governmental Experts (GGE)** and the **Open-Ended Working Group (OEWG)**, the UN has fostered consensus on foundational concepts such as the applicability of international law to cyberspace, respect for sovereignty, non-intervention, and the

peaceful settlement of disputes in the digital environment.[1] These processes have also contributed to the emergence of confidence-building measures (CBMs), capacity-building priorities, and efforts to promote transparency and cooperation among member states.[2] While UN cyber governance remains largely non-binding, it provides the essential normative infrastructure for developing shared expectations and fostering international dialogue.

At the same time, **regional organizations** such as the **Organization for Security and Co-operation in Europe (OSCE)**, the **European Union (EU)**, the **African Union (AU)**, the **Association of Southeast Asian Nations (ASEAN)**, and the **Organization of American States (OAS)** have played an indispensable role in implementing and operationalizing cybersecurity norms and policies. These organizations are often better positioned to address regional dynamics, tailor responses to local capabilities, and build trust among neighboring states.[3] They have developed region-specific CBMs, legislative frameworks, capacity-building programs, and cooperative security arrangements that contribute directly to international cybersecurity.[4] In particular, the OSCE has led in translating UN-endorsed cyber norms into actionable CBMs, providing a model for how regional institutions can support and reinforce global cyber stability.

[1] United Nations GA Report, *A/70/174 (2015).*
[2] United Nations General Assembly, Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, A/75/816 (2021), https://undocs.org/A/75/816.
[3] Elaine Korzak, "Regional Approaches to Cybersecurity and International Law," in The Oxford Handbook of Cybersecurity, eds. Myriam Dunn Cavelty and Florian Egloff (Oxford University Press, 2022), 215.
[4] Organization for Security and Co-operation in Europe (OSCE), OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of ICTs, 2016, https://www.osce.org/pc/227281.

This section explores the complementary contributions of the United Nations and regional organizations in achieving international cybersecurity. The first part, **"The Role of the United Nations in Shaping International Cyberspace Governance,"** examines how the UN has served as the primary platform for intergovernmental negotiation, norm development, and inclusive dialogue in the cyber domain. The second part, **"The Role of Regional Organizations in Achieving International Cybersecurity,"** highlights how regional mechanisms have transformed global principles into practical strategies, with particular attention to the OSCE as a case study in regional cyber diplomacy.

1. The Role of the United Nations in Shaping International Cyberspace Governance

The United Nations (UN) has played a pivotal role in initiating and shaping the discourse around international rules governing cyberspace. Given the cross-border nature of cyber threats and the absence of a centralized global regulator for the internet, the UN has emerged as a primary platform for promoting dialogue, establishing norms, and seeking consensus among its member states. Despite facing challenges related to political fragmentation and diverging interests among states, the UN's efforts have laid essential groundwork for future international governance of cyberspace.

The UN's first significant step in addressing cyber-related issues came through the **Group of Governmental Experts (GGE)**, first convened in 2004 under the auspices of the First Committee on Disarmament and International Security. The GGE was tasked with exploring potential threats

in the information space and considering measures to address them.[1] Over multiple iterations—2004, 2009, 2013, 2015, and 2021—the GGE has produced several consensus reports, each advancing the international community's understanding of cyber norms, confidence-building measures, and the applicability of existing international law to cyberspace.

The **2013 GGE report** was a landmark moment. It recognized for the first time the applicability of international law, including the UN Charter, to state behavior in cyberspace.[2] This affirmation marked a consensus that cyberspace is not a legal vacuum and that principles such as sovereignty, non-intervention, and the prohibition of the use of force also extend to cyber operations. The **2015 GGE report** built on this by articulating eleven voluntary, non-binding norms of responsible state behavior in cyberspace, including prohibitions against attacking critical infrastructure and using proxies for cyber operations.[3] These norms, while not legally binding, set behavioral expectations and have since informed the cyber policies of multiple countries and regional organizations.

In parallel with the GGE, the UN established the **Open-Ended Working Group (OEWG)** in 2018, which aimed to create a more inclusive process for developing cyber norms. Unlike the GGE, which included a limited number of states, the OEWG is open to all 193 UN member states. The OEWG has provided a platform for broader participation, particularly from developing countries, thereby democratizing the norm-making process.[4] The OEWG's 2021 final report reaffirmed many of the GGE's

[1] United Nations Office for Disarmament Affairs, "Developments in the Field of Information and Telecommunications in the Context of International Security," https://www.un.org/disarmament/ict-security/.
[2] Paris Call (France).
[3] United Nations GA Report, *A/70/174 (2015).*
[4] Katharina E. Höne, "The UN Open-Ended Working Group: A New Hope for Cyberspace Governance?," The Hague Journal of Diplomacy 15, no. 4 (2020): 471–478.

conclusions and added emphasis on capacity-building, multistakeholder engagement, and the protection of critical information infrastructure.[1]

The UN's role also extends to **confidence-building measures (CBMs)**, which are crucial in reducing the risk of conflict in cyberspace. The GGE and OEWG have both emphasized the importance of transparency, incident response cooperation, and points of contact among states.[2] In this context, the UN's Office for Disarmament Affairs (UNODA) supports member states in developing national cyber strategies and fostering regional cooperation. Regional organizations such as the OSCE, ASEAN Regional Forum, and OAS have subsequently adopted UN-recommended CBMs in their respective frameworks.

In addition to state-focused processes, the UN has increasingly recognized the importance of **multistakeholder engagement** in cyberspace governance. Initiatives such as the **Internet Governance Forum (IGF)**, established by the World Summit on the Information Society (WSIS), provide platforms for dialogue among governments, civil society, the private sector, and the technical community.[3] While the IGF does not produce binding decisions, it facilitates inclusive discourse on digital rights, cybersecurity, and internet access, complementing intergovernmental processes.

Despite these achievements, the UN's efforts have not been free from criticism. Key disagreements persist between Western liberal democracies and authoritarian regimes—particularly Russia and China—regarding the principles of cyberspace governance. Western states generally advocate for

[1] UN OEWG Final Report A/75/816 (2021).
[2] United Nations Institute for Disarmament Research (UNIDIR), Cyber Stability Conference Report (2021), https://unidir.org.
[3] Milton Mueller, *Networks and States* (MIT Press, 2010).

an open, interoperable, secure internet governed by multistakeholder models, whereas Russia and China promote a state-centric model emphasizing "cyber sovereignty."[1] These divisions have sometimes hampered consensus in UN forums, most notably in the 2017 GGE, which failed to produce a final report due to disagreements over the applicability of international law to cyber conflict.[2]

Furthermore, questions remain about enforcement mechanisms. The voluntary nature of the UN norms means that compliance is largely dependent on political will, peer pressure, and reputational considerations. While some states have incorporated these norms into national strategies, others have continued to engage in disruptive cyber behavior, highlighting the limitations of non-binding instruments.

Nonetheless, the UN's work has established a **baseline framework for responsible state behavior in cyberspace** and continues to serve as a central forum for dialogue. By integrating principles of international law, creating platforms for consensus-building, and promoting inclusivity, the UN has helped chart a path toward more stable and secure cyberspace governance. Its work remains ongoing through the OEWG's extended mandate (2021–2025), with future dialogues expected to tackle more complex challenges such as attribution, cyber conflict escalation, and the development of binding international treaties.[3]

[1] Laura DeNardis, *The Global War for Internet Governance.*
[2] Eneken Tikk, "The Failed UN GGE 2016–2017: UN Cyber Norms–A Battle Worth Fighting For?," EU Cyber Direct, September 2017, https://eucyberdirect.eu/content_research/the-failed-un-gge-2016-2017/.
[3] United Nations General Assembly, "Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies (2021–2025)," A/RES/75/240.

1.1 UN Group of Governmental Experts (GGE)

The United Nations Group of Governmental Experts (GGE) has been central to the international effort to develop norms, rules, and principles for responsible state behavior in cyberspace. Established under the First Committee of the United Nations General Assembly, the GGE was initiated in 2004 in response to growing concerns about information and communications technology (ICT) threats to international peace and security. Its primary mandate has been to study and articulate how international law applies to state conduct in cyberspace and to propose voluntary norms to reduce conflict risks in the cyber domain.[1]

The initial GGE, convened in 2004, was exploratory, setting the stage for further investigations into international cyber threats.[2] It wasn't until the 2010 GGE report that consensus began to emerge regarding the relevance of existing international legal frameworks.[3] The breakthrough, however, came with the 2013 GGE report, which for the first time explicitly affirmed that international law, including the UN Charter, is applicable to state behavior in cyberspace. This declaration underscored that cyberspace is not a legal vacuum and that principles such as sovereignty, non-intervention, and the prohibition of the use of force apply equally online as offline.[4]

The 2015 GGE, comprised of 20 member states, was perhaps the most influential iteration. It produced a consensus report that outlined 11 voluntary, non-binding norms of responsible state behavior. These included

[1] United Nations Office for Disarmament Affairs, Developments in the Field of Information and Telecommunications in the Context of International Security, https://www.un.org/disarmament/ict-security/.
[2] Elaine Korzak, *Norms in Cyberspace* (Lawfare).
[3] United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/65/201 (2010).
[4] United Nations General Assembly, "Report of the Group of Governmental Experts," A/68/98 (2013).

commitments not to target critical infrastructure, not to damage another state's cyber emergency response team (CERT), and to cooperate in investigating cybercrime.[1] These norms became a reference point for many regional organizations and were adopted or echoed in policy frameworks such as those of the OSCE and ASEAN Regional Forum. The 2015 report also emphasized confidence-building measures (CBMs) and capacity building, acknowledging disparities among states in cyber capabilities.[2]

Despite these achievements, the GGE process has been hampered by geopolitical tensions. The 2016–2017 GGE failed to issue a consensus report due to disagreements over the application of international humanitarian law, the right to self-defense, and attribution in cyberspace.[3] Notably, states such as the United States, Russia, and China diverged significantly on key principles: while the U.S. supported a rules-based order grounded in existing international law, Russia and China favored new treaties based on cyber sovereignty and state control over internet infrastructure.[4] The failure of this GGE highlighted the fragility of consensus in an increasingly polarized geopolitical climate.

To address these limitations, the UN established a parallel, more inclusive process: the Open-Ended Working Group (OEWG), which allowed all 193 UN member states to participate in cyber norm discussions.[5] While the OEWG provided a broader platform, the GGE continued its work with a narrower expert group. The most recent GGE, convened in 2019 and

[1] United Nations GA Report, *A/70/174 (2015).*
[2] James A. Lewis, "The UN GGE and the International Code of Conduct for Information Security," Center for Strategic and International Studies (2015), https://www.csis.org.
[3] Tikk, Eneken. "The Failed UN GGE 2016–2017: UN Cyber Norms – A Battle Worth Fighting For?" EU Cyber Direct, September 2017, https://eucyberdirect.eu.
[4] Tim Maurer, *Cyber Mercenaries.*
[5] Katharina E. Höne, "The UN Open-Ended Working Group: A New Hope for Cyberspace Governance?," The Hague Journal of Diplomacy 15, no. 4 (2020): 471–478.

reporting in 2021, again reached consensus and reaffirmed the applicability of international law to cyberspace. However, the report was careful not to define certain contested terms such as “armed attack” or “use of force” in the cyber context, reflecting continuing political sensitivities.[1]

The GGE's contributions extend beyond its formal outputs. It has served as a platform for confidence-building among states and for the gradual internalization of legal and normative standards. Moreover, the GGE has influenced national cyber strategies and inspired regional dialogues, such as those led by the Organization of American States and the African Union.[2] Importantly, the GGE process has encouraged states to establish national points of contact, share information on threat perceptions, and enhance transparency — measures that, although voluntary, can prevent miscalculation and escalation.

Nevertheless, critics argue that the GGE's limited membership and lack of enforcement mechanisms undermine its long-term impact. Developing countries have often been underrepresented, which raises concerns about the inclusivity and equity of the norm-development process.[3] Additionally, voluntary norms have not deterred state-sponsored cyberattacks or advanced persistent threats (APTs), illustrating the limitations of non-binding agreements in a domain characterized by asymmetric capabilities and weak attribution mechanisms.

In conclusion, the GGE remains a cornerstone of international efforts to manage state behavior in cyberspace. While not without shortcomings, it has

[1] United Nations General Assembly, “Report of the Group of Governmental Experts,” A/76/135 (2021).
[2] Organization of American States, Confidence-Building Measures and Regional Cyber Norms, https://www.oas.org/en.
[3] Jovan Kurbalija, “The UN GGE: What Comes Next for Cybersecurity Norms?,” DiploFoundation, 2021, https://www.diplomacy.edu.

helped legitimize the application of international law to cyber operations and fostered gradual alignment among key stakeholders. Its work has paved the way for more inclusive and institutionalized governance structures, even as the international community continues to grapple with the legal, political, and technical complexities of cybersecurity.

1.2 Open-Ended Working Group (OEWG) on Developments in the Field of ICTs

The **Open-Ended Working Group (OEWG)** on Developments in the Field of Information and Communication Technologies (ICTs) in the Context of International Security represents a significant mechanism through which the United Nations fosters multilateral dialogue on cybersecurity. Established by **United Nations General Assembly resolution 73/27 in 2018**, the OEWG is composed of all UN member states and operates with the purpose of examining existing and emerging threats related to ICTs, promoting a secure and peaceful cyberspace, and recommending norms, rules, and principles of responsible state behavior in cyberspace.[1]

What distinguishes the OEWG from its counterpart, the **Group of Governmental Experts (GGE)**, is its inclusive format. Unlike the GGE, which is limited to a select group of experts from member states, the OEWG is open to the participation of **all UN member states**, giving it a broader base for consensus-building and reflecting a diversity of geopolitical perspectives, particularly from the Global South.[2] This open format is critical, as many developing countries have emphasized the need for more

[1] United Nations General Assembly, Resolution 73/27: Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/73/27 (2018), https://digitallibrary.un.org/record/1650454.
[2] James A. Lewis, "Multilateral Agreement on Cybersecurity Norms," Center for Strategic and International Studies, March 2021, https://www.csis.org/analysis/multilateral-agreement-cybersecurity-norms.

equitable participation in global digital governance and have criticized the exclusivity of earlier GGE processes.[1]

The **first OEWG session** (2019–2021), chaired by **Ambassador Jürg Lauber** of Switzerland, concluded with the adoption of a final consensus report in March 2021. The report reaffirmed previous agreements reached by the GGEs, including the voluntary, non-binding norms of responsible state behavior as outlined in the 2015 GGE report.[2] These norms cover a range of behaviors, such as refraining from damaging critical infrastructure, cooperating in ICT-related incidents, and protecting the integrity of supply chains.[3] Importantly, the OEWG also stressed the **importance of capacity-building**, highlighting the unequal capabilities among states in cybersecurity, and calling for international assistance and regional cooperation mechanisms.[4]

The OEWG also brought new voices to the cybersecurity table, incorporating input from **non-governmental stakeholders**, including civil society, academia, and the private sector. While the level of participation and influence of these stakeholders remained limited compared to states, their inclusion marked a step forward in democratizing international cyber governance.[5] States such as Canada, the Netherlands, and Germany advocated strongly for multistakeholder participation, recognizing the complex and decentralized nature of cyberspace. However, countries such as

[1] Erica D. Borghard and Shawn W. Lonergan, "The United Nations and Cyberspace Norms," Council on Foreign Relations, March 9, 2021, https://www.cfr.org/blog/united-nations-and-cyberspace-norms.
[2] UN OEWG Final Report A/75/816 (2021).
[3] Ibid.
[4] Ibid.
[5] Kubo Mačák, "The United Nations Open-Ended Working Group: What Role for Non-Governmental Stakeholders?" Just Security, January 20, 2020, https://www.justsecurity.org/68118/the-united-nations-open-ended-working-group-what-role-for-non-governmental-stakeholders/.

Russia and China remained skeptical of non-state actors' involvement in what they perceive as a national security domain.[1]

Following the conclusion of the first OEWG, a **second OEWG was established for the 2021–2025 period**, chaired by **Ambassador Burhan Gafoor** of Singapore. This second OEWG builds upon the previous mandate but with an extended timeline and an expanded scope. It continues to address threats, rules, norms, and international law in cyberspace, while also seeking to operationalize norms through **confidence-building measures (CBMs)**, institutional dialogue, and national implementation strategies.[2] An essential development in the second OEWG has been the discussion around establishing **a global, intergovernmental, and UN-led regular institutional dialogue mechanism** on ICT security—an issue that has gained momentum as states express concern about the fragmentation of norms and the lack of enforcement mechanisms.[3]

Moreover, the OEWG has emerged as a site of geopolitical contestation. **Competing visions of internet governance**—between liberal democratic states advocating for an open, interoperable, and rights-respecting internet, and authoritarian regimes calling for cyber sovereignty and state control—are evident in OEWG debates.[4] The concept of **sovereignty in cyberspace** remains particularly contentious, as Russia and China push for stronger recognition of state control over digital

[1] Kubo Mačák, "The United Nations Open-Ended Working Group.
[2] United Nations Office for Disarmament Affairs (UNODA), Second Open-ended Working Group on Developments in the Field of ICTs, https://www.un.org/disarmament/open-ended-working-group/.
[3] International Telecommunications Union, "UN Negotiations on ICT Security: OEWG Second Session Summary," July 2022, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/OEWG.aspx. Samantha Bradshaw and Laura DeNardis, "The Governance of Cybersecurity: Institutions, Norms and Power," in The Oxford Handbook of Cybersecurity, ed. Paul Cornish (Oxford University Press, 2021), 423.
[4] Samantha Bradshaw and Laura DeNardis, "The Governance of Cybersecurity: Institutions, Norms and Power," in The Oxford Handbook of Cybersecurity, ed. Paul Cornish (Oxford University Press, 2021), 423.

infrastructure within their borders, while Western countries emphasize transborder data flows and freedom of expression.[1] These ideological differences continue to shape the negotiation of norms and the interpretation of international law in cyberspace.

Despite these challenges, the OEWG plays a pivotal role in **norm diffusion and capacity alignment** among states. For many developing countries, the OEWG is one of the few platforms where they can articulate national cybersecurity concerns, request assistance, and participate in global norm-making without exclusion.[2] As a result, the OEWG contributes not only to technical discussions but also to **normative equity** in global cyber governance.

In sum, the OEWG has institutionalized a more inclusive and transparent approach to international cyber governance under the United Nations. While it does not produce binding agreements, its deliberations have meaningful effects on state behavior, particularly by reinforcing **normative expectations** and encouraging **collective action** to address cyber threats.

1.3 Capacity Building and the United Nations' Role in Global Cyber Development

Capacity building in cyberspace has emerged as a central pillar of global cybersecurity governance, especially for ensuring that all states—regardless of technological advancement—can participate effectively and responsibly in the digital domain. The United Nations has played a crucial role in promoting cyber development through both political frameworks and

[1] Samantha Bradshaw and Laura DeNardis,The Governance of Cybersecurity.
[2] UN OEWG Final Report A/75/816 (2021).

operational initiatives, particularly by fostering inclusivity, bridging digital divides, and strengthening institutional resilience in the Global South.

At the heart of the UN's engagement in cyber capacity building is the recognition that many developing countries lack the technical infrastructure, policy frameworks, and human capital necessary to effectively manage cybersecurity threats. This recognition was formalized in the work of the **United Nations Group of Governmental Experts (GGE)** and the **Open-Ended Working Group (OEWG)** on developments in the field of ICTs in the context of international security. Both forums identified capacity building as one of the **eleven voluntary, non-binding norms** of responsible state behavior endorsed in the 2015 GGE consensus report.[1] The OEWG's 2021 report reinforced this position by affirming that capacity building must be "sustainable, demand-driven, and tailored to national contexts," and it called for increased international cooperation in providing assistance to states that request it.[2]

One of the key dimensions of cyber capacity building is the development of **national strategies and legal frameworks** that align with international law and global norms. The **United Nations Office for Disarmament Affairs (UNODA)** has facilitated regional workshops and seminars to support member states in drafting national cybersecurity strategies, legal reform, and incident response protocols.[3] Additionally, the UN has emphasized the importance of **Computer Emergency Response Teams (CERTs)** and **Computer Security Incident Response Teams (CSIRTs)**, particularly in under-resourced regions, where such institutions

[1] United Nations GA Report, *A/70/174 (2015).*
[2] UN OEWG Final Report A/75/816 (2021).
[3] UNODA, "Supporting National Implementation," https://www.un.org/disarmament/cybersecurity/.

are often absent or underdeveloped.[1] By helping states to establish these operational entities, the UN contributes directly to bolstering technical resilience and situational awareness in cyberspace.

Beyond legal and institutional development, the UN supports **human capacity development** by promoting education and training programs. For instance, the **United Nations Institute for Disarmament Research (UNIDIR)** and UNODA have collaborated with regional organizations to develop training modules that enhance the skills of policymakers, diplomats, and technical personnel involved in national cybersecurity governance.[2] These efforts not only promote awareness of existing international frameworks but also help states to meaningfully participate in multilateral negotiations and norm-building processes.[3] Importantly, such training opportunities are often tailored to the specific needs and capabilities of the target country or region, allowing for differentiated and context-sensitive implementation.

Another significant contribution by the UN lies in its **normative leadership**, which emphasizes that capacity-building efforts must be **inclusive and rights-respecting**. The OEWG's 2021 final report underscored that capacity-building initiatives should uphold human rights, promote gender equality, and prioritize the empowerment of marginalized communities, including women and youth.[4] This normative framing has gained support from states and civil society alike, with organizations such as

[1] United Nations Institute for Disarmament Research (UNIDIR), Cyber Policy Portal, https://cyberpolicyportal.org.
[2] UNIDIR, "Cyber Capacity-Building and the UN's Role," https://unidir.org.
[3] Ibid.
[4] UN OEWG Final Report A/75/816 (2021).

the Global Forum on Cyber Expertise (GFCE) and the CyberPeace Institute advocating for holistic and human-centric approaches to capacity building.[1]

The UN's role also extends to **coordination and information-sharing**. As the international system becomes more complex and fragmented, the UN has sought to serve as a **convening platform** to prevent duplication and enhance synergies among stakeholders. The OEWG has called for improved transparency in the mapping of global and regional capacity-building initiatives, including the establishment of voluntary repositories of national and regional practices.[2] In line with this objective, the **Cyber Policy Portal** maintained by UNIDIR provides a centralized, open-access platform for states to share their national policies, structures, and cooperation mechanisms, contributing to confidence-building and global cyber stability.[3]

However, challenges remain. One major concern is the **lack of sustainable funding** for capacity-building programs, especially in Least Developed Countries (LDCs). Despite increasing international recognition of the need for cyber development assistance, financial support often remains short-term or tied to donor interests.[4] Moreover, political disagreements—particularly between Western and non-Western states—sometimes complicate consensus on the scope and objectives of capacity-

[1] Global Forum on Cyber Expertise, "Global Agenda for Cyber Capacity Building," https://thegfce.org/global-agenda/.
[2] UNODA, "Second OEWG on ICTs," https://www.un.org/disarmament/open-ended-working-group/.
[3] UNIDIR, Cyber Policy Portal, https://cyberpolicyportal.org.
[4] Madeline Carr and Tim Stevens, "Governing Cybersecurity: Global Trends and Challenges," Contemporary Security Policy 40, no. 3 (2019): 379–401.

building efforts, especially when such efforts are perceived as vehicles for advancing geopolitical influence.[1]

Nevertheless, the United Nations continues to play an indispensable role in fostering equitable cyber development. By advancing inclusive capacity-building principles, supporting technical and legal infrastructure, and promoting transparent and rights-based governance models, the UN lays the groundwork for a **more secure, stable, and inclusive digital future** for all member states.

1.4 Criticism and Limitations of the United Nations' Approach to Cyberspace Governance

While the United Nations has positioned itself as a central forum for addressing cyber threats and fostering international cooperation in the digital domain, its role has not been free from criticism. Observers and practitioners have raised significant concerns regarding the **effectiveness, inclusiveness, and coherence** of the UN's approach to cyberspace governance, particularly in the context of growing geopolitical tensions, fragmented norm development, and structural limitations within the institution.

One of the foremost criticisms directed at the UN's role in cyber governance is its **limited enforcement capacity**. Although the UN has facilitated the development of voluntary norms—particularly through the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG)—these norms remain **non-binding**, and the UN lacks any mechanism to hold states accountable for violations.[2] As a result, there is a

[1] Maria Farrell and Niels ten Oever, "Infrastructure and Power in the Global Digital Space," Internet Policy Review 8, no. 4 (2019), https://policyreview.info/articles/analysis/infrastructure-and-power-global-digital-space.
[2] United Nations GA Report, *A/70/174 (2015).*

growing gap between norm creation and norm implementation, leading some scholars to argue that the UN process has produced **symbolic agreements with little practical consequence**.[1] The lack of enforcement mechanisms is particularly problematic in the wake of repeated cyber incidents attributed to state actors, including ransomware campaigns, intellectual property theft, and cyberattacks on critical infrastructure.[2]

Another limitation concerns the **slow pace of consensus-building** in UN forums. Given the organization's commitment to consensus among its member states, progress is often hampered by geopolitical rivalries—particularly between major cyber powers such as the United States, China, and Russia.[3] These divisions have led to **duplicative and overlapping initiatives**, as seen in the parallel establishment of the GGE and OEWG. Although both groups aim to address cyber stability, their existence reflects a compromise rather than a coherent institutional framework.[4] The political divisions are further exacerbated by **divergent conceptions of internet governance**, with some states advocating for a multistakeholder approach and others insisting on sovereign control over national cyberspace.[5]

The **exclusion of non-state actors** from many of the UN's cyber processes has also drawn criticism. Despite the multistakeholder nature of the digital ecosystem—where private companies, civil society, and technical communities play essential roles in internet governance—UN cybersecurity

[1] Joseph Nye, "Power and Norms in Cyberspace," Georgetown Journal of International Affairs 19, no. 3 (2018): 6–13.
[2] Max Smeets, No Shortcuts: Why States Struggle to Develop a Military Cyber-Force (Oxford University Press, 2022), 182–184.
[3] Erica D. Borghard and Shawn W. Lonergan, "The United Nations and Cyberspace Norms," Council on Foreign Relations, March 9, 2021, https://www.cfr.org/blog/united-nations-and-cyberspace-norms.
[4] James A. Lewis, "Multilateral Agreement on Cybersecurity Norms," Center for Strategic and International Studies, March 2021, https://www.csis.org/analysis/multilateral-agreement-cybersecurity-norms.
[5] Laura DeNardis, *The Global War for Internet Governance*, 52–55.

discussions have historically been **state-centric**.[1] While the OEWG has experimented with including non-governmental voices through consultations and written submissions, civil society organizations have reported that their involvement remains **superficial and poorly integrated** into decision-making.[2] This exclusion limits the diversity of perspectives in shaping cyber norms and reduces the legitimacy and practicality of proposed frameworks.

Further critique is aimed at the **asymmetry in cyber capacities** among member states, which is often inadequately addressed in UN deliberations. Developing countries frequently lack the resources and expertise to participate effectively in technical discussions or to implement agreed norms.[3] Although capacity building is regularly emphasized as a priority, critics argue that many initiatives are **poorly coordinated, insufficiently funded, or donor-driven**, reflecting the strategic interests of contributing states rather than the actual needs of recipients.[4] The resulting dependency undermines the goal of equitable cyber development and perpetuates power imbalances in global governance structures.

Moreover, the **absence of a permanent institutional framework** within the UN to address cybersecurity issues in a sustained and structured manner remains a notable gap. Current efforts—such as the OEWG—are **mandate-limited and time-bound**, often concluding without clear follow-

[1] Kubo Mačák, "The United Nations Open-Ended Working Group: What Role for Non-Governmental Stakeholders?" Just Security, January 20, 2020, https://www.justsecurity.org/68118/the-united-nations-open-ended-working-group-what-role-for-non-governmental-stakeholders/.
[2] Global Partners Digital, "Civil Society Engagement in the UN OEWG," 2020, https://www.gp-digital.org/publication/civil-society-engagement-in-the-un-oewg/.
[3] OEWG Final Report 2021, A/75/816, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf.
[4] Global Forum on Cyber Expertise, "Global Agenda for Cyber Capacity Building," https://thegfce.org/global-agenda/.

up mechanisms.[1] As cyber threats evolve rapidly, particularly with the rise of artificial intelligence, quantum computing, and hybrid warfare, the lack of institutional continuity hinders the UN's ability to adapt and respond effectively.[2] Some experts have called for the establishment of a **standing UN body** on cybersecurity to provide consistent oversight, support implementation, and serve as a repository for state practices and best practices.[3] However, proposals for such a body have yet to gain sufficient political traction.

Additionally, the **politicization of cyber discussions** at the UN undermines the organization's ability to function as a neutral platform for dialogue. Allegations of state-sponsored cyber operations are frequently raised in politically charged terms, and the attribution of cyber incidents remains contested.[4] These dynamics often prevent meaningful engagement, as states default to strategic posturing rather than constructive negotiation. In such an environment, the UN's diplomatic machinery—designed to foster trust and cooperation—can become a venue for **rhetorical escalation rather than conflict resolution**.[5]

Despite these criticisms, many analysts acknowledge the symbolic and normative significance of the UN's role. However, they caution that without **structural reforms**, improved stakeholder engagement, and stronger follow-through mechanisms, the UN risks **ceding influence to more agile and**

[1] United Nations Office for Disarmament Affairs (UNODA), "Second OEWG on ICTs," https://www.un.org/disarmament/open-ended-working-group/.
[2] Elaine Korzak, "Cybersecurity and the United Nations: The Quest for International Norms," in Global Cybersecurity Norms, ed. Patryk Pawlak (EU Institute for Security Studies, 2017), 43–46.
[3] Anriette Esterhuysen, "Cyber Norms and the UN: A Civil Society Perspective," APC Issue Papers, 2020, https://www.apc.org/en/pubs/cybernorms-and-un-civil-society-perspective.
[4] Robert Morgus and Justin Sherman, "Norms for Cyber Stability: Examining the UN GGE and OEWG," New America, April 2021, https://www.newamerica.org/cybersecurity-initiative/reports/norms-for-cyber-stability/.
[5] Tim Maurer, *Cyber Mercenaries.*

informal forums, such as regional organizations or industry-led coalitions.[1] The challenge ahead lies in reconciling the UN's universal legitimacy with the agility needed to address the fast-changing dynamics of cyberspace.

2. The Role of Regional Organizations in Achieving International Cybersecurity

In recent decades, regional organizations have emerged as pivotal actors in the promotion of cybersecurity and the governance of cyberspace. While the United Nations (UN) remains the primary international forum for dialogue on cyber norms, it is regional organizations that frequently operationalize these principles and provide localized responses to cyber threats. Regional mechanisms not only complement the efforts of the UN but also respond more directly to the political, technical, and socio-economic specificities of their respective member states. Through confidence-building measures (CBMs), legal harmonization, training, and infrastructure development, regional organizations are instrumental in advancing a more secure and cooperative international cyberspace.

The **Organization for Security and Co-operation in Europe (OSCE)** has been at the forefront of regional cyber diplomacy. In 2013 and 2016, it became the first regional organization to adopt a comprehensive set of CBMs aimed at reducing the risks of conflict stemming from the use of information and communication technologies (ICTs).[2] These measures include the exchange of information on national cyber strategies, the establishment of points of contact, and the promotion of public-private

[1] Amy Ertan, "Cybersecurity Governance: Multilateralism vs. Minilateralism," RUSI Journal, 167, no. 4 (2022): 40–49.
[2] Organization for Security and Co-operation in Europe, OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, OSCE, 2016, https://www.osce.org/pc/227281.

partnerships.[1] OSCE CBMs are explicitly aligned with the non-binding norms proposed by the UN Group of Governmental Experts (GGE), thus serving as a model of how regional initiatives can reinforce global norms.[2] Moreover, OSCE's consensus-based approach facilitates trust among its 57 participating states, many of which are also engaged in geopolitical rivalries.

Similarly, the **European Union (EU)** has developed a robust cybersecurity framework through both regulatory and strategic tools. The EU's **Cybersecurity Act** (2019) established a permanent mandate for the European Union Agency for Cybersecurity (ENISA) and introduced a cybersecurity certification framework for ICT products and services.[3] The EU has also adopted the **Network and Information Security (NIS) Directive**, which mandates member states to strengthen the security of critical infrastructure and to improve cross-border cooperation.[4] Through these legal mechanisms, the EU sets binding standards that enhance collective resilience. In addition to internal regulation, the EU engages externally through **cyber diplomacy**, having launched the EU Cyber Diplomacy Toolbox in 2017 to respond collectively to malicious cyber activities.[5]

In the Asia-Pacific region, the **Association of Southeast Asian Nations (ASEAN)** has made strides toward building a regional

[1] OSCE, OSCE, 2016.
[2] James A. Lewis, "Multilateral Agreement on Cybersecurity Norms," Center for Strategic and International Studies, March 2021, https://www.csis.org/analysis/multilateral-agreement-cybersecurity-norms.
[3] European Union, Regulation (EU) 2019/881 (Cybersecurity Act), https://eur-lex.europa.eu/eli/reg/2019/881/oj.
[4] European Commission, The EU's Cybersecurity Strategy for the Digital Decade, December 2020, https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade.
[5] European External Action Service, "Cyber Diplomacy Toolbox," 2017, https://www.eeas.europa.eu/eeas/cyber-diplomacy-toolbox_en.

cybersecurity architecture. ASEAN established a **Cybersecurity Cooperation Strategy** in 2017 and continues to strengthen ties with dialogue partners through the **ASEAN Regional Forum (ARF)**.[1] The ARF has supported track 1.5 and track 2 dialogues to facilitate regional cooperation and capacity building. Moreover, the **ASEAN-Singapore Cybersecurity Centre of Excellence**, launched in 2019, serves as a hub for regional training, technical exercises, and policy development.[2] While ASEAN's consensus-based approach can slow down decision-making, it has proven effective in maintaining regional unity and fostering mutual trust.

The **African Union (AU)**, while facing infrastructural and capacity constraints, has also taken significant steps toward cybersecurity development. The **Malabo Convention** (2014) on Cyber Security and Personal Data Protection aims to harmonize legal frameworks across African countries, although ratification has been slow.[3] The AU's collaboration with partners such as the **Council of Europe** and the **International Telecommunication Union (ITU)** has facilitated capacity-building workshops, legal reform, and incident response training.[4] Regional economic communities (RECs), such as the **Economic Community of West African States (ECOWAS)**, are also developing regional strategies and computer emergency response teams (CERTs).[5]

In Latin America, the **Organization of American States (OAS)** has positioned itself as a regional cybersecurity leader. Its **Inter-American**

[1] ASEAN, ASEAN Cybersecurity Cooperation Strategy 2017–2020, https://asean.org.
[2] ASEAN-Singapore Cybersecurity Centre of Excellence, "About Us," 2023, https://www.sgcoe.org.sg.
[3] African Union, African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), 2014, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.
[4] ITU, "Capacity Building in Africa," 2022, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx.
[5] ECOWAS, Regional Cybersecurity and Cybercrime Strategy, 2019, https://www.ecowas.int.

Committee against Terrorism (CICTE) operates a dedicated Cybersecurity Program that assists member states in drafting national strategies, creating incident response capacities, and organizing regional exercises.[1] The OAS's adoption of CBMs and its publication of best practices reinforce its role as a bridge between normative frameworks and practical implementation.[2] Moreover, its close engagement with civil society and the private sector exemplifies a multistakeholder approach in action.

Despite these achievements, the role of regional organizations is not without limitations. There is considerable **variation in capacity and political will** across and within regions, which can hamper the effectiveness of initiatives. Furthermore, the lack of **formal coordination mechanisms** between regional bodies and the UN can result in duplication of efforts or normative fragmentation.[3] Nevertheless, regional organizations remain indispensable in operationalizing global norms, tailoring solutions to regional needs, and building the foundational trust necessary for broader international cooperation in cybersecurity.

2.1 The OSCE as a Regional Implementer of UN Cyber Norms: A Case Study

The **Organization for Security and Co-operation in Europe (OSCE)** has established itself as one of the most active regional organizations in operationalizing and advancing the implementation of international cyber norms developed under the auspices of the United Nations. With its 57 participating states—spanning North America, Europe, and Central Asia—

[1] Organization of American States, "Cybersecurity Program – CICTE," https://www.oas.org/en/sms/cicte/cybersecurity.asp.
[2] Ibid.
[3] Elaine Korzak, "Cybersecurity and the United Nations: The Quest for International Norms," in Global Cybersecurity Norms, ed. Patryk Pawlak (EU Institute for Security Studies, 2017), 50.

the OSCE provides a rare platform where countries with conflicting geopolitical interests, including the United States, Russia, and EU member states, engage on matters of international cybersecurity. This makes it a uniquely influential forum for translating UN-endorsed voluntary norms into actionable regional practices.

The OSCE's role in cybersecurity governance gained prominence with the adoption of **Confidence-Building Measures (CBMs)** in the field of information and communication technologies (ICTs). In 2013, the OSCE became the first regional organization to agree on a dedicated set of CBMs for cyberspace, which was later expanded in 2016.[1] These CBMs are designed to reduce the risks of misperception, escalation, and conflict arising from ICT-related incidents between states. The OSCE's 16 CBMs include provisions for the **exchange of national cybersecurity strategies**, the **designation of Points of Contact (PoCs)** for cyber incidents, information sharing about national organizational structures, and voluntary transparency regarding ICT policies and doctrines.[2]

What distinguishes the OSCE's approach is its **close alignment with the UN's cyber norm-building processes**, especially those articulated by the **Group of Governmental Experts (GGE)** and the **Open-Ended Working Group (OEWG)**. Many of the OSCE CBMs reflect the 2015 GGE consensus norms, particularly those concerning cooperation, information sharing, and respect for sovereignty in cyberspace.[3] In this way, the OSCE has become a crucial **regional conduit** for the implementation

[1] Organization for Security and Co-operation in Europe (OSCE), Decision No. 1106: Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of ICTs, PC.DEC/1106, April 2013, https://www.osce.org/pc/109168.
[2] OSCE CBMs 2016.
[3] United Nations GA Report, *A/70/174 (2015).*

and regional contextualization of global UN norms. Its work offers a practical framework for how states can build mutual trust and transparency in the absence of binding international law on cyber conduct.

Operationally, the OSCE's **cyber diplomacy efforts** have focused on building channels of communication that can function during both peacetime and crises. For example, the **Points of Contact Directory**, created as part of CBM 8, provides states with 24/7 technical and policy contacts to facilitate rapid communication in the event of cyber incidents.[1] This directory has been praised as a **low-cost but high-impact mechanism** to de-escalate tensions and prevent misunderstandings in the ambiguous domain of cyberspace.[2] In addition, the OSCE has conducted **regional workshops, tabletop exercises, and scenario-based discussions**, all aimed at building trust and readiness among national cybersecurity teams.[3]

Despite these achievements, the OSCE's implementation of cyber CBMs has faced several challenges. First, **uneven levels of engagement and capacity** across participating states create implementation gaps. While some countries have fully operationalized CBMs through national structures and reporting, others lag behind due to limited technical resources or political will.[4] This asymmetry undermines the overall efficacy and credibility of the framework. Second, **geopolitical tensions**, especially between NATO-aligned countries and Russia, complicate trust-building. While cyber CBMs are designed to mitigate precisely such tensions,

[1] OSCE Secretariat, Points of Contact Directory: Implementation Overview, 2022, https://www.osce.org/secretariat/ict-cbm-poc.
[2] James Lewis, "Confidence Building in Cyberspace: A Comparative Analysis," Center for Strategic and International Studies, 2020, https://www.csis.org.
[3] OSCE, ICT CBMs Implementation Toolkit, 2021, https://www.osce.org/secretariat/ict-cbm-toolkit.
[4] Elaine Korzak, "Regional Approaches to Cyber Confidence-Building," in Global Cybersecurity Norms, ed. Patryk Pawlak (EU Institute for Security Studies, 2017), 58.

ongoing distrust has sometimes limited their practical use in politically sensitive incidents.[1]

Moreover, the **non-binding nature of CBMs**, while making them more politically acceptable, also limits their enforceability. States are not obligated to report on the implementation of CBMs, and there are no penalties for non-compliance. This lack of enforcement has led some analysts to argue that CBMs are useful but insufficient in the face of **persistent state-sponsored cyber operations and the growing militarization of cyberspace**.[2] Furthermore, while the OSCE has proven effective in convening stakeholders, it lacks the **technical capabilities and resources** of more specialized cybersecurity agencies, such as ENISA in the European Union or the ITU globally.[3]

Nonetheless, the OSCE continues to evolve its cybersecurity agenda. In recent years, it has focused increasingly on **capacity-building and technical assistance**, especially for smaller and less-developed participating states. The organization has also supported **cross-regional dialogues**, linking its CBMs with those of the African Union and ASEAN, thereby promoting the global harmonization of cyber norms.[4] In doing so, the OSCE strengthens the international community's collective ability to prevent cyber conflict and advances the broader UN goal of building a peaceful and stable cyberspace.

In conclusion, the OSCE stands as a **model for how regional organizations can localize and implement UN cyber norms** in practical,

[1] Joseph S. Nye Jr., *Deterrence and Dissuasion in Cyberspace*, 44–71.
[2] Max Smeets, No Shortcuts: Why States Struggle to Develop a Military Cyber-Force (Oxford University Press, 2022), 186.
[3] EU Agency for Cybersecurity (ENISA), "ENISA and Regional Cyber Cooperation," https://www.enisa.europa.eu.
[4] OSCE, "Cross-Regional CBMs: Sharing Lessons and Enhancing Coordination," 2023, https://www.osce.org/secretariat/ict-cbm-cross-regional

confidence-building ways. By combining diplomatic dialogue, technical cooperation, and transparency mechanisms, the OSCE contributes significantly to global cybersecurity governance, even as it navigates the inherent limitations of voluntary regimes and geopolitical friction.

2.2 The Future of UN-Led Cyber Governance

As the digital domain becomes increasingly integral to global security, economic systems, and democratic governance, the future of United Nations-led cyber governance will depend on its ability to adapt to emerging challenges while maintaining credibility, inclusivity, and institutional coherence. The United Nations, through bodies such as the General Assembly's First Committee, the Group of Governmental Experts (GGE), and the Open-Ended Working Group (OEWG), has laid the foundation for state behavior in cyberspace. Yet, the rapidly evolving threat landscape and the acceleration of technological change are testing the limits of the current UN cyber governance architecture.

A key issue shaping the future of UN cyber governance is the **growing sophistication and frequency of cyber threats**, including ransomware, attacks on critical infrastructure, and AI-driven disinformation campaigns.[1] These developments demand not only stronger technical responses but also the evolution of **legal and normative frameworks**. As international tensions intensify, particularly among major cyber powers, the challenge lies in forging **consensus-based mechanisms** that go beyond voluntary norms. The GGE and OEWG processes have proven that even non-binding agreements are politically valuable, yet there is increasing pressure on the

[1] Center for Strategic and International Studies (CSIS), Significant Cyber Incidents Since 2006, updated 2024, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

UN to consider **binding instruments** that can ensure greater accountability.[1]

One possible development is the **establishment of a permanent institutional mechanism** within the UN to handle cybersecurity-related issues. At present, cyber discussions occur within ad hoc and time-bound groups like the GGE and OEWG. The lack of a standing body impedes continuity, coordination, and institutional memory.[2] Proposals have been made for a dedicated **UN Cybersecurity Council** or an independent platform to oversee implementation, monitor compliance, and provide technical assistance.[3] Such an entity could draw lessons from existing mechanisms, such as the UN Counter-Terrorism Committee, which combines norm-setting with capacity-building and compliance evaluation.

The UN's future role will also depend on its ability to **bridge the digital divide** through meaningful and tailored capacity-building. While current initiatives recognize this need, many developing states remain underrepresented in norm development and lack the infrastructure to effectively implement cyber CBMs or secure their critical networks.[4] The next generation of UN cyber governance must ensure **equitable participation**, possibly by embedding capacity-building obligations into

[1] Elaine Korzak, "Cybersecurity and the United Nations: The Quest for International Norms," in Global Cybersecurity Norms, ed. Patryk Pawlak (EU Institute for Security Studies, 2017), 44–47.
[2] Amy Ertan, "Why the UN Needs a Permanent Cybersecurity Body," RUSI Commentary, 2022, https://www.rusi.org/explore-our-research/publications/commentary/why-un-needs-permanent-cybersecurity-body.
[3] Anriette Esterhuysen, "Cyber Norms and the UN: A Civil Society Perspective," APC Issue Papers, 2020, https://www.apc.org/en/pubs/cybernorms-and-un-civil-society-perspective.
[4] UN OEWG Final Report A/75/816 (2021).

global agreements or creating a funding mechanism analogous to the Green Climate Fund in climate negotiations.[1]

The **question of stakeholder inclusion** remains central to the future legitimacy and effectiveness of UN cyber initiatives. While the OEWG has made modest progress in engaging civil society and the private sector, their role remains peripheral in many key negotiations.[2] The UN will likely face increasing demands for more **institutionalized multistakeholder participation**, especially given the private sector's dominance in digital infrastructure and the role of civil society in accountability and transparency. A future-proof UN model would need to develop procedural innovations—such as formal consultative mechanisms or observer status—for non-state actors within cyber deliberations.[3]

Another critical factor is **harmonization with regional and non-UN multilateral initiatives**. Bodies like the OSCE, ASEAN, and the African Union, as well as coalitions such as the Freedom Online Coalition, are generating their own cyber norms and capacity frameworks.[4] Without coordination, these efforts may fragment the global cybersecurity landscape. The UN could serve as a **meta-forum**, harmonizing standards and best practices developed across regions, while reinforcing the universality of international law in cyberspace.[5]

Finally, the UN must consider how to address **emerging technologies**—particularly **artificial intelligence**, **quantum computing**,

[1] Global Forum on Cyber Expertise, Global Agenda for Cyber Capacity Building, 2021, https://thegfce.org/global-agenda/.
[2] Global Forum on Cyber Expertise, Global Agenda for Cyber Capacity Building, 2021, https://thegfce.org/global-agenda/.
[3] Global Partners Digital, UN OEWG: Reflections and Recommendations on Stakeholder Engagement, 2021, https://www.gp-digital.org.
[4] Elaine Korzak, "Regional Approaches to Cybersecurity and International Law", 215.
[5] Tim Maurer, *Cyber Mercenaries*, 138.

and **space-based ICT systems**—which are not yet fully covered by existing norms.[1] There is growing discourse around establishing preemptive ethical and legal boundaries for these technologies before they become vectors for interstate conflict. To maintain its relevance, the UN must proactively incorporate these domains into its cyber governance agenda, perhaps through dedicated thematic sub-groups under future OEWG or GGE mandates.

In essence, the future of UN-led cyber governance hinges on institutional reform, increased stakeholder integration, and the ability to remain agile in the face of accelerating technological change and political fragmentation. Without these adaptations, the UN risks being sidelined by more flexible coalitions or regional blocs, potentially weakening the coherence of the international cybersecurity order.

[1] International Telecommunication Union (ITU), Emerging Technologies and Cybersecurity Risks, 2023, https://www.itu.int/en.

Section Two: Regional rules governing international cybersecurity

As global reliance on digital infrastructure deepens, the absence of a binding international legal framework governing state behavior in cyberspace has led to the emergence of alternative normative efforts. In this legal vacuum, various regional actors, expert communities, and political blocs have proposed interpretative guides, declarations, and codes of conduct to articulate their visions of responsible behavior in the cyber domain. These frameworks do not operate as enforceable treaties but rather as **soft law instruments**—tools designed to shape behavior, clarify legal obligations, and influence international discourse.

Among the most influential of these are the **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2017)**, a product of the NATO Cooperative Cyber Defence Centre of Excellence, and the politically-driven **Paris Call for Trust and Security in Cyberspace (2018)** and **Shanghai Cooperation Organisation (SCO) Code of Conduct (2015)**. Each of these initiatives emerges from distinct geopolitical and normative contexts and reflects the **diverging priorities of their sponsoring actors**—whether academic, Western democratic, or authoritarian-leaning regional alliances.

The first part of this section examines the **Tallinn Rules**, a comprehensive academic effort to interpret how existing international law applies to cyberspace. Drafted by an independent group of legal experts, the Tallinn Manual 2.0 expanded the scope of its predecessor to include not only cyber warfare but also peacetime operations, offering detailed commentary on sovereignty, non-intervention, due diligence, state responsibility, and

human rights.[1] Although not endorsed by states, the manual is widely regarded as a **reference point in cyber legal scholarship** and has been influential in shaping governmental and multilateral cyber postures.[2]

The second part explores the **Paris and Shanghai Rules**, two state-led frameworks that present **competing models for global cyber governance**. The **Paris Call**, initiated by France, advances a liberal, multistakeholder vision of cyberspace, emphasizing transparency, international law, and cooperation between governments, private entities, and civil society.[3] By contrast, the **Shanghai Code**, supported by China, Russia, and other SCO members, adopts a **state-centric approach** rooted in information sovereignty, content regulation, and the protection of internal political stability.[4] These frameworks highlight the **normative contestation** surrounding cybersecurity governance and reflect the growing polarization between open internet principles and cyber-sovereignty doctrines.

Together, these regional and bloc-based initiatives offer important insights into the **fragmented nature of global cyber norm development**. Their co-existence underscores not only the limitations of consensus-building in multilateral fora but also the strategic use of norm-setting to advance political and ideological objectives in the digital realm.

1. Tallinn Rules of International Law Applicable to Cyber Operations (2017)

The **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, published in 2017 by the NATO Cooperative Cyber

[1] Tallinn Manual 2.0 (Schmitt, ed.) , 1–3.
[2] Michael N. Schmitt, "The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: What It Is and Isn't," Just Security, February 9, 2017, https://www.justsecurity.org/37559/.
[3] Paris Call (France).
[4] SCO, *International Code of Conduct for Info Securit.*

Defence Centre of Excellence (CCDCOE), represents the most comprehensive non-binding academic effort to clarify how existing rules of international law apply to cyberspace.[1] It builds on the original **Tallinn Manual (2013)**, which focused narrowly on cyber warfare and the law of armed conflict, by expanding the legal analysis to include a wide range of peacetime cyber operations. Although not a document endorsed by states, **Tallinn Manual 2.0** has become a key point of reference for scholars, practitioners, and policymakers seeking to navigate the complex and evolving legal landscape of cyber activities.

The **Tallinn Manual 2.0** addresses 154 "rules" of customary and conventional international law as they relate to cyber operations, ranging from sovereignty and non-intervention to human rights, state responsibility, and the law of armed conflict.[2] The manual does not create new law but instead interprets how existing legal frameworks apply to the cyber domain. It was drafted by an international group of legal experts, known as the International Group of Experts (IGE), who operated independently of any government or international organization. Their interpretations, however, were informed by a comprehensive review of state practice, opinio juris, and relevant jurisprudence.[3]

One of the most discussed aspects of **Tallinn Manual 2.0** is the treatment of **sovereignty** in cyberspace. Rule 4 states that a cyber operation violates the sovereignty of a state if it results in a loss of functionality of cyber infrastructure or interferes with inherently governmental functions.[4]

[1] Tallinn Manual 2.0 (Schmitt, ed.).
[2] Ibid., 3–4.
[3] Michael N. Schmitt, "The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: What It Is and Isn't," Just Security, February 9, 2017, https://www.justsecurity.org/37559/.
[4] Tallinn Manual 2.0 (Schmitt, ed.) , 20–24.

However, the experts were divided on whether all unauthorized intrusions, such as data exfiltration or cyber espionage, automatically constitute violations of sovereignty.[1] This reflects a broader ambiguity in international law regarding the threshold at which cyber operations become internationally wrongful acts, an issue that continues to be debated by states and scholars alike.

Another significant contribution of the manual lies in its analysis of the **principle of non-intervention**. Rule 66 affirms that cyber operations that interfere with the internal or external affairs of a state in areas traditionally within its domaineréservé—such as elections or the functioning of public institutions—may constitute unlawful intervention.[2] However, the manual also notes that economic coercion and propaganda are generally not prohibited under this principle unless they rise to the level of coercive interference.[3] This distinction has practical implications in assessing state responsibility for operations like misinformation campaigns, election meddling, or cyber-enabled economic sabotage.

Due diligence is another contested area addressed by the manual. Rule 6 provides that states have an obligation not to knowingly allow their territory to be used for cyber operations that harm the rights of other states.[4] While this rule is rooted in established international jurisprudence, including the *Corfu Channel* case, the extent of this obligation and its enforceability in the cyber context remain uncertain.[5] Notably, few states have explicitly endorsed the due diligence obligation in official statements, although

[1] Tallinn Manual 2.0 (Schmitt, ed.) , 25–28.
[2] Ibid., 318–323.
[3] Ibid., 327–329.
[4] Ibid., 35–37.
[5] International Court of Justice, Corfu Channel Case (UK v. Albania), ICJ Reports 1949, 4.

some—including the Netherlands and France—have acknowledged it in their national cyber postures.[1]

The **attribution of cyber operations to states** is a recurring challenge in cyber law, and Tallinn Manual 2.0 reflects this complexity. It applies the **Articles on State Responsibility** adopted by the International Law Commission (ILC), focusing on whether cyber operations are carried out by state organs, entities acting under state control, or non-state actors whose actions are later adopted by a state.[2] However, the manual acknowledges that attribution in the cyber realm is technically difficult, politically sensitive, and often lacks publicly available evidence. This has led to a cautious approach by many governments, with relatively few cases of explicit state attribution to date.[3]

The manual also explores how **international human rights law (IHRL)** applies to cyber operations. It affirms that states have human rights obligations in cyberspace, including the rights to privacy, freedom of expression, and access to information.[4] Yet the application of IHRL to cyber surveillance, data retention, and internet shutdowns remains controversial, particularly with regard to extraterritorial obligations and private-sector involvement. The Tallinn Manual does not resolve these disputes but provides a structured legal framework for analysis and debate.

Despite its academic nature and lack of formal legal authority, the **Tallinn Manual 2.0** has had a significant impact on cyber diplomacy and norm development. It has been referenced in national cybersecurity

[1] Government of the Netherlands, "Appendix: International Law in Cyberspace," May 2019, https://www.government.nl/documents.
[2] Schmitt, Tallinn Manual 2.0, 43–50.
[3] Duncan B. Hollis, "Why State Attribution Is So Difficult," Lawfare, May 28, 2021, https://www.lawfareblog.com/why-state-attribution-so-difficult.
[4] Schmitt, Tallinn Manual 2.0, 578–582

strategies, government statements, and international dialogues, including the UN Group of Governmental Experts and Open-Ended Working Group processes.[1] While some states, notably Russia and China, criticize it as reflecting a Western-centric legal perspective, others see it as a valuable tool for clarifying legal ambiguities and fostering greater predictability in state behavior.

1.1 Alternative Normative Frameworks in Global Cyber Governance

The fragmentation of global cyber governance has led to the proliferation of **alternative normative frameworks** advanced by different political, regional, and ideological blocs. While the United Nations processes—such as the Group of Governmental Experts (GGE) and Open-Ended Working Group (OEWG)—have yielded consensus on certain voluntary norms, several states have sought to assert their own visions of cyberspace through separate declarations, rules, and coalitions. These competing frameworks reflect fundamental divergences in how states view sovereignty, information control, surveillance, and the role of international law in cyberspace.

One of the key features of this fragmentation is the emergence of **regional or alliance-based cyber doctrines**, which seek to reinterpret or supplement existing international law. The **Tallinn Manual**, though influential in Western academic and strategic circles, is often viewed with skepticism by states such as China and Russia, who argue that it represents a Western-centric, militarized interpretation of cyberspace law.[2] In response, states in the Global South and East have developed **counter-narratives** that

[1] United Nations GA Report, *A/76/135 (2021).*
[2] Michael N. Schmitt, "The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: What It Is and Isn't," Just Security, February 9, 2017, https://www.justsecurity.org/37559/.

emphasize different priorities, such as state sovereignty, information control, and cultural relativism in human rights interpretation.

For example, China, Russia, and several allied states have repeatedly advocated for a **new international legal instrument** on information security within the framework of the United Nations.[1] This push is grounded in a desire to shift the normative debate away from voluntary, non-binding norms and toward a treaty-based approach centered on state control of digital information and network sovereignty. These efforts gained traction through initiatives such as the **Shanghai Cooperation Organisation's (SCO) 2015 rules of conduct** in cyberspace, which promote state-centric cyber governance and restrict content that threatens "social stability" or "national security."[2]

In contrast, Western-aligned states have supported normative frameworks that emphasize **a free, open, and secure internet**, often grounded in liberal principles such as transparency, multistakeholderism, and the protection of individual rights. The **Paris Call for Trust and Security in Cyberspace (2018)** is one such example. Spearheaded by France and endorsed by over 70 countries, it promotes cooperation across governments, private sector actors, and civil society in addressing cyber threats, disinformation, and election interference.[3] Although non-binding, the Paris Call signals a push toward inclusive governance and ethical behavior in cyberspace, standing in clear contrast to more restrictive models.

[1] United Nations General Assembly, Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General, A/69/723, January 13, 2015, https://undocs.org/A/69/723.
[2] SCO, *International Code of Conduct for Info Security.*
[3] Paris Call (France).

These parallel initiatives underscore a deeper struggle over **normative leadership in cyberspace**, where cyber governance is not merely a matter of legal codification, but also of **geopolitical alignment** and **ideological contestation**. The existence of multiple, often incompatible frameworks risks undermining efforts at universal norm convergence and raises concerns about **splinternet dynamics**, where competing standards could lead to fragmentation of the global internet.[1]

2. Paris Rules (2018) and Shanghai Rules (2015)

In the absence of a binding international treaty on state conduct in cyberspace, several normative frameworks have emerged from regional or multilateral initiatives, reflecting divergent geopolitical visions. Among the most influential are the **Paris Call for Trust and Security in Cyberspace (2018)**, proposed by France and supported by liberal democratic states and non-state actors, and the **International Code of Conduct for Information Security (2015)**, proposed by member states of the **Shanghai Cooperation Organisation (SCO)**, including China and Russia. These frameworks offer competing principles and priorities in cyber governance, highlighting the ideological and strategic fault lines that shape global cyberspace policy.

The **Paris Call**, launched on November 12, 2018, by French President Emmanuel Macron, is a **voluntary, non-binding** initiative that seeks to promote a shared commitment to international norms and rules in cyberspace.[2] It emphasizes the protection of human rights online, the application of existing international law to cyber operations, and multistakeholder cooperation to prevent malicious activities. The Call has

[1] Kubo Mačák, "Fragmentation and Cyber Norms: Between Universalism and Regionalism," in Research Handbook on International Law and Cyberspace, ed. Nicholas Tsagourias and Russell Buchan (Edward Elgar, 2021), 193–212.
[2] Paris Call (France).

garnered endorsements from over **1,200 entities**, including more than 80 states (primarily Western democracies), hundreds of private companies, and civil society organizations.[1] Its key principles include defending the integrity of the internet, preventing election interference, combating cybercrime, and fostering digital trust.

Notably, the Paris Call promotes a **multistakeholder approach**, urging collaboration among governments, the private sector, technical communities, and civil society.[2] This inclusion reflects Western liberal values, in contrast to state-centric models of governance. Moreover, the Call reaffirms the **applicability of international humanitarian law (IHL) and international human rights law (IHRL)** to cyberspace, supporting the idea that existing legal frameworks are sufficient for regulating cyber operations—a position aligned with the Tallinn Manual and the United Nations GGE.[3]

On the other hand, the **Shanghai Rules**—formally known as the **International Code of Conduct for Information Security**—reflect a **state-centric, sovereignty-focused** vision of cyberspace governance. First proposed to the UN General Assembly in 2011 and updated in 2015, the Code was endorsed by China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan, all members of the SCO.[4] It calls for strict adherence to the principle of **non-interference in the internal affairs of other states**, framing cyberspace not only as a technical space but also as an arena of ideological and political stability.

[1] Microsoft, "The Paris Call for Trust and Security in Cyberspace," 2023, https://www.microsoft.com/en-us/cybersecurity/paris-call.
[2] Paul Meyer, "The Paris Call for Trust and Security in Cyberspace: A Multistakeholder Normative Response to Malicious Cyber Activity," Cybersecurity and Global Affairs Journal 5, no. 1 (2020): 11–16.
[3] United Nations GA Report, *A/70/174 (2015).*
[4] UN GA Letter A/69/723 (2015).

The Shanghai Code emphasizes the right of states to **regulate content, control information flows**, and safeguard "political, economic, social, and cultural stability."[1] Unlike the Paris Call, which supports openness and transparency, the Shanghai Rules highlight **information sovereignty**, a concept that allows states to control the dissemination of content within their territories. This model legitimizes content-based restrictions and national firewalls, such as China's Great Firewall, under the guise of national security and public order.[2]

Moreover, the Code calls for an international agreement or **legal instrument** on information security, advocating for new binding rules to regulate cyberspace, particularly in areas such as cybercrime, cyberterrorism, and the misuse of information technologies to destabilize societies.[3] This push diverges from the Western view that existing international law is sufficient, signaling a fundamental disagreement over the need to codify new global treaties in cyberspace governance.

These two frameworks—**Paris and Shanghai**—epitomize the broader contest between **liberal internationalist** and **sovereigntist authoritarian** approaches to global cyber governance. The Paris Call aligns with the norms promoted by the UN GGE and OEWG, reinforcing consensus on voluntary principles and accountability, while the Shanghai Rules challenge this normative consensus by asserting a different conception of cyber threats,

[1] SCO, *International Code of Conduct for Info Security*.
[2] James A. Lewis, "Sovereignty and the Role of Government in Cyberspace," Center for Strategic and International Studies, July 2021, https://www.csis.org.
[3] Ibid.

focused less on infrastructure attacks and more on **content and ideological security**.[1]

The practical implications of these competing visions are significant. While the Paris Call encourages **transparency, restraint, and cross-sector cooperation**, the Shanghai Rules justify **state surveillance, censorship, and the restriction of civil liberties** in cyberspace. These divergences have contributed to the **polarization of international cyber diplomacy**, complicating the development of a unified global framework for cyberspace governance.[2] Furthermore, they raise the specter of **cyber "balkanization"**, in which regional blocs follow incompatible regulatory models, threatening the integrity and interoperability of the global internet.

In conclusion, the Paris and Shanghai frameworks are more than normative texts; they represent **strategic blueprints for the future of cyberspace**. As digital technologies become more deeply embedded in global politics and security, the contest between these models will shape not only how cyber threats are addressed, but also the values that govern the digital age.

[1] Elaine Korzak, "Norms in Cyberspace: The SCO Code of Conduct," in Global Cybersecurity Norms, ed. Patryk Pawlak (EU Institute for Security Studies, 2017), 48–52.
[2] Tim Maurer, *Cyber Mercenaries, 157.*

General Conclusion

This thesis has examined the complex and evolving field of international protection of cyberspace, with a specific focus on how to balance national sovereignty with the collective need for global cybersecurity. In the digital age, cyberspace transcends physical borders, introducing novel challenges for international law and cooperation, particularly in addressing transnational threats, cross-border jurisdiction, and the responsibilities of states in ensuring the security of their digital infrastructure.

The first chapter of the thesis laid out the conceptual framework, beginning with an in-depth discussion of cyberspace and cybersecurity. It highlighted the unique characteristics of cyberspace as a domain without borders, encompassing physical, logical, and human elements. The chapter further explored the scope and impact of cyber threats on national and international security. It became clear that the borderless nature of cyberspace allows both state and non-state actors to carry out disruptive or harmful actions with limited accountability, thereby amplifying concerns related to sovereignty and national security.

The second chapter investigated the international legal framework governing cyberspace. It analyzed the role of the United Nations and various regional organizations in building a governance model for international cybersecurity. The chapter addressed the progress made through initiatives such as the UN Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG), both of which confirmed the applicability of international law to cyberspace. However, the discussions also revealed

persistent geopolitical divides and a lack of consensus on binding rules, which limits the effectiveness of international regulatory efforts.

Regional approaches were also examined, including frameworks developed by the European Union, the African Union, the Shanghai Cooperation Organisation, and the Organization of American States. These initiatives provide important regional responses to global cyber risks, though they sometimes diverge in normative orientation, which may lead to fragmentation of global standards.

The thesis found that, while international law provides a general framework applicable to cyberspace, further clarification is required in key areas such as state responsibility, due diligence, and proportionality. It also became evident that voluntary norms and regional agreements are useful tools for building trust and cooperation, though they cannot substitute for binding legal instruments. Another major challenge is the disparity in technological capabilities between states, which hinders equal participation in international cybersecurity efforts and raises concerns about digital divides.

In summary, this research affirms that the protection of cyberspace at the international level requires a cooperative, inclusive, and legally grounded approach. States must work within a framework that respects sovereignty but also acknowledges the interconnected nature of cyber threats. The evolving governance of cyberspace illustrates the need for continual dialogue, norm development, and enhanced legal coherence, both globally and regionally.

References

Access Now. "Russia's Sovereign Internet Is a Model for Censorship." April 7, 2021. https://www.accessnow.org/russia-sovereign-internet-censorship/.

African Union. *African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)*. 2014. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

Amnesty International. "Forensic Methodology Report: How to Catch Pegasus." July 18, 2021. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-pegasus/.

Bradshaw, Samantha, and Laura DeNardis. "The Governance of Cybersecurity: Institutions, Norms and Power." In *The Oxford Handbook of Cybersecurity*, edited by Paul Cornish, 423. Oxford: Oxford University Press, 2021.

Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*. O'Reilly Media, 2011.

Center for Strategic and International Studies (CSIS). *Significant Cyber Incidents Since 2006*. Updated 2024. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

CISA (Cybersecurity and Infrastructure Security Agency). "Cyber Essentials." https://www.cisa.gov/cyber-essentials.

CISA. "Cyber Information Sharing and Collaboration Program (CISCP)." https://www.cisa.gov/cyber-information-sharing-collaboration-program.

CISA. "DarkSide Ransomware: Best Practices for Preventing Business Disruption." May 2021.

Coleman, Gabriella. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous.* London: Verso, 2014.

Deibert, Ronald J. *Black Code: Inside the Battle for Cyberspace.* Toronto: Signal, 2013.

Deibert, Ronald J. *Reset: Reclaiming the Internet for Civil Society.* Toronto: House of Anansi, 2020.

DeNardis, Laura. *The Global War for Internet Governance.* New Haven: Yale University Press, 2014.

European Commission. "EU Cybersecurity Strategy for the Digital Decade." 2020. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

European Commission. "General Data Protection Regulation (GDPR)." https://ec.europa.eu/info/law/law-topic/data-protection_en.

European Parliament and Council. *General Data Protection Regulation*, Regulation (EU) 2016/679.

FireEye. "APT33: Cyber Espionage Group Linked to Iran." September 2017. https://www.fireeye.com/blog/threat-research/2017/09/apt33-cyber-espionage-group.html.

Freedom House. "Iran." *Freedom on the Net 2022*. https://freedomhouse.org/country/iran/freedom-net/2022.

Gellman, Barton. *Dark Mirror: Edward Snowden and the American Surveillance State.* New York: Penguin Press, 2020.

Greenberg, Andy. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers.* New York: Doubleday, 2019.

Greenwald, Glenn. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State.* New York: Metropolitan Books, 2014.

Healey, Jason, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.* Vienna, VA: Cyber Conflict Studies Association, 2013.

ITU (International Telecommunication Union). "Capacity Building in Africa." 2022. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx.

Krebs, Brian. "KrebsOnSecurity Hit with Record DDoS." *Krebs on Security*, September 21, 2016. https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/.

Lessig, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.

Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge: Cambridge University Press, 2018.

Microsoft. "Digital Geneva Convention." https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

Mueller, Milton. *Networks and States: The Global Politics of Internet Governance.* Cambridge, MA: MIT Press, 2010.

Mueller, Milton. *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace.* Cambridge: Polity Press, 2017.

National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.* Gaithersburg, MD: NIST, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Nye, Joseph S. "Deterrence and Dissuasion in Cyberspace." *International Security* 41, no. 3 (2017): 44–71.

OECD. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* 2013. https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

Rid, Thomas. *Cyber War Will Not Take Place.* Oxford: Oxford University Press, 2013.

Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

Singer, P. W., and Emerson T. Brooking. *LikeWar: The Weaponization of Social Media.* Boston: Houghton Mifflin Harcourt, 2018.

United Nations. *Final Substantive Report of the Open-Ended Working Group on Developments in the Field of ICTs.* A/75/816. March 2021. https://documents.un.org.

United Nations. *International Covenant on Civil and Political Rights*. 1966. Articles 17 and 19. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

United Nations. *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace*. A/76/135 (2021). https://undocs.org/A/76/135.

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* New York: Crown Publishing, 2014.

Zuboff, Shoshana. *The Age of Surveillance Capitalism.* New York: PublicAffairs, 2019.

مــلخص مذكرة الماستر

أدى التطور السريع في الفضاء السيبراني إلى تغيير طبيعة العلاقات بين الدول، لكنه أثار تحديات كبيرة تتعلق بحماية السيادة الوطنية وضمان الأمن السيبراني العالمي. تهدف هذه الدراسة إلى البحث في كيفية تحقيق التوازن بين حماية سيادة الدولة وتعزيز التعاون الدولي في مجال الأمن السيبراني. يتم تحليل الأطر القانونية القائمة، خاصة تلك التي وضعتها الأمم المتحدة والمنظمات الإقليمية، لمعرفة مدى كفايتها في مواجهة التهديدات السيبرانية المتزايدة. توصلت الدراسة إلى أن التعاون الدولي ضروري، لكنه يتطلب وضوحاً قانونياً وثقة متبادلة وحواراً متعدد الأطراف لتحقيق استقرار طويل الأمد في الفضاء الرقمي.

الكلمات المفتاحية:
1/ الفضاء السيبراني 2/ الأمن السيبراني
3/ القانون الدولي 4/ السيادة
5/ التهديدات السيبرانية 6/ التعاون الدولي

Abstract of Master’s Thesis

The rapid growth of cyberspace has reshaped international relations but also raised serious concerns about national sovereignty and global cybersecurity. This study explores how to balance the protection of state sovereignty with the need for international cooperation to counter cyber threats. It examines whether current legal frameworks—especially those of the United Nations and regional bodies—are adequate for ensuring cybersecurity. The findings highlight the need for legal clarity, trust, and inclusive dialogue to achieve lasting digital stability.

Keywords:
1/ Cyberspace 2/ Cybersecurity 3/ International Law
4/ Sovereignty 5/ Cyber Threats 6/ International Cooperation