CYBER AND TECHNOLOGICAL SECURITY IN INTERNATIONAL RELATIONS: IMPACT OF CYBERATTACKS, DATA PRIVACY, AND MISINFORMATION ON NATIONAL AND GLOBAL STABILITY

Ms. Khushboo Farid Khan Ghouri
Lecturer Science & Humanities
FAST-National University of Computer & Emerging Sciences
Karachi - Pakistan
khushboo.farid@nu.edu.pk

Dr. Nausheen Wasi
Assistant Professor
University of Karachi
Karachi - Pakistan
nwasi@uok.edu.pk

Abstract:

The rapid evolution of cyberspace and digital technologies has transformed the landscape of international relations, redefining the concepts of security, sovereignty, and social stability. This paper explores the multifaceted impact of cyber and technological security challenges, such as cyberattacks, data privacy concerns, and digital misinformation, at individual, national, and global levels. It examines how cyberattacks threaten national security by targeting critical infrastructure, influencing elections, and increasing the risk of cyber warfare, with geopolitical consequences that extend beyond borders. At the societal level, digital misinformation campaigns erode public trust, polarize communities, and distort democratic processes, while data privacy concerns raise pressing questions about surveillance and individual rights. The study also investigates the intersection of these cyber threats with global power dynamics, highlighting how states leverage cyber capabilities to gain strategic advantages, manipulate information, and challenge traditional notions of sovereignty. By analysing real-world cases and recent cyber conflicts, this paper underscores the urgent need for inclusive global cooperation, enhanced cybersecurity frameworks, and the establishment of international norms to mitigate the risks posed by technological vulnerabilities. Ultimately, it argues that cyber and technological security has become a central component of modern international relations, with far-reaching implications for peace, security, and global governance in the digital era. This research is part of my Ph.D. dissertation and contributes to the broader thesis titled: Emerging

Technologies and International Relations: Understanding the Future Threat Potential of Great Power Competition in the Scramble for Skies.

Key Words: *Cyber Security, Cyberattacks, Digital Misinformation, Data Privacy, Great Powers Rivalry*

I. INRODUCTION

The rapid advancements in digital technologies and the expansion of cyberspace have fundamentally reshaped the world of international relations, transforming traditional concepts of security, sovereignty, and global governance. As nations increasingly rely on interconnected digital networks, cyber threats have emerged as a prominent issue, presenting new risks that extend beyond the confines of national borders. Cyberattacks, data privacy violations, and misinformation campaigns now constitute major security challenges for states, businesses, and individuals alike, with the potential to destabilize national security, undermine democratic processes, and disrupt international relations (Singer & Friedman, 2014).

In the digital age, cyber vulnerabilities not only expose critical infrastructure to attacks but also affect geopolitical stability by influencing elections, amplifying disinformation, and eroding public trust (Rid, 2020). As global power dynamics shift, the capacity to wield cyber capabilities has become a new measure of state power, prompting an urgent need to understand how cyber threats impact national and international stability.

This research is highly significant in today's digitally interconnected world, where cyberspace has become a critical arena of geopolitical competition and national defense. As states increasingly face threats from cyberattacks, data breaches, and disinformation, the traditional frameworks of security, sovereignty, and global governance are being fundamentally challenged (Nye, 2010). This study provides an analysis of how such cyber threats not only jeopardize national infrastructure and data privacy but also polarize societies and disrupt democratic systems (Rid, 2020). Contributing to the broader academic discourse on emerging technologies and great power competition, this research enhances our understanding of the digital transformation of international relations and the critical role of cyber power in shaping the global order.

While significant research exists on cybersecurity and technological threats, there is a growing need to address how cyberattacks, digital misinformation, and data privacy concerns intersect with international power dynamics and sovereignty. Many studies tend to examine these issues in isolation rather than comprehensively exploring their broader implications for global stability. Existing frameworks for international cybersecurity cooperation remain fragmented and inadequate to address the scope and scale of these challenges (Tikk, 2018).

This study is grounded in the *Theory of Securitization*, developed by the Copenhagen School of International Relations, particularly scholars like Barry Buzan, Ole Wæver, and Jaap de Wilde.

Securitization theory provides a valuable lens to understand how issues are framed as existential threats requiring extraordinary measures, moving them from the realm of normal politics into emergency politics (Buzan, Wæver, & de Wilde, 1998).

In the context of cyber and technological security, the securitization framework helps explain how states label cyberattacks, data privacy breaches, and digital misinformation as threats to national sovereignty, public safety, and democratic governance. Once these issues are securitized, typically by political leaders, security agencies, or influential actors, they legitimize exceptional responses such as surveillance, militarization of cyberspace, and international cooperation on cybersecurity. This theoretical approach is crucial for examining how cybersecurity and emerging technologies have become central to national and international security discourse, especially in the wake of high-profile incidents like ransomware attacks on critical infrastructure, election interference, and cyber espionage operations. It also helps analyse the political processes and power dynamics involved in labelling certain cyber activities as 'threats', and how such framing influences international norms, laws, and diplomatic relations. Furthermore, this research applies securitization theory to compare how different states, such as the U.S., China, Russia, and India, construct and respond to cyber threats, reflecting their unique political contexts, strategic goals, and positions in the global order.

Moreover, despite the increasing attention to cyber conflicts, the regional focus, particularly concerning South Asia, remains underdeveloped. The relationship between cyber threats and regional power struggles, particularly in sensitive areas like Pakistan and India, has yet to be fully explored. This research aims to fill these gaps by examining the intersection of cyber threats and geopolitical power, with a focus on regional stability in South Asia and its implications for global security.

1. To analyse the impact of cyberattacks, data privacy breaches, and digital misinformation on national security and international relations.
2. To explore how cyber threats influence geopolitical power dynamics and challenge traditional notions of sovereignty.
3. To assess the state of cybersecurity frameworks and propose international cooperation measures to mitigate cyber threats.
4. To evaluate the implications of cyber threats for regional stability in South Asia, particularly in the context of Pakistan and India.

The following questions will be raised and responded to in this research paper.

1. Why are states striving to excel and dominate in cyberspace, and how does this influence global power struggles?
2. How do cyberattacks and data privacy concerns affect national security and the stability of international relations?
3. In what ways do misinformation campaigns disrupt democratic processes and polarize societies?
4. How can states leverage cyber capabilities to gain a competitive geopolitical advantage?

5. What international cybersecurity frameworks are needed to address the growing cyber threat landscape?

Hypothesis:

The increasing prevalence of cyberattacks, digital misinformation, and data privacy breaches poses significant risks to national security and global stability. The lack of comprehensive international cybersecurity frameworks exacerbates these risks, leading to regional power struggles, particularly in conflict-prone areas.

II. LITERATURE REVIEW

The literature on cyber and technological security highlights the growing complexity of threats posed by cyberattacks, misinformation, and data privacy breaches. Scholars such as Singer and Friedman (2014) argue that cyber threats have become a crucial dimension of modern warfare, affecting both state and non-state actors. Rid (2020) further elaborates on the impact of cyberattacks on national security, particularly focusing on how cyber incidents have been used to influence elections, hack critical infrastructure, and launch espionage campaigns.

Available literature also examines how cyber threats, including attacks on critical infrastructure, digital misinformation, and data privacy/surveillance issues, affect national and international security. The analysis combines theoretical insights with empirical cases and emphasizes impacts on international relations, state sovereignty, and emerging security norms.

Cyberattacks on Infrastructure

Critical infrastructure (power grids, water systems, transportation, etc.) is deeply networked today, making it vulnerable to cyber disruption. Early analysts warned that malware targeting industrial control systems could cause physical damage and crisis. For example, a U.S. Congress report explained that the Stuxnet worm (2010) was designed to "degrade or destroy" software controlling Iran's nuclear facilities, illustrating how cyber weapons can render critical systems inoperable.

Kerr et al. (2010) argue that such attacks "could result in manipulation of control system code to the point of inoperability or long-term damage," potentially leaving civilians "without life sustaining…services" and threatening national security(Congressional Research Service, 2010). Other pre-2015 works, such as Clarke and Knake (2010), raised similar alarms about a potential "cyber Pearl Harbor" on infrastructure. Empirical cases in the 2015–2025 period confirm these risks. Notably, U.S. analysts report that Russia's GRU orchestrated cyberattacks on Ukraine's power grid in 2015–2016. These attacks used BlackEnergy malware delivered via spear-phishing, destroying computers and disrupting Supervisory Control and Data Acquisition (SCADA) systems at multiple regional utilities (Congressional Research Service, 2024). In one incident, Ukrainian operators manually restored power after breaker controls were taken over by the attackers. More recently, the 2022 Russian invasion of Ukraine included further cyber strikes on electricity and communications (Humphreys, 2024). Other infrastructure attacks have occurred globally: examples include the 2012 Shamoon malware that crippled Saudi Aramco, ransomware shutdowns of US pipelines in 2021,

and water plant hacks in Florida (2021). These cases underscore that sophisticated cyberattacks on energy, water, and transport can cause widespread economic and safety impacts (Humphreys, 2024; Kerr et al., 2010).

The literature emphasizes that cyberattacks on infrastructure are not purely technical incidents but also strategic acts. In IR terms, a cross-border cyber strike on critical systems can be viewed as a violation of sovereignty akin to aggression. States have begun treating such attacks as national security events. For example, the Ukrainian government labelled the 2015 grid attacks as hostile acts by Russia (Humphreys, 2024). This raises questions of deterrence and international law: if a cyberattack knocks out power for hundreds of thousands, is it an act of war? Analysts note that international legal norms (e.g. the Tallinn Manual) are still evolving for cyber warfare, but states are already invoking sovereignty and self-defence in cyberspace (Chatham House, 2019). In sum, critical-infrastructure attacks have become a global security concern: countries must protect "national assets" and may face international repercussions if attributed (Kerr et al., 2010; Humphreys, 2024).

Moreover, digital misinformation (falsehoods spread on social media) and disinformation (state-sponsored falsehoods) have emerged as major security issues. With the rise of Facebook, Twitter, and messaging apps, scholars note that social media is now a primary channel for news and political discourse(Woolley & Howard, 2017). This connectivity has also enabled malicious actors to manipulate public opinion. In foundational research, Allcott and Gentzkow (2017) studied the 2016 U.S. election and documented how "fake news" stories were widely shared online, although they initially found limited impact. Subsequent works broaden this view: the Oxford Internet Institute's "computational propaganda" project (Woolley & Howard, 2017) finds that social platforms have been exploited by both autocracies and democracies to spread targeted misinformation (e.g. via bots and trolls). Bradshaw and Howard (2018) summarize that young people worldwide often get political news on social media, where it can be amplified by automated accounts. They report that "political bots…have been used to manipulate online discussion" in many countries. Gerrits (2018) examines the strategic use of disinformation in international relations and its growing impact on global security. In short, scholars agree that digital misinformation is a global phenomenon affecting diverse contexts (Brazil, Russia, India, etc.).

Channels like Facebook, Twitter, WhatsApp, YouTube, state news outlets are use in order to spread misinformation. Many cases involve social-media platforms with large local usage. While actors like State agents and proxies (e.g. Russian troll farms, Chinese cyber armies), partisan groups, and increasingly, non-state "troll farm" entrepreneurs are involved. Both authoritarian regimes and political campaigns in democracies use micro-targeting and bots. For instance, Russian interference in the 2016 U.S. election; disinformation around the 2017 French election; manipulation of Philippine and Indian elections via social media; COVID-19 falsehoods spread by various state-linked networks.

These campaigns have significant political effects. They can deepen polarization, erode trust in institutions, and skew public perceptions. Internationally, misinformation has strained state relations. For example, U.S. intelligence accused Russian entities of "weaponizing" information to influence foreign politics(Gerrits, 2018). States have responded with sanctions, indictments, and new laws (e.g. countering foreign election interference), reflecting the view that foreign disinformation can violate sovereignty. However, some scholars caution that while disinformation is disruptive, it "parasites on existing divisions" and has not (yet) fundamentally altered great-power balances. Still, others warn it is "an incisive instrument of state policy" that operates at all levels of government strategy. In summary, the academic consensus is that digital misinformation has become a security issue worldwide – a tool of modern "hybrid warfare" – and has prompted debates on protecting electoral integrity and free speech in an interconnected world (Woolley & Howard, 2017; Bjola & Pamment, 2019).

Furthermore, data privacy concerns and surveillance practices form the third major cyber threat impacting security. The tension between protecting citizens and invading privacy predates the internet, but has intensified with big data and global networks. Foundational studies (Regan, 2001) recognized that expanded government surveillance can undermine civil liberties. The Snowden revelations (2013) dramatically exposed the scale of NSA and allied surveillance, sparking a wave of research on privacy vs. security. In response, many countries have tightened data protection laws. For instance, the EU's 2018 General Data Protection Regulation (GDPR) enshrines citizens' rights over personal data, reflecting a strong norm of individual privacy. In contrast, other governments prioritize state security: China explicitly asserts "cyber sovereignty," granting itself broad power to control all digital content and data within its borders. Rogier Creemers (2020) notes that Beijing's vision is "state-centered, Westphalian," whereby each country has the right to "establish national online spaces and fully control content and data flows"(Creemers, 2020, p. 3). Many developing states (Brazil, India, and Russia) have also pursued data localization policies for similar reasons.

Global data governance is shaped by regional regulations such as the EU's GDPR, China's Cybersecurity and Personal Information Protection Laws, India's proposed Personal Data Bill, and U.S. sectoral laws like HIPAA, while technologies like the U.S.-UK "Five Eyes" surveillance alliance, China's social-credit and censorship systems, and corporate data harvesting (e.g., the 2018 Cambridge Analytica scandal) illustrate the ongoing tension between privacy and security, where governments argue surveillance ensures stability, but critics caution it fosters coercion and undermines public trust. Richards (2013) argues that surveillance threatens intellectual privacy and democratic freedom, calling for legal frameworks that treat surveillance as a civil liberties issue.

The international dimension is significant. Cross-border data flows are essential for commerce and cyber defines, yet are increasingly constrained by privacy and security laws. Scholars like Kuner (2015) have documented how transnational data-sharing regimes (e.g. EU-US Privacy Shield) face tension when national security is at stake. For example, U.S. intelligence requests for data stored overseas can clash with European privacy rules, leading to legal and diplomatic disputes. China's

emphasis on cyber sovereignty has realigned global norms: Western-led forums promoting free information flow have had to accommodate Chinese demands for border controls (Creemers, 2020). Even democratic states are grappling with this: some EU officials lament a "Brussels effect" in which GDPR expands privacy norms globally, while others see rising authoritarian data-controls. In sum, the scholarship shows that data privacy and surveillance are reshaping notions of sovereignty. Cybersecurity is no longer just technical; it now involves competing visions of state power and citizen rights, with implications for trade, diplomacy, and human rights.

Across all threat categories, cyber issues profoundly affect international relations and security norms. At the strategic level, states are revising doctrines and forging alliances. The reality that a cyberattack on energy grids or communications can originate from abroad has led countries to treat certain cyber intrusions as breaches of sovereignty or even acts of force. This is visible in new policies (e.g. cyber defense pacts in NATO, attribution of attacks as hostile acts) and in calls to update international law. Global institutions are responding: the United Nations and NATO have initiated discussions on "cyber norms," such as non-intervention in electoral processes, protection of civilian infrastructure, and transparency in surveillance. For instance, studies note that information manipulation now functions as "an instrument of foreign policy," often grouped under broad "hybrid warfare" concepts (Gerrits, 2018).

Diplomats have begun to agree (or contest) principles like limiting state-sponsored disinformation, and advocating for a balance between internet freedom and national security. In practice, cyber threats are putting strain on state sovereignty and alliances. Western democracies emphasize free flow of information and cross-border cooperation on cybercrime. Authoritarian states emphasize control and domestic enforcement (e.g. China's Great Firewall, Russia's sovereign Internet law). These divergent models are creating tensions in trade negotiations and international bodies. The literature highlights that cyber challenges are globalizing security debates: liberal norms (e.g. human rights online) are being tested against realist impulses (state control). While consensus is still emerging, scholars agree that the era of relatively open cyberspace is giving way to contested "digital order." In sum, cyber threats like those reviewed here have driven a reevaluation of sovereignty and international norms, compelling states to define acceptable cyber behavior and to collaborate (or compete) on a new domain of security (Creemers, 2020; Bjola & Pamment, 2019).

III. RESEARCH METHODOLOGY

This research adopts a qualitative approach to analyse the multifaceted impact of cyber threats on national and international stability. The study relies primarily on official documents such as government reports, national cybersecurity strategies, and international conventions, which serve as the main sources of primary data. For secondary data, scholarly articles, academic journals, research papers, and think tank publications are thoroughly reviewed to support theoretical grounding and contextual understanding. The methodology includes content analysis of relevant policy documents and cybersecurity frameworks to assess how various states respond to cyber threats. A comparative analysis is conducted to examine the cybersecurity strategies and geopolitical behaviour of major

global actors, including the United States, China, Russia, and India, with a focus on how they utilize cyber capabilities to assert influence in international relations. Additionally, key real-world incidents—such as ransomware attacks, cyber espionage campaigns, and misinformation tactics employed during elections in the United States, India, and Pakistan—are explored to demonstrate the tangible implications of cyber insecurity. This comprehensive qualitative methodology allows for an in-depth understanding of how cyber threats are reshaping modern international relations and contributing to evolving security paradigms.

Nonetheless, early debates to integrate cyberspace with broader concepts and theories of International Relations (IR) have started to move from the periphery to the core of the discipline (Dunn Cavelty, 2020; Gartzke & Lindsay, 2024). However, this engagement tends to focus on particular aspects of cyberspace: its use in war or deterrence, its combination with other tools in particular states' foreign policies, and so forth. But theorization remains nascent in the sense that how International Relations as discipline has struggled to formulate broader policy. This is partially because cyber scholarship in IR has lacked the theoretical tools to do so.

Moreover, most of the cyberspace debate in IR has occurred against the backdrop of cyberspace understood as a domain through which actors conduct cyber operations against other actors. Some scholars explain how cyber operations revolutionize the practice of international relations concerning deterrence or war. However, the debate about cyberspace as a domain is challenged by scholars who argue that cyberspace does something different in terms of interconnection: it shapes all states' behavior across international relations (Brantley, 2018; Buchanan, 2016; Fischerkeller et al., 2022; Gartzke & Lindsay, 2024; Kello, 2017, 2022; Kreps & Schneider, 2019; Libicki, 2007; Lindsay, 2020; E. D. Lonergan & Schneider, 2023; Maschmeyer, 2023; Smeets, 2022).

These scholars have started to develop theories about the circumstances under which cyberspace matters in international relations, how actors shape the cyber domain, and how the cyber domain in turn influences actors' interaction capacity.
While this literature is promising, it suffers from two key problems:

- It has received relatively little attention as a collective body of work, and
- It has overlooked the policy and theoretical potential of further integrating cyberspace with IR theory and concepts.

IV. FINDINGS/RESULTS

Preliminary findings indicate that cyber threats have profound implications for national security and international relations. Cyberattacks on critical infrastructure pose significant risks to economic stability and governance, while misinformation campaigns have been found to weaken democratic processes by polarizing societies (Rid, 2020). In South Asia, the rivalry between India and Pakistan has been exacerbated by cyber espionage and misinformation tactics, raising concerns about regional stability (Chaudhary & Dickson, 2022). Additionally, the lack of cohesive international cybersecurity frameworks has left many states vulnerable to cyber threats, prompting a need for

enhanced global cooperation.

Moreover, recent evidence shows that cyberspace has become a central arena of strategic competition. Major Powers explicitly pursue cyber dominance as a component of national security and power projection. For example, two-thirds of global experts anticipate a fragmented, multipolar order in which states contest new rules of cyberspace(World Economic Forum, 2024). In practice, nations are investing heavily in offensive and defensive cyber capabilities to augment their geopolitical leverage (KnowBe4, 2024). According to the report Cyber operations, ranging from sophisticated espionage to offensive attacks, are treated by states as an extension of traditional power tools. As one industry analyst notes, adversaries "have made [attacks on infrastructure] a powerful addition to their arsenal of digital weapons". These developments underscore that cyber superiority is now viewed as necessary for great-power competition and deterrence. Cyberattacks on critical infrastructure are sharply affecting economic and governance stability. Recent reports document a dramatic surge in such attacks. For instance, utilities worldwide experienced over 420 million cyberattacks in a one-year period (Jan 2023–Jan 2024), roughly 13 attacks per second, a ~30% rise over the previous year. Attacks often target energy grids, transportation systems, water treatment, and telecommunications. Their impacts can be catastrophic: large-scale outages disrupt healthcare, emergency services and government operations across regions. In practical terms, recent energy-sector breaches have reached record costs – averaging about US$4.7 million per incident in 2022(Casanovas & Nghiem, 2023), and have disabled critical controls (e.g. wind-farm controls, smart meters). In the absence of stronger safeguards, such assaults increasingly threaten supply chains, investor confidence, and civilian welfare. These trends are summarized in Table 1, which presents recent global cyber threat metrics from authoritative sources.

Table 1. Global Cyber Threat Statistics (2020–2024)

Category	Statistic (Global)	Source (Year)
Cyberattacks on critical infrastructure	*Over 420 million attacks in one year (2023)* ↓30% increase from 2022	KnowBe4 (2024)
Disinformation/misinformation campaigns	*189 documented disinfo campaigns (Africa, 2023) 87% of citizens surveyed are concerned about disinfo's impact*	Africa Center/ UNESCO (2023)
Data breaches/privacy violations	*5,199 confirmed breaches* (global, 2023)	Verizon (2023)

Note. Data drawn from international cybersecurity reports and studies (2021–2024)

Misinformation and disinformation continue to destabilize societies and democracies. Global

surveys reveal that citizens recognize disinformation as a serious threat to political life. In a multi-country study, 87% of respondents believed online disinformation had already had a major impact on their country's politics(UNESCO & IPSOS, 2023). Empirical analyses confirm that organized disinformation campaigns are pervasive, often tied to elections or social unrest. For example, researchers documented at least 189 distinct disinformation campaigns targeting African nations in 2023 – nearly four times the count from 2022 (Lemos, 2024), many engineered to sway public opinion during elections. Nearly 60% of these African campaigns were state-sponsored (e.g. by Russia, China or Gulf states)(Africa Center for Strategic Studies, 2024), illustrating how foreign powers weaponized disinformation to influence other countries. These malign narratives deepen polarization, erode trust in institutions, and have directly fueled violence and democratic backsliding in some regions(UNESCO, 2023; Africa Center for Strategic Studies, 2024). The World Economic Forum notes that "misinformation and disinformation" now rank among the biggest short-term global risks, precisely because of their corrosive effect on social cohesion. States routinely use cyber operations for geopolitical advantage beyond pure data theft. Cyber tools are embedded in modern diplomacy and conflict. In peacetime, intelligence agencies conduct cyber espionage to steal secrets and gain strategic insight. In rivalry, states launch disruptive attacks on rivals' infrastructure to apply pressure without open warfare. For instance, documented incidents show adversaries targeting energy or communications grids to influence an opponent's decision-making. In a recent report, industry experts warn that cyberattacks on critical sectors "pose a significant risk to national security and economic stability". Likewise, the World Economic Forum observes that advanced cyber tools enable more "goal-oriented attacks" capable of high political and economic damage(World Economic Forum, 2024). In short, modern states integrate cyber-espionage, sabotage and influence (including disinformation) into their foreign-policy arsenals to gain advantage over rivals.

Cyber threats also escalate regional tensions. Unchecked cyber aggression can provoke retaliation and amplify mistrust among states. Experts caution that without norms or constraints, digital skirmishes risk spiralling into broader conflicts. As the WEF notes, "cyberattacks are another battlefront in which escalation is a key risk" (World Economic Forum, 2024). Recent history bears this out: cyber incidents (real or alleged) between states like the U.S., Russia, China, Iran and North Korea have repeatedly raised tensions. When a state suffers a destructive attack on its critical systems, its response may target the perpetrator's assets, further deepening animosities. This dynamic was highlighted in expert projections: breaches of strategic systems (e.g. power grids, GPS, banking) "could lead to open cyberwarfare" and undermine trust in governments' ability to protect citizens.

In sum, cyber operations do not occur in a vacuum – they interact with geopolitical rivalries and can intensify conflicts even in the absence of conventional warfare. Despite these mounting threats, international cybersecurity frameworks remain weak, underscoring the need for cooperation. Currently, no comprehensive global treaty governs state behaviour in cyberspace. Cross-border cybercrime and disinformation largely go unpunished, and unilateral approaches prevail. Surveys of experts find that "cross-border cyberattacks and misinformation" are among the least effectively

mitigated risks globally. In practice, states often prioritize narrow national security goals over collective norms, leading to minimal information sharing or joint deterrence efforts. Observers warn that without new multilateral rules, states will continue reactive, siloed policies – a recipe for mutual distrust. The World Economic Forum's 2024 Global Risks Report explicitly calls attention to the shortfall in cooperation on cyber issues. Taken together, the findings indicate an urgent need for strengthened international dialogue and binding frameworks (analogous to arms control) to manage cyber-technological threats. In the interim, capacity building and joint exercises may help bridge the trust gap, but the long-term solution will require political will to cooperate on cybersecurity.

V. CONCLUSION

In the digital age, cyber and technological security issues have become critical components of international relations, with far-reaching implications for national and global stability. The increasing prevalence of cyberattacks, data privacy violations, and misinformation campaigns has transformed the nature of conflicts, expanding them into the virtual realm. These cyber threats undermine national security by targeting critical infrastructure, influencing electoral outcomes, and challenging traditional notions of sovereignty. Furthermore, digital misinformation erodes public trust, polarizes societies, and distorts democratic processes, while data privacy concerns raise critical questions about individual security and state surveillance.

The literature review and analysis indicate that cyberattacks, data breaches, and misinformation now pose systemic risks to national and global stability. Empirical findings highlight that modern cyber intrusions can disable critical infrastructure and undermine institutional trust. For example, UN experts note that malicious cyber operations against public institutions and elections "erode trust, fuel tension and sow the seeds of violence and conflict". Likewise, misinformation, increasingly powered by AI, is identified as a top global threat, undermining democratic systems and public confidence in governance. Scholars describe this convergence of cyber warfare and information warfare as a new form of digital great-power contestation.

At the same time, diverging national policies on data governance (e.g. the EU's GDPR versus China's data-security laws) are fragmenting the global internet and complicating cross-border collaboration. In sum, the evidence shows that cyber and technological threats have widespread, transnational impacts that amplify political tensions and destabilize societies. These findings carry profound implications for international relations and sovereignty. States increasingly treat cyberspace and data flows as spheres of sovereign power, intensifying geopolitical rivalry. Cyber conflicts now traverse borders – over two-thirds of significant attacks spill over into neutral countries and even non-state actors (hacktivists, criminal groups) are implicated, blurring the line between war and crime.

The resultant erosion of trust – through covert data exploits or viral disinformation – can weaken alliances and democratic resilience. As the UN Security Council has emphasized, "peace and security in the physical world demand new approaches" that integrate the digital realm under rule-

of-law norms. In effect, cyber threats are no longer confined to technical domains but have become central to questions of international stability, national sovereignty, and the liberal international order .

Policy Recommendations: Drawing on these insights, we propose the following actions for governments and multilateral institutions.

- Negotiate binding cyber norms and treaties. States should finalize an updated international cybercrime convention and related agreements. Multilateral frameworks must define and enforce norms (e.g. attribution of attacks, limits on targeting civilians) and mandate sanctions for malicious actors. In practice, this means supporting UN and regional initiatives to codify cyber conduct (as the UN Secretary-General has urged) and holding violators accountable through legal and diplomatic means.
- Harmonize data privacy standards. Governments should forge interoperable privacy regimes that protect individuals while enabling trusted data flows. For example, like-minded countries could align their laws with EU-style data protection (GDPR) and join agreements such as the Global Cross-Border Privacy Rules Forum. Crafting common frameworks and mutual certification will reduce fragmentation and build "data flows with trust" among allies.
- Invest in capacity-building and information sharing. Wealthy states and international organizations must support cyber-defence capabilities in lower-income regions. This includes joint training, shared threat intelligence, and technical assistance. Regional bodies (e.g. African Union, ASEAN) have adopted cyber strategies and should be empowered to host incident response centers and cross-border working groups. By pooling resources and expertise, states can raise collective resilience and reduce mistrust in the cyber domain
- Counter misinformation collaboratively. To combat the erosion of social trust, governments should fund media-literacy programs and fact-checking networks that transcend borders. Social-media platforms must be pressured to increase transparency and remove malicious bots. State and non-profit actors can coordinate on early-warning systems for deepfakes and propaganda. As the WEF reports, GenAI-driven disinformation "is disrupting democratic systems and undermining public trust in critical institutions", so joint public–private initiatives are needed to inoculate societies and uphold information integrity.
- Each of these steps requires concerted multilateral effort, blending diplomatic, legal, and technical measures. In particular, enhanced cooperation between major powers (in forums like the G20 or a UN cyber commission) is crucial to prevent a "digital Cold War" and to ensure that norms apply universally.

Limitations and Future Research: This study's scope, while global, inevitably faces limitations. Rapid technological change (e.g. advances in AI and quantum computing) means that some predictions are provisional, and many policy frameworks are still evolving. Additionally, incomplete data on covert cyber operations and state-sponsored disinformation complicates quantitative

assessment. The diversity of national legal regimes also means that one-size-fits-all solutions are difficult to implement.

Future research should address these gaps. Key questions include:

- What mechanisms can effectively enforce international cyber norms in the absence of a supranational authority? For instance, how can attribution and sanctions be applied credibly when states conduct covert cyber operations?
- How will emerging technologies reshape cyber conflict and misinformation? Research should examine the impact of AI (e.g. autonomous cyberattacks, synthetic media) and quantum computing on both offense and defence, to guide adaptive security strategies.
- How can policy reconcile divergent data sovereignty laws while protecting privacy? In particular, what models can integrate the economic benefits of data flows with robust citizen protections, given current EU–US–China policy differences?

By answering these and related questions, scholars and practitioners can further refine strategies to safeguard stability in a digitally interconnected world.

References

Africa Center for Strategic Studies. (2024, March 13). *Mapping a surge of disinformation in Africa.* https://africacenter.org/spotlight/mapping-a-surge-of-disinformation-in-africa/

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of Economic Perspectives,* 31(2), 211–236.

Bjola, C., & Pamment, J. (2019). Disinformation in international relations: How important is it? *Security and Human Rights*, 29(1–4), 3–18. https://brill.com/view/journals/shrs/29/1-4/article-p3_3.xml

Casanovas, M., & Nghiem, A. (2023, August 1). *Cybersecurity – is the power system lagging behind?* Summit on the Future of Energy Security. International Energy Agency. https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind

Chaudhary, A., & Dickson, G. (2022). *Cyber Conflict and Political Rivalries in South Asia.* Routledge.

Clarke, R. A., & Knake, R. (2010). *Cyber war: The next threat to national security and what to do about it.* HarperCollins.

Creemers, R. (2020). *China's approach to cyber sovereignty.* Konrad-Adenauer-Stiftung. https://www.kas.de/documents/252038/7995358/China%E2%80%99s+Approach+to+Cyber+Sovereignty

Gerrits, A. W. (2018). Disinformation in International Relations: How Important Is It?. *Security and Human Rights,* 29(1-4), 3-23. https://doi.org/10.1163/18750230-02901007

Humphreys, B. E. (2024). *Attacks on Ukraine's electric grid: Insights for U.S. infrastructure security and resilience* (Congressional Research Service Report No. R48067). U.S. Government. https://sgp.fas.org/crs/row/R48067.pdf

International Energy Agency. (2023, August 1). *Cybersecurity – is the power system lagging behind?* IEA. https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind

Kerr, P. K., Rollins, J. W., & Theohary, C. A. (2010). *The Stuxnet computer worm: Harbinger of an emerging warfare capability* (Congressional Research Service Report No. R41524). U.S. Government. https://www.congress.gov/crs_external_products/R/PDF/R41524/R41524.3.pdf

KnowBe4. (2024, August 26). *Cyber attacks on infrastructure: The new geopolitical weapon* [Press release]. https://www.knowbe4.com/press/knowbe4-report-reveals-critical-infrastructure-under-siege-with-cyber-attacks-increasing-30-percent-in-one-year

Lemos, R. (2024, March 26). *Africa tackles online disinformation campaigns during major election year.* Dark Reading Global. https://www.darkreading.com/cyberattacks-data-breaches/africa-tackles-online-disinformation-campaigns-during-major-election-year

Richards, N. M. (2013). The dangers of surveillance. *Harvard Law Review*, 126(7), 1934–1965. https://harvardlawreview.org/print/vol-126/the-dangers-of-surveillance/

Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare.* Farrar, Straus and Giroux.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know.*

Oxford University Press.

Tikk, E. (2018). *International Cyber Norms: Legal, Policy & Industry Perspectives.* Cambridge University Press.

UNESCO & Ipsos. (2023, September). *Survey on the impact of online disinformation and hate speech.* https://www.unesco.org/sites/default/files/medias/fichiers/2023/11/unesco_ipsos_survey.pdf

United Nations Educational, Scientific and Cultural Organization (UNESCO). (2023). *Study on the impact of online disinformation during election campaigns (*Ipsos–UNESCO). https://www.unesco.org/sites/default/files/medias/fichiers/2023/11/unesco_ipsos_survey.pdf

Verizon Business. (2023). *2023 data breach investigations report (DBIR) public sector snapshot.* Verizon. https://www.verizon.com/business/resources/reports/dbir

Wardle, C., & Derakhshan, H. (2017). Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. *Council of Europe.*

World Economic Forum. (2024, January 10). *Global risks report 2024: Disinformation tops global risks as environmental threats intensify* [Press release]. https://www.weforum.org/press/2024/01/global-risks-report-2024-press-release/

Woolley, S. C., & Howard, P. N. (Eds.). (2017). *Computational propaganda: Political parties, politicians, and political manipulation on social media.* Oxford University Press.

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. *PublicAffairs.*