CASS

CENTRE for AEROSPACE & SECURITY STUDIES

Cyberspace as a Global Common: Formulation and Applicability of International Law

Analysis Report

July 2024

PRESIDENT
Air Marshal Javaid Ahmed (Retd)

ROUNDTABLE COORDINATOR
Air Marshal Zahid Mehmood (Retd)

EDITED BY
Sarah Siddiq Aneel

RAPPORTEURS
Syed Moiz Rafay | Ajwa Hijazi | Shah Muhammad | Mustafa Bilal | Uswa Khan | Shaheer Ahmad | Muhammad Qasim

LAYOUT
Hira Mumtaz

All correspondence pertaining to this document should be addressed to CASS, Islamabad through post or email on the following address:

Centre for Aerospace & Security Studies

+92 051 5405011
cass.thinkers
cass.thinkers@casstt.com
cassthinkers
@CassThinkers
Centre for Aerospace & Security Studies

Old Airport Road, Islamabad, Pakistan
www.casstt.com

CASS

CENTRE for AEROSPACE & SECURITY STUDIES

Cyberspace as a Global Common: Formulation and Applicability of International Law

Analysis Report

Contents

INTRODUCTION

In the modern digital age, cyberspace has become an integral part of daily life. However, as cyberspace transcends physical borders, it poses unique challenges to traditional legal frameworks. Understanding cyberspace as a 'global common' and the applicability of international law within this realm is crucial for ensuring security, stability, and cooperation in the digital domain.

To address these critical issues, the Centre for Aerospace & Security Studies (CASS) organised a roundtable discussion on 8 July 2024 on ***'Cyberspace as a Global Common: Formulation and Applicability of International Law.'***

The roundtable aimed to explore the concept of cyberspace as a global common, assess the applicability of international law in regulating activities within this domain, create a deeper understanding of the challenges and opportunities presented by cyberspace and facilitate discussion on the development of effective legal frameworks to address them.

The distinguished subject matter experts who spoke at the roundtable included:

- Jamal Aziz, Executive Director, Research Society of International Law (RSIL), Pakistan
- Khawaja Mohammad Ali, Cyber Security, Data Privacy & Digital Forensics Expert

Dr Zunera Jalil, Professor and Chair of the Department of Cyber Security and Dr Kashif Kifayat, Professor from the Department of Cyber Security at Air University also shared brief thoughts. The discussion was moderated by Air Marshal Zahid Mehmood (Retd), Director at CASS with Opening and Concluding Remarks by President CASS Air Marshal Javaid Ahmed (Retd).

EXECUTIVE SUMMARY

In his brief *Welcome Remarks*, ***Air Marshal Javaid Ahmed (Retd)*** highlighted Pakistan's cybersecurity vulnerabilities, and shared his hope that the roundtable would add value to related national policies and participation in the international cyberspace governance conversation.

In his Introduction, ***Air Marshal Zahid Mehmood (Retd)*** focused on cyberspace's emergence as the newest and most critical global common. He highlighted how cyberspace is currently internationally unregulated, except for technical standards, with most attempts at regulation having only resulted in regional frameworks and affirmations of national sovereignty. He highlighted the national security implications of cyberspace and invited the speakers to shed light on Pakistan's position on these issues.

In his presentation on *Applicability of International Law in Global Commons & Enforcement Mechanisms*, ***Mr Jamal Aziz*** stated that technical standard setting was the main battleground in cyberspace regulation, and that Pakistan currently had no contribution in this process. He discussed how regulating cyberspace was arguably even more difficult than other global commons, because firstly, it involved many distinct domains and sub-domains, all of which had their own regulatory questions. Secondly, because conflicting priorities created deadlocks between nations, preventing global consensus. Thirdly, because it was mostly owned by private companies. Fourthly, because of numerous unresolved regulatory questions. Despite all this, he said nations were actively shaping regulations in their favour by being the first to develop effective laws and advocating for their adoption as international standards. Overall, he predicted a future mix of international regulatory regimes, some focused on openness and others on state sovereignty, with Pakistan leaning towards the latter (though he urged research into the benefits and drawbacks of doing so). Given the lack of global consensus, he concluded that regulating cyberspace with international law was currently improbable.

On the subject of *National Cyber Security Policy, Cyber Threats to National Security & Response Mechanism*, ***Mr Khawaja Mohammad Ali***, warned about the potential impacts of cyberattacks and urged treating cybersecurity as a national security matter, with implications for Pakistan's economy and survival. He agreed that cyberspace was a global common but said that Pakistan lacked any voice in its governance due to its total dependence on foreign technology, which also made it vulnerable to cyber threats. He traced Pakistan's cybersecurity efforts from 2003 to the forthcoming 2025 National Cybersecurity Policy, noting improvements and work yet to be done, while also recommending more frequent policy updates. He outlined in depth how an ideal response setup of CERTs would work and advocated for a Canadian-style centralised cybersecurity model for Pakistan. He advised Pakistan to

engage in global cyber diplomacy; cyber technology indigenisation; introduction of effective CERTs; and treating cyberspace security as a defence challenge.

In her remarks, ***Dr Zunera Jalil*** argued against treating cyberspace as a global common while urging effective cross-border cyber legislation. She lamented how slow adoption of emerging technologies by the public sector made critical infrastructure vulnerable and recommended better utilisation of global cyber threat intelligence. She identified generative AI and fileless malware as emerging cyber threats. She noted Pakistan's low ranking in the Global Cybersecurity Index (GCI) and urged faster implementation of the existing cyber security policy. She also stressed the need for indigenisation of software, hardware and most critically, Pakistan's data.

Dr Kashif Kifayat contrasted cyberspace with other global commons, noting its universal accessibility and general dependency on it. He highlighted how cyber risks emerge as organisations adopt technology. He pointed out the difficulty in detecting cyber capabilities and attacks and suggested that such attacks were already ongoing. He further speculated that Pakistan's cyber security was compromised due to its complete dependence on foreign technology, with other nations having the capability to take hostile actions, just currently choosing not to. He attributed Pakistan's dependency to its weakness in the economic, political, technological and human resource sectors, which also limited its voice in cyberspace governance. He shared efforts by Air University to develop cyber security human resources and recommended a national cyber security roadmap, emphasising human resource development.

In his *Concluding Remarks* and *Vote of Thanks*, President CASS ***Air Marshal Javaid Ahmed (Retd)*** offered his perspective on several key points. Firstly, he noted that data was a powerful tool in decision-making and warned that Pakistan was making itself vulnerable by not indigenising its national data. Secondly, he pointed to the growing divide between Eastern and Western technological blocs and suggested Pakistan could face a strategic choice between them in the future. However, he was hopeful that Pakistan possessed pockets of excellence which would help the country deal with these challenges effectively.

KEY TAKEAWAYS

- Cyberspace is arguably more difficult to regulate than other global commons due to its complex subdomains, private ownership, and conflicting national priorities.
- Technical standards setting is the key battleground in international cyberspace governance.
- In terms of future scenarios, cyberspace will likely not be regulated as a global common. Instead, the world is likely evolving towards a mix of international regulatory frameworks - those calling for openness and those advocating state sovereignty. Pakistan is leaning towards the latter.
- Currently, international cyberspace regulation is happening without Pakistan's proactive engagement. Effective domestic regulations, indigenous cyber technologies and cyber diplomacy can help secure Pakistan a voice in shaping the international standards and regulations it will encounter in the future.
- Cyberspace should be treated as the fifth domain of warfare, potentially superseding traditional security domains in its impact on the economy.
- Pakistan faces significant cyber threats and challenges because of lack of awareness, thus far inadequate policy frameworks and near total reliance on foreign technologies.
- Cyberspace comprises many different domains and sub-domains. Each of them has strategic, legal, security aspects that must be addressed separately. It is not possible or advisable to address it via a single monolithic policy or institution. Cyber security, cybercrime, data privacy, IT security should be dealt with by separate but interconnected policies and agencies.
- The 2021 National Cybersecurity Policy needs refinement and regular updates.
- Pakistan's implementation of the 'National Cybersecurity Policy' has been slow and needs to improve.
- Pakistan needs a holistic national cyber security response setup, and sector-specific and organisation-specific CERTs.
- Pakistan can benefit from emulating a centralised cybersecurity agency model, similar to Canada.
- Capacity building and developing skilled human resources in various cyber security domains is critical.
- Pakistan's dependence on both Eastern and Western tech blocs may necessitate future strategic choices regarding technological partnerships.
- Pakistan must prioritise the development and utilisation of indigenous data and cyber technologies.

PROPOSED WAY FORWARD

The following recommendations emerged from the roundtable discussion:

Indigenise cyber capabilities to reduce foreign dependence and vulnerability to cyber threats

- Prioritise data localisation within Pakistan's borders
- Invest in indigenous hardware, software, platforms and expertise
- Support domestic technology development initiatives on war-footing.

Enhance and regularly update the National Cyber Security Policy

- Refine the National Cyber Security Policy (NCSP) to address existing gaps and ensure regular updates to keep pace with rapidly evolving threats.

Enhance cyber security policy implementation and threat response infrastructure

- Treat cybersecurity as a national security issue
- Accelerate implementation of NSCP across all sectors, especially critical infrastructure
- Emulate successful models of centralised cybersecurity agencies, such as Canada
- Ensure well-equipped and empowered National CERTs with a network of sector-specific and organisation-specific CERTs, ensuring funding sustainability
- Foster information sharing between organisations and CERTs
- Enhance cyber security threat intelligence gathering and research.

Improve efforts in cyber diplomacy

- Develop comprehensive domestic cyber laws that not only safeguard national interests but also set a precedent, potentially serving as a model for influencing international cyberspace regulation
- Ensure that Pakistan has representation in and official channels with relevant international forums to avoid risks of non-compliance and blacklisting
- Rather than expecting cyber space to be regulated as a global common in the foreseeable future, focus on cross-border legislation between friendly countries

Develop quality human resources in and foster awareness of cyber security

- Prioritise developing quality human resources in cyberspace domains and support initiatives like a National Cyber Security Academy.
- Foster a culture of cyber security awareness and responsibility, especially in the public sector.

Develop a National Cyber Security Roadmap

- Implement necessary improvements by developing a comprehensive, time-bound National Cyber Security Strategy for Pakistan, aligned with international best practices.

SUMMARY OF PROCEEDINGS

Air Marshal Javaid Ahmed (Retd)

President, Centre for Aerospace & Security Studies, Islamabad

Welcome Remarks

Air Marshal Javaid Ahmed (Retd) opened the forum by welcoming the distinguished speakers and acknowledging their extensive experience and contributions. He briefly discussed the current cyber security landscape in Pakistan, highlighting that several national institutions had faced security breaches, leading to concerns over data safety. He noted that these challenges stem partly from a lack of awareness and underscored the critical need to align with global cyber security measures to enhance protection and resilience. Expressing his hope, he stated that the discussion might serve as a catalyst for national policy reforms and encourage Pakistan's active participation in international cyberspace governance forums. Furthermore, he expressed his anticipation that CASS would contribute effectively by providing policy guidelines in this area.

Air Marshal Zahid Mehmood (Retd)

Director, Centre for Aerospace & Security Studies, Islamabad

Introduction

As the moderator of the roundtable, Air Marshal Zahid Mehmood (Retd) laid the groundwork for the discussion by outlining the concept of 'Global Commons', explaining the historical and contemporary challenges of governing shared natural resources beyond national jurisdictions -like the oceans, outer space, and the Antarctic. He began by defining 'Global Commons' through traditional academic perspectives and the United Nations' definitions, underscoring the challenges posed by the absence of single nation governance over these areas. He further traced the academic discourse back to William Foster Lloyd in 1833 and highlighted Garrett Hardin's seminal 1968 work, 'The Tragedy of the Commons'. Hardin expanded on Lloyd's ideas, arguing that without regulated access to shared resources, like grazing grounds, all users would suffer. This concept was further refined by Hardin himself, who later suggested his paper should have been titled 'The Tragedy of the Unregulated Commons.'

Air Marshal Mehmood then transitioned to discuss the regulatory frameworks governing these commons, like the UN Convention on the Law of the Sea and the Outer Space Treaty. He pointed out the shortcomings in these international agreements, such as the partial ratification of treaties and the ongoing territorial disputes like those in the South China Sea. He emphasised the challenges in enforcing these treaties and the discrepancies between their goals and real-world applications.

Focusing on cyberspace, the Air Marshal also debated its classification as a global common; and drew parallels to traditional commons, noting cyberspace's accessibility and non-exclusivity, yet highlighted its unique challenges as a man-made, intangible domain. Unlike natural commons, cyberspace's boundaries and content are virtually limitless, complicating regulatory efforts. He referenced various national and international efforts to address cyberspace governance, including the ICANN and W3C standards for data handling and web communication, and the varied success of legal frameworks like the Budapest Convention on Cybercrime.

He wrapped up by reflecting on the importance of understanding and addressing the security threats emerging from these global commons, particularly through cyber avenues. He cited different national strategies, like Canada's approach to cybersecurity, and mentioned contrasting national policies like Iran's 'Halal Internet' and China's 'Great Firewall.' He concluded with a call for more robust international dialogue and cooperation to ensure effective governance of global commons in the face of evolving threats and technological advancements; and invited the speakers to shed light on Pakistan's stance on these issues and future scenarios.

Speakers

Jamal Aziz

Executive Director, Research Society of International Law (RSIL), Pakistan

Applicability of International Law in Global Commons & Enforcement Mechanisms

Mr Jamal Aziz expressed his gratitude to CASS for the invitation and lauded its contributions to research in various academic and intellectual areas and the significance of such efforts in shaping policy. He began his presentation by highlighting that the real battleground in international cyberspace politics lay in the establishment of technical standards, harmonisation, and best practices. He noted that Pakistan lacked a strategic approach to these areas, resulting in negligible contributions that could benefit its strategic interests. Mr Aziz also critiqued Pakistan's domestic laws for being reactive rather than systematic, leading to inadequate responses in both domestic and international arenas.

Discussing the regulation of global commons, Mr Aziz referenced specific treaties, customary international law, and general practices that govern domains like outer space, polar regions, the environment, and the high seas. He remarked that the governance of outer space, initially established during the Cold War with the Outer Space Treaty, was now outdated due to new challenges and the difficulty of achieving consensus on a new model. He then touched on Antarctica, governed by the Antarctic

Treaty of 1959. For the high seas, he mentioned that despite numerous disagreements, it was relatively well-regulated under UNCLOS, which, although not ratified by many states, was considered customary international law. Lastly, he addressed the environment where, despite existing global agreements and guidelines, there was a lack of enforcement mechanisms primarily due to deadlocks on climate change issues, resulting in a fragmented framework of regulations.

Moving to the complexities of regulating cyberspace, Mr Aziz pointed out its intricate landscape filled with numerous domains and subdomains, each governed by distinct legal and regulatory frameworks. He questioned which regulatory bodies should oversee these various areas, highlighting the challenge of establishing uniform oversight. He then shifted the conversation to whether cyberspace should be regulated as a global common. He presented arguments in favour of this perspective, emphasising the internet's transnational nature, the benefits of the free flow of information, shared digital spaces, and the inherent need for cooperative governance. Conversely, he noted significant counterarguments including sovereignty issues, conflicts between domestic and international laws, and the lack of technical expertise in developing countries which hinders their meaningful participation in setting cyberspace standards.

Continuing on the subject of regulatory challenges, Mr Aziz discussed the divergent views among major global players. He noted that the US, with its advanced capabilities and leading tech companies, was advocating for an open and free-flowing internet to support commercial interests and maintain its espionage capabilities. In contrast, China and Russia were pushing for stringent state control over cyberspace to monitor and regulate the flow of information within their borders. Moreover, he highlighted the role of private companies in owning significant portions of cyberspace infrastructure, which was complicating public management and governance, further muddying the waters of cyberspace regulation.

Mr Aziz addressed the unresolved regulatory and legal gridlocks that challenge states, highlighting tensions not just between rivals like the US and China, but even among allies such as the US and the EU. He discussed specific contentious issues like net neutrality, the 'Right to be Forgotten' laws, and data localisation practices. He noted that these disputes underscore deeper regulatory challenges and jurisdictional issues. Mr Aziz pointed out that due to the fragmented nature of these regulations, companies often find themselves heavily staffed with lawyers.

The speaker also discussed the significant role that great power competition plays in shaping the governance of cyberspace. He pointed out how countries like China and Russia were actively worked to influence the Group of Governmental Experts (GGE) to ensure that state sovereignty was recognised, aiming to shape the development of international law in ways that align with their interests. Further, citing the example of China, Mr Aziz noted the strategic advantage countries gain when they successfully

develop strong national legislation and then integrate their domestic laws into international standards to gain a competitive edge over rivals.

Mr Aziz also highlighted several unresolved questions in the domain of cyberwarfare, such as attributing cyberattacks, regulating non-state actors, determining the appropriate level of offensive capabilities for nations, and fostering international cooperation in response to cyber threats.

He then turned his attention to various other sub-domains such as digital services, social media, e-commerce, and AI, noting that each area was complex enough to merit its own detailed presentation. Specifically, in the subdomain of social media, he addressed the challenges of content moderation and the prevention of misinformation, hate speech, and harmful content. He criticised Pakistan's lack of expertise in managing these issues. Regarding data privacy, he questioned how personal information shared on social media and e-commerce platforms could be protected. He also touched on the influence of external entities on elections, referencing the Cambridge Analytica scandal. Lastly, he discussed the U.S. Communications Decency Act that provides legal immunity to social media platforms for content posted by users, noting the varied perspectives on this issue both between and within countries.

To conclude his presentation, Mr Aziz outlined two potential future scenarios for cyberspace governance. In the first scenario, countries collaborate to establish universal standards and norms, treating cyberspace as a shared resource similar to the high seas or outer space. This model would involve governance by multiple stakeholders and support seamless cross-border flows. The second scenario envisioned countries or groups of countries developing their own regulatory frameworks and governance models that prioritise national control over digital infrastructure and data. This would lead to diverse regulations and standards and the formation of geopolitical blocs with limited interactions.

Mr Aziz was of the view that the future would likely be a hybrid of these two scenarios. He speculated that Pakistan, due to its limited capacity, would probably lean towards promoting state sovereignty and a more closed-off cyberspace. However, he cautioned that this approach was likely to come with both benefits and drawbacks that need thorough discussion. Mr Aziz concluded his discussion by stating that regulating cyberspace as a global common would require international consensus. However, he noted that in the current environment, where states had competing interests, achieving such regulation was likely not possible.

Khawaja Mohammad Ali

Cyber Security, Data Privacy & Digital Forensics Expert

National Cyber Security Policy, Cyber Threats to National Security & Response Mechanism

Mr Khawaja Muhammad Ali commenced his presentation by defining cyberspace as 'anything connected to the internet,' highlighting its pervasive role in daily life. He clarified that cyber security, according to ISO standards, was not merely about protecting data, systems, or connectivity but was focused on 'protecting people, states, and nations.' He argued that cyberspace should be recognised as a critical domain for national security and even proposed it as the fifth mode of warfare, suggesting that it surpassed all other domains because attacks on a country's critical cyber infrastructure could impact its economy and survival more significantly than physical invasions.

Mr Ali was in favour of looking at cyberspace as a global common because no single nation-state could tackle its challenges alone. The necessity for international cooperation in addressing cyberspace issues underscored its status as a common with global implications, necessitating coordinated governance and response.

Discussing the role of indigenous capabilities in global governance, Mr Ali discussed the complexities of cyberspace governance and how countries like Pakistan could effectively participate in it. He raised critical questions about who governs this domain and how Pakistan could assert itself in this arena. Drawing a parallel with the repercussions similar to those experienced under FATF sanctions, he stressed the strategic need for Pakistan to develop its own cyber capabilities to actively influence global cyber policies.

Without indigenous technologies, platforms, and expertise, Mr Ali underscored that Pakistan risked remaining a passive follower, susceptible to cyber threats and attacks. He illustrated this point by referencing significant cyber incidents like the SolarWinds, Stuxnet, and attacks on major corporations like Microsoft and Siemens, showing how cyber threats continually sought vulnerabilities in critical infrastructure sectors including banking, healthcare, and energy. He also pointed out the potential consequences of disruptions in the global cyber supply chain, highlighting that such disruptions could have far-reaching effects due to Pakistan's reliance on international cyber infrastructure and services.

Giving a historical background, Mr Ali shared that when Pakistan's cyber security efforts began in 2003, they were overly simplistic, as only a single department of the FIA was expected to handle all the various subdomains of cyberspace regulation. He explained how a Cyber Security Policy was introduced in 2013, aimed at differentiating between subdomains like cyber crime, cyber security, and cyber warfare. He shed light on the long process from that point to the development of a National Cyber Security

Policy in 2021, as well as the establishment of the National Cyber Crime Investigation Agency (NCCIA) and the Data Privacy Commission, now independent bodies. He stated his hope that the 2013 policy would be updated again by 2025 to address all prior shortcomings and frequently updated, considering the rapid changes in the field. Mr Ali stressed the importance of the Cyber Security Policy to Pakistan's survival and international dealings, calling it even more essential than the National Security Policy.

Mr Ali was of the view that while Pakistan had made progress in developing a cyber security policy, the focus needed to shift towards effective implementation. He compared Pakistan's approach to India's, observing that despite not having a formal written policy, India had strong implementation and prioritisation of cyber security.

He argued that different aspects of cyberspace regulation, such as cybercrime, cyber security, and IT security, required distinct regulations. He remarked that the Cyber Security Policy was specifically brought to the Defence and Production Committee because cyber security is a matter of national defence and advocated that it should not be under the Ministry of IT.

The speaker also mentioned that new bodies like the National CERT (Cyber Emergency Response Team), Data Protection Regulatory Authority, and National Cybersecurity Investigation Agency (NCSIA) were also being established. He noted that there were ways to significantly improve cloud computing security, such enforcing regulations requiring cloud computing nodes to be located in friendly countries.

On the topic of response mechanisms, Mr Ali underscored the crucial need to protect institutions and critical infrastructure, warning that severe cyberattacks could potentially collapse the country's economy. He detailed the need for a cooperative framework among national, sectoral, and organisational CERTs, each tasked with distinct roles. He underscored the importance of sustainable funding for organisational cyber security and referenced various international models.

Mr Ali elaborated on the roles CERTs play, such as disseminating credible information, defusing false flags, empowering institutions, conducting security assessments, collecting information on all attacks (Essential Elements of Information, EEIs), providing threat intelligence, and offering technical assistance. He said that it was the ethical and moral responsibility of organisations to share information about threats and attacks, though he noted that currently, this was often not the case. He urged regular publication of technical reports like Strategic Cyber Threat Intelligence Reports, sharing findings from international research, and issuing advisories after cyber incidents. He also advocated that Pakistan should align with emerging international standards in cyber security, rather than developing its own divergent standards, as well as the creation of global agreements and treaties that prohibit harmful activities in cyberspace, similar to the Comprehensive Nuclear-Test-Ban Treaty (CTBT). Mr Ali also recommended that Pakistan adopt global best practices and models such as Canada's approach to centralising cyber security functions under one

central agency, which consolidates various cybersecurity functions under a single body with senior leadership. Furthermore, he emphasised the need to engage in international cyber security forums and dialogues, to shape governance and norms. He warned of the critical dangers of not having established official channels and representation, including potential blacklisting.

Discussing global cyber space supply chains and Pakistan's dependency, Mr Khwaja Muhammad Ali also drew a distinction between the emphases on software by major Western companies and on hardware by major Eastern ones. He explored the competitive dynamics between these entities, aiming for dominance in cyber technology sectors. During his analysis, he pointed out Pakistan's precarious position, heavily reliant on both sectors. To mitigate these vulnerabilities, Mr Ali advocated for a robust development of local technology. He used the example of the US, which actively reduced its dependence on foreign technology for cyber security reasons, to underline the necessity for Pakistan to bolster organisations like NCCA, accelerating indigenous technology development. He posited a scenario where a sudden unavailability of major cyber space applications, such as WhatsApp, could severely disrupt the economy and affect the daily lives of citizens.

Concluding his presentation, Mr Ali called for the establishment of competent CERTs and underlined the importance of civil-military collaboration to brace for the challenges of cyberspace security, recognising it as a critical fifth domain of defence.

Guest Discussants

Dr Zunera Jalil

Professor and Chair, Department of Cyber Security, Air University

Dr Zunera Jalil presented arguments against treating cyberspace as a global common, stressing its economic significance, daily relevance, and susceptibility to manipulation. She expressed concerns about the public sector's sluggish adoption of emerging technologies, which she argued left critical infrastructure exposed to cyber threats. She also highlighted the value of global cyber threat intelligence, which provides widely accessible information that can be instrumental in tailoring cyber security measures specific to Pakistan's needs. She pointed to the challenges posed by generative AI, such as the proliferation of disinformation, phishing, ransomware, and deepfakes. To combat these threats, she advocated for the development of defensive AI to counteract malicious AI activities.

Dr Jalil also raised concerns about fileless malware, noting it as a burgeoning threat that posed significant challenges for Pakistan, especially given the country's limited capabilities in digital forensics for file-based malware. She critiqued Pakistan's slow progress in implementing its 2021 Cybersecurity Policy and pointed out the

country's low ranking - 79th - in the Global Cybersecurity Index (GCI). She urged for accelerated cyber security initiatives, particularly within the public sector that controls critical infrastructure.

Concluding her remarks, Dr Jalil recommended focusing on mature cross-border legislation, fostering indigenous development of software and hardware, and prioritising data localisation within Pakistan's borders, rather than advocating for cyber security to be treated as a global common.

Dr Kashif Kifayat

Professor, Department of Cyber Security, Air University

Dr Kifayat clarified the distinction between natural and human-made global commons noting that while natural global commons have only been exploited as countries developed, developing nations have faced challenges due to limited resources. He identified cyberspace as a human-made global common, which initially presented no security concerns. However, growing universal reliance on cyberspace and cyber technologies had led to the emergence of cyber risks. Dr Kifayat expressed concern over the difficulty in assessing the cyber capabilities of opponents, noting that such attacks develop gradually and can have long-range impacts. He proposed that due to Pakistan's reliance on foreign technology, its cyber security might already be compromised, and it was only the restraint of other actors that prevented hostile actions.

Dr Kifayat also discussed Pakistan's limited influence in global cyber security legislation due to its dependency on foreign technology and weaknesses in political, economic, technological, and human resource sectors. He also touched upon the psychological warfare threats posed through cyberspace.

Highlighting proactive efforts, he mentioned Air University's initiatives since 2017 in developing human resources in cyber security. This includes introduction of an undergraduate programme in cyber security and the establishment of the National Cyber Security Academy, aimed at cultivating world-class cyber security experts for Pakistan.

Concluding his remarks, Dr Kifayat stressed the need for a national cyber security roadmap and timeline based on seven common pillars, particularly focusing on human resource development as a crucial element in addressing all national security challenges.

Air Marshal Javaid Ahmed (Retd)

President, Centre for Aerospace & Security Studies, Islamabad

Concluding Remarks & Vote of Thanks

In his *Concluding Remarks* and *Vote Thanks*, President CASS Air Marshal Javaid Ahmed (Retd) appreciated the novel perspectives shared by the panel of experts and assured the audience that this would not be the last discussion on this important topic. He introduced the concept of 'data wars' and the central role of data in decision-making processes. Air Marshal Ahmed highlighted the increasing centralisation of data, notably in personal devices like mobile phones. For example, he shared how accessing a suspect's mobile phone could often resolve a case. Another example cited was the Turnitin programme, which, he argued, provides its owners with access to global academic research.

President CASS also discussed the transformation in data interpretation capabilities, attributed to advancements in AI and big data analytics. He expressed concerns over Pakistan's vulnerability due to its reliance on foreign hardware and software for managing its data. The President also pointed out the emerging geopolitical divisions in cyber technology between the eastern and western blocs, suggesting that Pakistan might soon have to make strategic choices similar to those it faced in military technology. He noted that the East, particularly China, was rapidly catching up with the West in the technological power balance, especially in sectors like computer chips and electric vehicles.

Highlighting a recent legislative change, he critiqued the government's legal allowance for intercepting citizen data, arguing that an overemphasis on traditional military security without sufficient focus on economic and national data security issues was detrimental to the country.

Concluding on a hopeful note, Air Marshal Ahmed remarked on positive trends in cyber security and increased threat awareness within Pakistan. He encouraged all experts and attendees to continue supporting the government, particularly towards the indigenisation of critical areas such as cloud computing. He ended his remarks with an optimistic view of Pakistan's strengths and pockets of excellence and thanked the panel of speakers for their insights.

ANNEXURES

Profiles of Speakers

Mr Jamal Aziz

Executive Director, Research Society of International Law (RSIL), Pakistan

Mr Jamal Aziz is Executive Director of the Research Society of International Law (RSIL). Additionally, he is the honorary Director of the Centre of Excellence for International Law (CEIL) at the National Defence University (NDU). Mr Aziz is a recognised international law expert, working at the forefront of criminal justice, international law and national security issues in Pakistan since 2010. He specialises in rule of law delivery and public sector legal reform projects and has overseen the development of over 200 publications related to International and Pakistani law, resulting in legislative reforms and policy actions at both federal and provincial levels. Mr Aziz has also helped develop indigenous legal capacity in state institutions, like the national and provincial police, prosecution and judicial academies, major universities and strategic institutions. He graduated with distinction from University College London with an LL.M.

Mr Khwaja Mohammad Ali

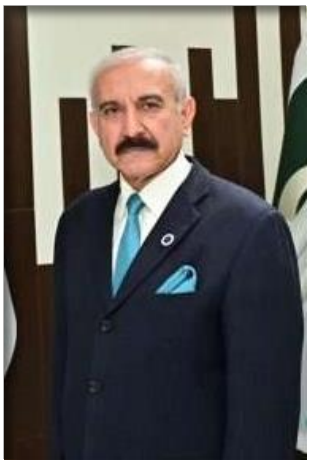
Cyber Security, Data Privacy & Digital Forensics Expert

Mr Khwaja Mohammad Ali is an IT Governance & Information Security professional with expertise in cyber security, data privacy, and digital forensics. He graduated in IT from Curtain University of Technology, Australia. He is currently serving as Head of Technology Strategy, Risk, and Governance at the National Bank of Pakistan. With a background as a former Regional Director (Cyber Crimes) at the Federal Investigation Agency of Pakistan, Mr Ali is a founding member of the Cyber Security Alliance of Pakistan (CSAP) and the Pakistan Information Security Association (PISA). He holds international certifications in data privacy and cyber security, contributing to national initiatives for Pakistan's cyber security strategy and the establishment of a national Cyber Emergency Response Team.

Air Marshal Zahid Mehmood (Retd)

Director, Centre for Aerospace & Security Studies, Islamabad

Air Marshal Zahid Mehmood (Retd) joined the Centre for Aerospace & Security Studies, Islamabad as Director in November 2023. A graduate of National Defence University and Air War College, he has 36 years' experience of military aviation as a fighter pilot in the Pakistan Air Force. During his service with the PAF, he has held various Command and Staff appointments including Assistant Chief of Air Staff (Plans), Director General C4I, Deputy Chief of Air Staff Personnel and Vice Chief of Air Staff. He holds Master's Degrees in Strategic Studies and Defence & Strategic Studies. An alumnus of the Harvard Kennedy School for National and International Security (USA), his areas of expertise include National Security with emphasis on traditional security threats and response options; Doctrine and Policy. He lectures regularly at Pakistan's National Defence University and Air War College on related subjects. He is a recipient of Hilal-i-Imtiaz (Military) for his services to the PAF.



Air Marshal Javaid Ahmed (Retd)

President, Centre for Aerospace & Security Studies, Islamabad

Air Marshal Javaid Ahmed (Retd) was appointed President of the Centre for Aerospace & Security Studies, Islamabad on 29 April 2024. Previously, he served as Vice Chancellor of Air University.

With a distinguished career spanning approximately 40 years in the Pakistan Air Force (PAF), he has held several critical positions. His roles have included Chairman of the Pakistan Aeronautical Complex (PAC) Kamra, Officer Commanding of the Combat Commanders School, and Chief Project Director of the JF-17 Fighter Aircraft Production Program. He is recognised for his expertise in aerospace development policies, as well as doctrine formulation and implementation strategies.

Air Marshal Ahmed is an alumnus of the Air War College, where he graduated in Defense & Strategic Studies. He also holds Master's degree in War Studies from the National Defence University. His skills in command and management are complemented by his advanced knowledge in emerging academic fields. Previously, he also served as Director of Policy and Doctrine at CASS, Islamabad. In recognition of his significant contributions to the Pakistan Air Force, he awarded Tamgha-i-Imtiaz, Sitara-i-Imtiaz, and Hilal-i-Imtiaz (Military).

Press Release

CASS Roundtable Recommends Strengthening Domestic Cybersecurity Legislation & Indigenous Solutions

9 July 2024

The Centre for Aerospace & Security Studies (CASS), Islamabad, conducted a roundtable on the *'Cyberspace as a Global Common: Formulation and Applicability of International Law.'*

Air Marshal Zahid Mehmood (Retd), Director (National Security) at CASS, set the stage for the discussion by outlining critical issues surrounding the governance of cyberspace. Drawing parallels to natural assets outside national jurisdictions such as oceans and outer space, he highlighted the unique challenges and responsibilities faced in regulating cyberspace as a 'global common'. Air Marshal Mehmood highlighted several international initiatives working to establish norms for cyberspace governance, including efforts of the Internet Corporation for Assigned Names and Numbers (ICANN); the United Nations' Group of Governmental Experts (GGE); and the World Wide Web Consortium (W3C). Additionally, he referenced legal frameworks like the

Budapest Convention on Cybercrime; the African Union Convention on Cyber Security and Personal Data Protection; and NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE)'s Tallinn Manual 2.0 that are shaping the landscape of cyber law. Despite these efforts, he lamented that cyberspace remains largely unregulated, underscoring the pressing need for enhanced international cooperation.

Mr Jamal Aziz, Executive Director, Research Society of International Law (RSIL), remarked that discussions on great power rivalry, geopolitics, and the multipolar world often remained superficial, pointing out that the real confrontation was now unfolding in the technological domain, particularly in cyberspace. He highlighted that international standard setting works in tandem with strategic and domestic institutions, a process that needs sharp focus by Pakistan. Additionally, he noted that domestic laws were not systematically coordinated, leading to ineffective domestic and international responses. Mr Aziz also expressed concern over the basic nature of agreed-upon cyber security norms and the complexity of cyber warfare, including issues of attributing cyber-attacks and managing non-state actors. He underscored

the importance of developing strong domestic legal frameworks in the digital domain, noting that countries like the US and China were advancing regulations to set the pace for global standards in their interest.

Mr Khawaja Mohammad Ali, a Cyber Security, Data Privacy, and Digital Forensics Expert, was of the view that cyberwarfare must be recognised as the fifth domain of warfare, highlighting its importance for national security. He cautioned that future sanctions could stem from cyberspace governance, underscoring the need for

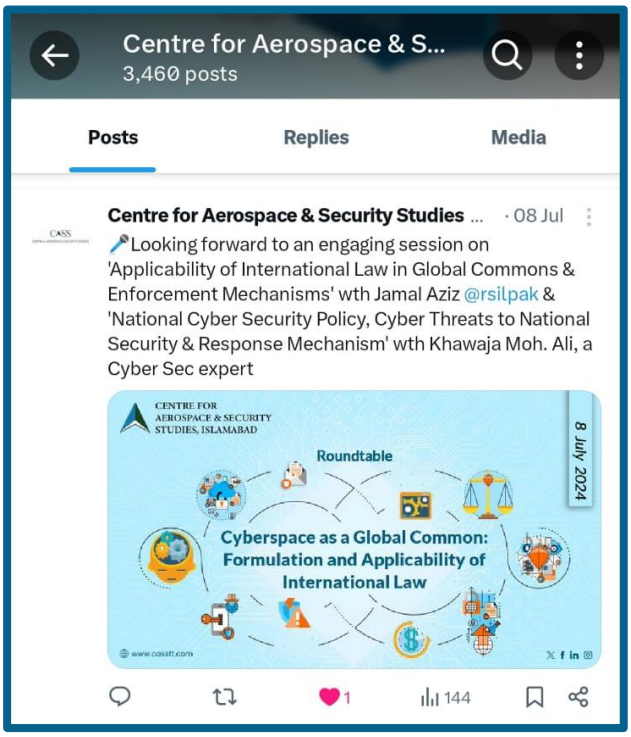
Pakistan to establish a presence in cyberspace and participate in its governance to avoid remaining vulnerable to cyber threats. He pointed out the importance of the global supply chain in cyberspace, indicating the need for sophisticated cybersecurity measures. He mentioned that cybersecurity, once a buzzword around 2003-04, is now being seriously implemented by organisations across Pakistan. However, he expressed concerns that Pakistan's cybersecurity policy, currently under review in Parliament, does not address emerging technologies such as AI and cloud computing, emphasising the necessity of actionable policies rather than mere paper plans. Mr Ali also highlighted the need for securing institutions and critical infrastructure from adversaries. He concluded by stressing the importance of enhancing cyber-diplomacy; establishing international linkages to strengthen Pakistan's position in global cyberspace governance; and focusing on indigenous development in cybersecurity solutions.

Discussants Dr Zunera Jalil and Dr Kashif Kifayat from Air University also shared their views on the subject.

In his *Concluding Remarks* and *Vote of Thanks*, ***Air Marshal Javaid Ahmed (Retd)***, President CASS, Islamabad highlighted that nowadays, decision-making was entirely data-dependent, hence, it was crucial to secure data. He commended ongoing efforts within academia to bolster the cyber ecosystem through R&D. Discussing global technology dynamics, he opined that Pakistan would soon need to make strategic choices between aligning with Western or Eastern technological standards. President CASS stressed the importance of supporting existing areas of excellence within the country rather than focusing solely on vulnerabilities. He urged government policymakers to acknowledge and invest in Pakistan's human resources to enhance national cybersecurity capabilities.

Social Media Engagement

Twitter



Facebook


Centre for Aerospace & Security Studies
8 Jul
Air Marshal Javaid Ahmed (Retd), President, Centre for Aerospace & Security Studies, Islamabad delivering ... See more
Roundtable
Cyberspace as a Global Common: Formulation and Applicability of International Law
You and 3 others
Like
Comment
Send
Share


Centre for Aerospace & Security Studies
8 Jul
Air Marshal Zahid Mehmood (Retd) outlines the significant threats posed by cybersecurity challenges
#cassevent #roundtable #cybersecurity #InternationalLaw #globalcommon #futuretech
CASS
Threats
More and more countries becoming aware of these threats
Iran – Halal Internet
China – Behind the Great Fire Wall
US - International Cyberspace & Digital Policy Strategy
Pakistan ?
What does the future hold ?
You and 3 others
Like
Comment
Send
Share


Centre for Aerospace & Security Studies
8 Jul
No clear indication by all States that cyberspace should be regulated as a global common. States are territorial... See more
4
Like
Comment
Send
Share


Centre for Aerospace & Security Studies
8 Jul
Securing critical infrastructure systems is not simply a matter of operational efficiency; it is a matter of national security and sovereignty - Khawaja Mohammad Ali, Cyber Security, Data Privacy & Digital Forensics Expert, speaking at the CASS roundtable on 'Cyberspace as a Global Common'
#cassevent #roundtable #cybersecurity #InternationalLa
#globalcommon #futuretech
2
Like
Comment
Send

Instagram


cassthinkers
International Law, Cyberspace and the Global Commons
3 likes
cassthinkers The fundamental prerequisite for regulating global commons is state consensus that it should be treated as such, which is currently lacking - Jamal Aziz, Executive Director @rsilpak, at the CASS roundtable on 'Cyberspace as a Global Common'
#cassevent #roundtable #cybersecurity #InternationalLaw #globalcommon #futuretech
8 July


cassthinkers
Liked by ajwahijazi and 8 others
cassthinkers Indigenous cybersecurity development and technology are critical for building resilient and sovereign digital defences - Khawaja Mohammad Ali, Cyber Security Expert, speaking at the CASS roundtable on 'Cyberspace as a Global Common'
#cassevent #roundtable #cybersecurity #InternationalLaw #globalcommon #futuretech
8 July


cassthinkers
Liked by ajwahijazi and 4 others
cassthinkers Decision-making is entirely data-dependent, and data is a powerful tool; it is vital to secure it - Air Marshal Javaid Ahmed (Retd), President @cassthinkers , Islamabad, delivering concluding remarks at the CASS roundtable on 'Cyberspace as a Global Common: Formulation and Applicability of International Law'
#cassevent #roundtable #cybersecurity #InternationalLaw #globalcommon #futuretech
7 days ago
cassthinkers


cassthinkers
Liked by ajwahijazi and 9 others
cassthinkers And that's a wrap!
A thought-provoking roundtable on 'Cyberspace as a Global Common: Formulation and Applicability of International Law' with our eminent speakers advocating for a two-pronged approach: global cooperation enhanced by robust local measures for cyberspace governance. International norms should be complemented by strong national cybersecurity strategies, aiming to forge a secure, stable and resilient digital environment.
#cassevent #roundtable #cybersecurity #InternationalLaw #globalcommon #futuretech
7 days ago


Roundtable
Cyberspace as a Global Common:
Formulation and Applicability of
International Law
8 May 2024


2024

ABOUT CASS

Established in 2018, the Centre for Aerospace & Security Studies (CASS) in Islamabad is a non-partisan think tank offering future-centric analysis on aerospace and security issues. CASS engages with thought leaders and informs the public through evidence-based research, aiming to influence discussions and policies at the national, regional, and global level, especially concerning airpower, emerging technologies, traditional and non-traditional security.

VISION

To serve as a thought leader in the aerospace and security domains globally, providing thinkers and policymakers with independent, comprehensive and multifaceted insight on aerospace and security issues.

MISSION

To provide independent insight and analysis on aerospace and international security issues, of both an immediate and long-term concern; and to inform the discourse of policymakers, academics, and practitioners through a diverse range of detailed research outputs disseminated through both direct and indirect engagement on a regular basis.

CORE AREAS OF RESEARCH

Aerospace

Emerging Technologies

Security

Strategic Foresight

CASS www.casstt.com
CENTRE FOR AEROSPACE & SECURITY STUDIES, ISLAMABAD
Independence | Analytical Rigour | Foresight

cass.thinkers@casstt.com
+92 051 5405011
@CassThinkers
Centre for Aerospace & Security Studies
cassthinkers
cass.thinkers
Old Airport Road, Islamabad, Pakistan