



**ACDC**  
ARMS CONTROL & DISARMAMENT CENTRE

## ACDC SPECIAL REPORT

On

**“Comprehensive National Security  
and Emerging Technologies”**

**August 2022**



*Prepared for the 49th Foundation Day of the  
Institute of Strategic Studies Islamabad (ISSI)*

**Edited by:** Malik Qasim Mustafa (Director ACDC-ISSI)

**Prepared by:** Ms Ghazala Yasmin Jalil, Research Fellow, ACDC-ISSI

Ms Aamna Rafiq, Research Associate, ACDC-ISSI

**Composed &**

**Designed by:** Malik Qasim Mustafa (Director ACDC-ISSI)

**Published by:**

**The Arms Control and Disarmament Centre (ACDC)**

Institute of Strategic Studies Islamabad (ISSI)

Sector F-5/2, Islamabad, Pakistan.

Tel: 0092-51-9204423-24, 9205882, 9205886

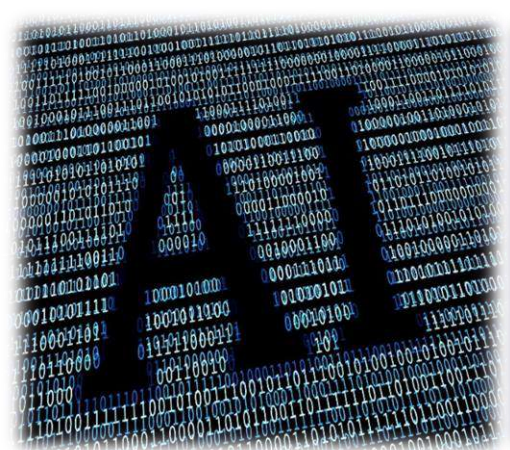
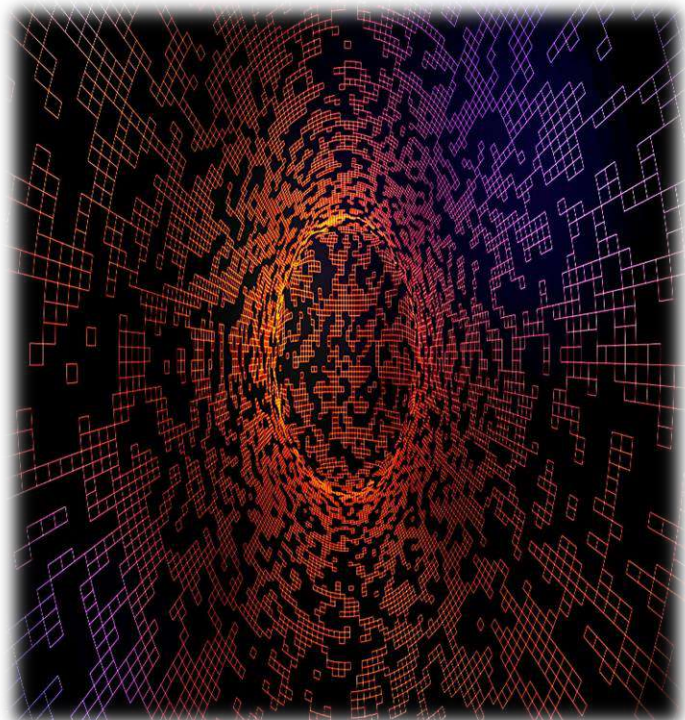
Fax: 0092-51-9204658

Email: [acdc@issi.org.pk](mailto:acdc@issi.org.pk)

Website: [www.issi.org.pk](http://www.issi.org.pk)

## Contents

<b>Introduction of ACDC</b>	<b>01</b>
<hr/>	
<b>Acknowledgment: 49th Foundation Day of ISSI</b>	<b>02</b>
<hr/>	
<b>Role of Emerging Technologies in Achieving Comprehensive National Security</b>	<b>03</b>
<hr/>	
<b>Cyber Technologies, Artificial Intelligence and International Security</b>	<b>08</b>
<hr/>	
<b>Securing Pakistan's Cyber Domain: Challenges and Opportunities</b>	<b>14</b>
<hr/>	
<b>Artificial Intelligence and National Security</b>	<b>19</b>
<hr/>	
<b>Artificial Intelligence for Socio-Economic Development in Pakistan</b>	<b>24</b>
<hr/>	
<b>Space Technologies for Socio-Economic Development in Pakistan</b>	<b>28</b>
<hr/>	
<b>Big Data for National Security: A Case of Pakistan</b>	<b>34</b>
<hr/>	
<b>Key Takeaways</b>	<b>38</b>
<hr/>	





# ACDC

ARMS CONTROL & DISARMAMENT CENTRE

## Introduction of ACDC

The Arms Control and Disarmament Centre (ACDC), which is a part of the Institute of Strategic Studies Islamabad (ISSI), was established on October 30, 2019, under the leadership of Ambassador Aizaz Ahmad Chaudhry, Director General ISSI. Mr Sohail Mahmood, Foreign Secretary of Pakistan, inaugurated the Centre.



The ACDC was established with a vision “to contribute focused research and quality policy input through in-depth analysis and dialogue on issues of arms control, disarmament, nuclear safety and security, nuclear deterrence, emerging technologies and challenges to peace and strategic stability.”

The ACDC performs the following key functions:

**Monitor** regional and international developments pertaining to strategic stability, disarmament, non-proliferation, arms control and related domains.

**Organise** dialogues in the form of in-house meetings, roundtable discussions, national and international seminars, conferences and workshops and book launches on themes of relevance to Pakistan.

**Disseminate** information through research projects, special reports, magazines, newsletters, info-graphs, electronic flyers and electronic and social media tools.

**Provide** quality policy inputs to the government and relevant official departments to promote and strengthen Pakistan’s narrative on nuclear issues and arms control and disarmament.

**Maintain** database and contacts with relevant official organisations, similar national and international think tanks, institutions and centres.

For overall guidance, policy directions, preparation of the annual Programme of Work and annual performance review, the ACDC has constituted its Advisory Board, which is comprised of representatives of government and official organisations, academia, think tanks, former diplomats and officials and experts.

## 49th Foundation Day of ISSI



To commemorate the “49th Foundation Day” of the Institute of Strategic Studies Islamabad (ISSI), the ACDC has dedicated the first half of the year 2022 to the ISSI’s theme of the year 2022, “National Security: Expanding Horizons.”

On this special day, the ACDC presents this Special Report on “Comprehensive National Security and Emerging Technologies,” to reinforce ISSI’s motto “Strategic Perspectives through Research and Dialogue.”

This research and the event-based special report also contribute to the core values of the ISSI i.e., “To provide quality policy inputs through informed research, objective analyses and dialogue on global and regional issues affecting peace, security and development of Pakistan.”



## **“Role of Emerging Technologies in Achieving Comprehensive National Security”**

*Malik Qasim Mustafa,  
Director, ACDC, ISSI*

## “Role of Emerging Technologies in Achieving Comprehensive National Security”

Malik Qasim Mustafa,  
Director ACDC-ISSI

Technology is a “fundamental agent of change,” which is not only changing our day-to-day life but has the potential to transform our future. In recent years, in the technology domain, the term “emerging technology” is gaining much attention. In a simplistic manner, “emerging technology” refers to the emergence of new technology or the continuing development of existing technology, with a significant impact on a single or across all domains including social, economic, human and traditional security ones. For example, the Internet of Things (IoT), Artificial Intelligence (AI), 3D printing, Quantum Computing, 5G, Block chain, autonomous weapon systems, drones, robotics, hypersonic missiles and other technologies are considered among some of the top emerging technologies. These emerging technologies are providing us with endless possibilities to achieve progress, growth, peace and prosperity and a sustainable future. The world is witnessing this technological revolution and like other developing nations, Pakistan should benefit from this technological revolution. Pakistan strongly believes that the application of emerging technologies is set to reshape the future of societies and economies and can play an important role in achieving the goals of comprehensive national security - social, economic, human and traditional security.<sup>1</sup> Although access to such technologies, their application and the realisation of their true potential, sometimes create complex challenges. However, it is the right time for Pakistan to invest its time and resources in key emerging technologies. With this premise, this Special Report prepared by the ACDC aims to explore the role of some of the key emerging technology in achieving comprehensive national security.<sup>2</sup>



Today, emerging technologies are impacting almost all aspects of human life—traditional and non-traditional. In the traditional security domain, military modernisation programmes are a major driver of world-changing technological innovations, which are not only advancing fast but also are impacting weaponry, military operations, wartime preparations and defence budget priorities.<sup>3</sup> States are utilising emerging technologies for military superiority and battlefield dominance, which is already altering the “balance of power” and fuelling up new regional and global arms races. For instance, the 2018 US National Defence Strategy clearly outlines that new technologies like big data analytics, AI, autonomy, robotics, directed energy, hypersonic and biotechnology are the very technologies that ensure that the US will be able to fight and win the wars of the future.<sup>4</sup> Consequently, new regional and global “Strategic Competitions” are evolving. States are investing heavily in the development of new advanced conventional

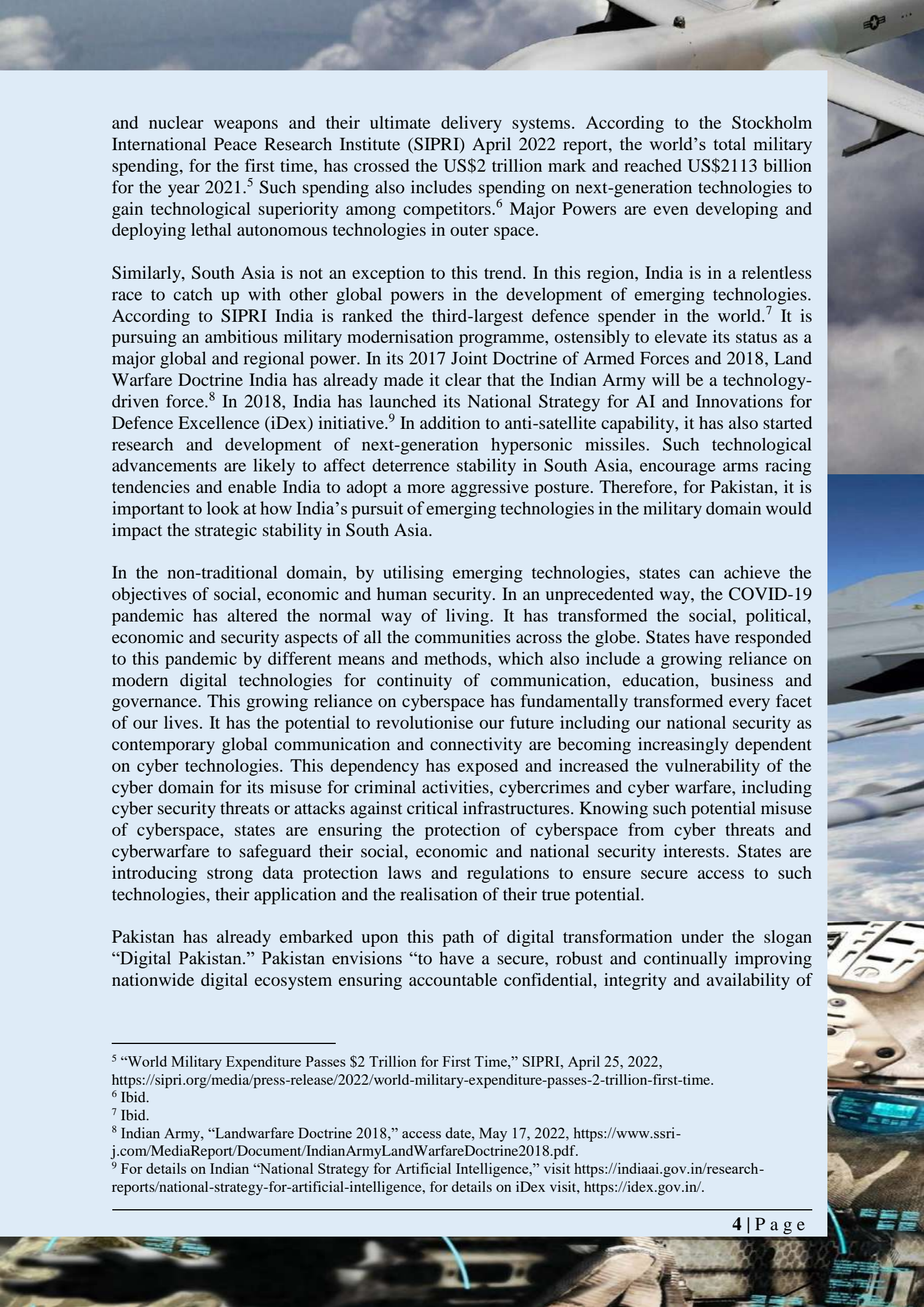
<sup>1</sup> For details see, National Security Division (NSD), Government of Pakistan, *National Security Policy of Pakistan 2022-2026*, NSD, 2022.

<sup>2</sup> This report is a compilation of research articles and reports of a series of events, which were organised by the ACDC around the theme “Comprehensive National Security and Emerging Technologies.” This special report is prepared to commemorate the “49th Foundation Day” of the Institute of Strategic Studies Islamabad (ISSI).

<sup>3</sup> Michael E O’Hanlon, “Forecasting Change in Military Technology, 2020-2040,” Brookings, September 2018, <https://www.brookings.edu/research/forecasting-change-in-military-technology-2020-2040/>.

<sup>4</sup> The US Department of Defence, the United States of America, *Summary of 2018 National Defence Strategy of the United States*, January 22, 2018, available at, <https://www.hsdl.org/c/2018-national-defense-strategy/>.





and nuclear weapons and their ultimate delivery systems. According to the Stockholm International Peace Research Institute (SIPRI) April 2022 report, the world's total military spending, for the first time, has crossed the US\$2 trillion mark and reached US\$2113 billion for the year 2021.<sup>5</sup> Such spending also includes spending on next-generation technologies to gain technological superiority among competitors.<sup>6</sup> Major Powers are even developing and deploying lethal autonomous technologies in outer space.

Similarly, South Asia is not an exception to this trend. In this region, India is in a relentless race to catch up with other global powers in the development of emerging technologies. According to SIPRI India is ranked the third-largest defence spender in the world.<sup>7</sup> It is pursuing an ambitious military modernisation programme, ostensibly to elevate its status as a major global and regional power. In its 2017 Joint Doctrine of Armed Forces and 2018, Land Warfare Doctrine India has already made it clear that the Indian Army will be a technology-driven force.<sup>8</sup> In 2018, India has launched its National Strategy for AI and Innovations for Defence Excellence (iDex) initiative.<sup>9</sup> In addition to anti-satellite capability, it has also started research and development of next-generation hypersonic missiles. Such technological advancements are likely to affect deterrence stability in South Asia, encourage arms racing tendencies and enable India to adopt a more aggressive posture. Therefore, for Pakistan, it is important to look at how India's pursuit of emerging technologies in the military domain would impact the strategic stability in South Asia.

In the non-traditional domain, by utilising emerging technologies, states can achieve the objectives of social, economic and human security. In an unprecedented way, the COVID-19 pandemic has altered the normal way of living. It has transformed the social, political, economic and security aspects of all the communities across the globe. States have responded to this pandemic by different means and methods, which also include a growing reliance on modern digital technologies for continuity of communication, education, business and governance. This growing reliance on cyberspace has fundamentally transformed every facet of our lives. It has the potential to revolutionise our future including our national security as contemporary global communication and connectivity are becoming increasingly dependent on cyber technologies. This dependency has exposed and increased the vulnerability of the cyber domain for its misuse for criminal activities, cybercrimes and cyber warfare, including cyber security threats or attacks against critical infrastructures. Knowing such potential misuse of cyberspace, states are ensuring the protection of cyberspace from cyber threats and cyberwarfare to safeguard their social, economic and national security interests. States are introducing strong data protection laws and regulations to ensure secure access to such technologies, their application and the realisation of their true potential.

Pakistan has already embarked upon this path of digital transformation under the slogan "Digital Pakistan." Pakistan envisions "to have a secure, robust and continually improving nationwide digital ecosystem ensuring accountable confidential, integrity and availability of

---

<sup>5</sup> "World Military Expenditure Passes \$2 Trillion for First Time," SIPRI, April 25, 2022, <https://sipri.org/media/press-release/2022/world-military-expenditure-passes-2-trillion-first-time>.

<sup>6</sup> Ibid.

<sup>7</sup> Ibid.

<sup>8</sup> Indian Army, "Landwarfare Doctrine 2018," access date, May 17, 2022, <https://www.ssri-j.com/MediaReport/Document/IndianArmyLandWarfareDoctrine2018.pdf>.

<sup>9</sup> For details on Indian "National Strategy for Artificial Intelligence," visit <https://indiaai.gov.in/research-reports/national-strategy-for-artificial-intelligence>, for details on iDex visit, <https://idex.gov.in/>.

digital assets leading to socio-economic development and national security.”<sup>10</sup> To materialise this digital transformation, Pakistan has taken several initiatives including drafting Pakistan’s Cyber Security Policy 2021 and attaches top priority to securing Pakistan’s cyberspace in its National Security Policy 2022-2026.<sup>11</sup> However, there is a need to raise awareness, promote cyber security culture, bridge the technological divide, develop cyberspace norms and address other related challenges at the national level.

Similarly, emerging technologies can help rapidly achieve 17 life-changing goals, commonly known as Sustainable Development Goals (SDGs) set by the UN in 2015. Emerging technologies can help reduce poverty, reduce carbon emissions, revolutionise global connectivity, transform global mobility and can make advances in health care, education, agriculture and energy sectors. Pakistan was among the first counties to endorse and adopt 17 ambitious SDGs as its 2030 Agenda for Sustainable Development in Pakistan.<sup>12</sup> Regarding the SDGs, Pakistan has already entered into the “decade of action.”<sup>13</sup> The main objective is to identify key emerging technologies and their impact on the 2030 Agenda for Sustainable Development in Pakistan.

Regarding AI, it is now widely believed that AI is one of the major driving forces of the fourth Industrial Revolution and it has the potential to bring socio-economic development to a country. The COVID-19 pandemic has shown us how digital technologies and AI-based models have addressed public health management challenges. Likewise, AI can play a substantive role in achieving 17 UN SDGs that are the building blocks of the 2030 agenda for sustainable development. Hence, it is high time for Pakistan to harness AI for its socio-economic development, as AI can play a major role in urban planning and monitoring, smart cities, precision agriculture and food production, water resource management and the health sectors.

Regarding big data, experts believe that a large volume of a complex data set, which is received at a fast velocity rate and contains greater variety, can influence every aspect of individual human life and society and the global landscape. It enables everything from access to knowledge and global communication to the delivery of services and infrastructure. Big data analytics is positively transforming the ways of doing business, trade, governance, politics, communications and social services. However, it is also creating new, novel, inescapable and unpredictable international, national and individual security challenges. Therefore, its misuse can equally exacerbate national security threats and can create new and unpredictable ones.

<sup>10</sup> Ministry of Information Technology & Telecommunication (MOITT), Government of Pakistan, *National Cyber Security Policy 2021*, MOITT, July 2021, <https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf>.

<sup>11</sup> Ibid.

<sup>12</sup> Government of Pakistan, *Pakistan’s Implementation of the 2030 Agenda for Sustainable Development: Voluntary National Review, 2019*,

[https://sustainabledevelopment.un.org/content/documents/233812019\\_06\\_15\\_VNR\\_2019\\_Pakistan\\_latest\\_version.pdf](https://sustainabledevelopment.un.org/content/documents/233812019_06_15_VNR_2019_Pakistan_latest_version.pdf).

<sup>13</sup> “National Initiative for Sustainable Development Goals, <https://www.sdgpakistan.pk/> and “The UN and Pakistan,” UNSDG, <https://unsdg.un.org/un-in-action/pakistan>.

Pakistan recognises the potential and reaches of big data for socio-economic development and national security challenges. Big data is an unexplored and uncharted territory in Pakistan. However, there is a need to identify the potential spectrum for designing the normative and legal framework at the national level for big data. This requires a comprehensive and result-oriented discussion among all relevant stakeholders like policymakers, diplomats, the private sector, technical community, civil society and academia.

This growing reliance on technology has put tremendous pressure on global technological infrastructure, including cyberspace. Therefore, it is the collective responsibility of technologically advanced states to share and transfer technological expertise to the developing states for the greater good. In this regard, there is a need to develop an emerging technology sharing mechanism at the regional and international levels.

To formulate policy recommendations to ensure sustainable development and comprehensive national security by utilising the true potential of emerging technologies in Pakistan the ACDC in the first half of the year 2022 organised webinars, web talks and wrote extensively on some of the key emerging technologies. The main purpose was to explore the potential of these emerging technologies and purpose a recommendation based road map/ a way forward for Pakistan to follow. Following are some key arguments and questions that were raised in these activities and ACDC research to understand the evolving concept and explore the key characteristics of emerging technologies:

- In this digital age, the emergence of the COVID-19 pandemic has increased the excessive use of communication technologies by people, businesses and state institutions. In this regard, there is a need to explore what kind of stress it can place on the existing digital landscape of Pakistan and what are the options to overcome this stress.
- Although the use of technology as a “new normal” has brought its benefits at all levels, however, it has exposed us to new risks and challenges. Therefore, there is a need to analyse that what are the prospects and challenges of this overreliance on technology and how it is going to impact a state’s national security.
- This global interconnected digital communication infrastructure is helping us to virtually communicate with each other. However, this raise very important questions, how we can identify major cybersecurity threats and enhance the credibility and security of digital communication?
- How this new normal will impact the development of new technologies in the short, medium and long term?
- There is also a need to explore the prospects of international cooperation for developing, mutually beneficial, technologies to cope with such situations. What role the international community can play to develop new technologies?
- What are the practicalities of Block chain for the SDGs in Pakistan?
- How can we use Digital Economy for rural development in Pakistan?

- What are the challenges related to malicious activities in cyberspace and their implications on peace, security and development in Pakistan?
- How can we ensure the cyber safety and security of critical infrastructure?
- How can we enhance our national information security?
- What are the challenges for Pakistan in building a national cyber recovery model?
- How can we build a national cyber security culture in Pakistan?
- There is a need to identify the socio-economic opportunities and security challenges posed by big data in Pakistan.
- How to analyse the various ways to enhance responsible behaviour and mechanisms vis-à-vis big data management in Pakistan.
- What is the way forward for Pakistan for building a national framework for Big Data?
- What should be our technology roadmap: A Way Forward for Pakistan?





**Two Day Online Workshop**  
on  
**“Cyber Technologies, Artificial Intelligence  
and International Security”**

*January 24-25, 2022*

## Two Day Online Workshop

on

### “Cyber Technologies, Artificial Intelligence and International Security”



The Arms Control & Disarmament Centre (ACDC) at the Institute of Strategic Studies Islamabad (ISSI) organised a two-day online workshop on “Cyber Technologies, Artificial Intelligence and International Security” in collaboration with the United Nations Institute for Disarmament Research (UNIDIR), Geneva on January 24 -25, 2022.

The opening session was moderated by Ms Moliehi Makumane, Researcher, UNIDIR. In opening remarks, Ambassador Aizaz Ahmad Chaudhry, Director General ISSI, said that every new century has witnessed the emergence of new technologies. In the present one, AI and cyber technologies have opened new vistas of cooperation. However, they also have the potential to undermine international security as well.

In his welcome remarks Dr Robin Geiss, Director UNIDIR, said that in this hybrid workshop and discussion on AI, cyber technologies and international security it is important to work toward a more secure world. While Ambassador Khalil Hashmi, Pakistan’s Permanent Representative to the UN, said that even as discussions of how to approach and address the military application of cyber and AI technologies have taken place for several years at the UN, meaningful progress on developing, commensurate principles and morals remains elusive. Pakistan has continued to call for the development of commensurate legal rules promptly, failing and many states would feel obliged to develop these capabilities to defend themselves.

Session I on “Cybersecurity 101” was moderated by Dr Andraz Kastelic, Researcher, UNIDIR. The speakers introduced key concepts of cybersecurity that are relevant to contemporary conversations. Dr Mehreen Afzal, Associate Professor, Department of Cybersecurity, Air University, Islamabad, said that cyber security is key to contributing to having a secure life, not only at the individual level but also at the corporate, organisational and national levels. She recommended a hybrid approach to deal with cyber threats—a combination of education and effective security controls. While Dr Samuele Dominioni, Researcher UNIDIR, talked about the political and international security dimensions of cybersecurity, the transformative developments in the cyber domain and their impact on security. He also talked about the international community’s efforts at regulating cyberspace including the development of confidence-building measures (CBMs). He recommended that the international community’s efforts at regulating cyberspace should be strengthened and the need for more international efforts to understand the consequences on the victim of cyber threats. He also stressed the need to provide capacity-building support to other countries, which is an enabler to increasing stability and security globally.

Session II on “Cybersecurity and UN” was moderated by Dr Tughral Yamin, Dean CIPS, NUST. Mr Usman Jadoon, Director General, UN Division, Ministry of Foreign Affairs, Pakistan, in his presentation said that Information and Communications Technologies (ICTs) have reshaped and transformed every aspect of our lives, economies and societies. Progress in this field today is both a measure and a driver of economic growth and prosperity. However, malicious use of ICTs risks undermining its benefits. The unregulated use of cyberspace for military purposes poses a serious challenge to international peace and security. He characterised the hostile use of cyber as a weapon of mass destruction. He recommended developing a legally binding international instrument, specifically tailored to the unique attributes of ICTs, to provide a regulatory framework that creates stability and security in cyberspace. He recommended the need to bridge the digital divide between developed and developing countries for the global transition to modern and efficient national economies and effective international cooperation, as well as to enhance the objective of cyber security. In her presentation, Ms Makumane took a deeper dive into the current discussions at the UN in the open-ended working group and reflected on the true consensus reports of GGE and OEWG both of which came out in 2021. During the discussion at the UN, member states have also added the threat of ransomware and called for more regulations on the use of emerging technologies that may include the dark web blockchain, mass data collection, facial recognition, cloud computing and AI. She recommended a deeper appreciation of the issues of information security - the disinformation and misinformation, terrorists’ use of ICTs and espionage and the need for greater discussion, sharing of views and dialogue at UN forums.

Session III on “Responsible and Coordinated Vulnerability Disclosure” was moderated by Dr Kastelic. It explores normative approaches including the concept of vulnerability disclosure and how it could be implemented. In his presentation by Mr Ahmer Bilal Soofi, former Federal Minister of Law, Justice, Parliamentary Affairs and Human Rights, defined what a vulnerability disclosure is and delved into various types of vulnerabilities. He also highlighted vulnerability disclosures in Pakistan and discussed its benefits. He emphasised the formulation of a Vulnerability Disclosure Policy whereby all the relevant stakeholders could be involved in the creation of a safer digital space in Pakistan. He also emphasised the formulation of a “Vulnerability Disclosure Policy” whereby all the relevant stakeholders could be involved in the creation of a safer digital space in Pakistan. While Ms Kaja Ciglic, Senior Director, Digital Diplomacy, talked about the idea of a global perspective of coordinated vulnerability disclosure and its latest trends. She stated that security vulnerability is effectively a weakness a computer

product can have that allows a hacker to exploit the system. To report the vulnerability, companies have a vulnerability disclosure policy. She said that there are international cybersecurity standards in the space as well. She said that the importance of vulnerability disclosure has increased over the years, over 100 tech companies have opted for a coordinated vulnerability disclosure process. She recommended the need for governments to play a vital role in encouraging good behaviours. They can develop CVD policies in collaboration with the industry by leading through examples of their systems. Governments can also create bug bounty programmes. She recommended legal exemptions for security researchers so they are not prosecuted, bringing together the stakeholders to highlight the importance of coordination.

Session IV on “Global Supply Chains” was moderated by Dr Dominioni. In her Presentation Ms Anastasiya Kasovca, Senior Manager for Public Affairs, Kaspersky, introduced the concept of supply chain security and thus helped to conceptualise how, as a company, as a vendor, they are also an industry partner. She also touched on the challenges of supply chain attacks and how to address those threats and a possible way forward or some particular micro trends in the coming years. To address the challenge of supply chain attacks, she suggested the growing regulatory compliance and the growing government’s efforts to ensure the security of supply chains; both on the industry side and the consumer side and build cyber defences. While Mr Khawaja Ali, Head of Technology Strategy, Risk & Governance, National Bank of Pakistan, discussed the technicalities of cyber security and how the global supply chain is linked to all the technology. He said that the definition of critical infrastructure has changed from the protection of nuclear assets, protecting military assets to the civil side of the infrastructure that increasingly runs through the global supply chain. He said that due to more reliance on the IoT, there is a greater risk of a cyber-attack on global supply chains. He emphasised the need for civil-military cooperation in cybersecurity, which is the fifth domain of defence.

In closing remarks on day 1, Dr Giacomo Persi Paoli, Head of Programme, UNIDIR, said that the private sector has a key role to play in cybersecurity. Governments have remained the key actors when it comes to policy and decision-making. However, as the world is becoming increasingly digitised, other private-sector actors need to be civilised and educated as well. The power of the market should not be underestimated. He said that not everything has to be resolved using treaties or conventions but rather by leveraging the expertise of the private sector.





The second day was opened with remarks by Dr Cécile Aptel, Deputy Director, UNIDIR, who said that Lethal Autonomous Weapons Systems (LAWS) are at the heart of the discussion at the UN GGE. It is important to discuss the legal and ethical implications of developments in the field of LAWS. She highlighted the technical complexities that states have to grapple with LAWS and autonomy and the importance of discussing the dual-use nature of the technology and its implications for international security.

Session I on “Artificial Intelligence and Autonomy 101” was moderated by Ms Ioana Puscas, Researcher, UNIDIR. Speakers included Dr Yasar Ayaz, CPD/Chairman at National Center of Artificial Intelligence (NCAI) & Professor of AI & Robotics at NUST, Islamabad, and Dr Giacomo Persi Paoli, Head of Programme, UNIDIR. Mr Paoli explained key concepts involved in AI and autonomy. AI systems range from deterministic, which are fully predictable to Non-Deterministic, which is less predictable. Talking about the role of humans in AI he said that it ranges from full direct control i.e. no autonomy, to humans in the loop where humans need to validate and humans in the loop where humans intervene if necessary. He recommended that there is a need to look at autonomous systems beyond algorithms and also focus more on the availability of digitalised big data and improving computing power. Dr Ayaz spoke on how can AI be used for the benefit of humans. It is already been used widely in finance, judiciary and medical science in Pakistan. He underscored how it is a transformative technology with immense economic benefits. AI software market revenue worldwide was over US\$34 billion in 2021 and is expected to increase. Countries are investing hundreds of billions of dollars in AI. While talking about the misuse of AI, he said that there is a need to demilitarise emerging technologies.

Session II on “AI, Autonomy and UN” was moderated by Mr Usman Jadoon, Director General, UN Division, Ministry of Foreign Affairs, Pakistan. Speakers included Ms Aamna Rafiq, Research Associate, ACDC-ISSI and Ms Ioana Puscas UNIDIR. Ms Puscas said that discussions started on LAWS at the UN in 2014 and 11 guiding principles were adopted in

2019. She identified two distinct positions that have emerged at the UN—one that endorses the need to develop specific law in the contest of Autonomous Weapons Systems (AWS) and the second position endorses non-legally binding instruments. While there is agreement on the need for compliance with international humanitarian law, no consensus was reached over substantive matters of the 2021 GGE meeting. Ms Rafiq discussed the way forward based on the 11 principles that have been adopted at GGE. However, she opined that in all situations international humanitarian law should be applicable and respected. She highlighted the need for implementation mechanisms and proposals at the UN like the national legal reviews and establishing links between national and international regulations.

Session III on “Black Box Unlocked: Predictability and Understanding of AI Systems” was moderated by Dr Giacomo Persi Paoli. Speakers were Major General (Retd) Ausaf Ali, Advisor Strategic Plans Division, Pakistan and Dr Pascale Fung, Director, Centre for Artificial Intelligence Research, Professor, Hong Kong University of Science and Technology. Maj Gen Ali in his presentation stated that predictability and understandability are widely held to be the vital qualities of AI systems and represent an important point among the many different parties to the debate on emerging technologies in the area of LAWS and other forms of military AI. He also raised concerns regarding the AI system including extensive use in military applications, absence of legal framework, open-source access to AI system and third party risk amongst others. He proposed that for AI to be used effectively and appropriately, there needs to be a balance between extensive support and regulation for the use of AI. Dr Fung spoke on natural language processing in terms of AI systems and modern AI. She was of the view that there are multiple issues that can be seen with the use and emergence of AI technologies including superior privacy, safety, sustainability and environment, legality, fairness and source bias amongst others. She shed light on the common ethical principles that are common between the Chinese government and the EU and around the world like fairness and justice, privacy, safety, interoperability, diversity, environmental wellbeing etc. During her presentation, she shed light on the foundational models and is trained for the existing text on the internet with parameters called language models, which are then used for various other tasks. To avoid the harmful social impacts of questabale data, there is a need to take care of ethical principles during data creation, curation, adaption and deployment.

Session IV on “Data and Autonomous Systems” was moderator by Dr Rabia Akhtar, Director CSSPR, Lahore. Speakers included Air Cadre (Retd) Khalid Banuri, former Director General, Arms Control and Disarmament Affairs, Strategic Plans Division, Pakistan and Mr Arthur Holland Michel, Senior Fellow, Carnegie Council for Ethics in International Affairs. Mr Holland during his presentation was of the view that all the autonomous systems and machines that operate without humans at any given stage of operation require data. However, a machine supersedes the environment and acts appropriately according to the data and at times can create problems with the data that the autonomous system collected. He reiterated that machine learning relies highly on the knowledge which is developed through a process. He opined that it is impossible to train autonomous systems with a wide variety of data that exists in real-time complex situations. To deal with this paradox, there is a need to accept the fact that all autonomous systems will fail at a certain level. Air Cadre (Retd) Banuri while making his remarks stated that today’s world is increasingly becoming a complex world both politically and technologically. While recommending the hybrid military operations, he suggested that hybrid military operations require a lot of teamwork and interactions involving a lot of human aspects, a key element missing in machine operating systems. Therefore, it is necessary to always keep humans in the loop.

The closing session of day 2 was moderated by Malik Qasim Mustafa, Director ACDC-ISSI. In closing remarks Dr Paoli while concluding the two-day workshop proceedings stressed the importance and significance of the issues of cyber technology and AI. He made a note of thanks to the Government of Pakistan and ACDC at ISSI for conducting the workshop. In his concluding remarks Ambassador Khalid Mahmood, Chairman BoG, ISSI, stated that it has been a learning experience. He stated that what is important is to improve human involvement in the larger system and make sure the use of ethical grounds on issues dealing with technologies and cyberspace. There is a need to put in place legally binding instruments along with confidence and capacity-building measures. However, this requires political will and constructive engagement.

Ambassador Zaman Mehdi, Deputy Permanent Representative of the Permanent Mission of Pakistan to the UN, Geneva, expressed gratitude to ISSI and the team at UNIDIR while making his Note of thanks. He stated that the workshop led to fruitful discussion and has set the discourse of debate on a pressing issue.



$$ab+ac=a(b+c)$$
$$\frac{a}{\frac{b}{c}} = \frac{ab}{c}$$
$$\frac{\frac{a}{\frac{b}{c}}}{\frac{d}{e}} = \frac{ac}{b}$$
$$\frac{a}{\frac{b}{\frac{c}{d}}} = \frac{ad+bc}{bd}$$

$$X^2 - 4X + 5 \leq 5$$
$$X^2 - 4X \leq 0$$

$$n(B \cap C) = 22$$
$$n(B) = 68$$
$$n(C) = 84$$

$$n(B \cup C) = n(B) + n(C) - n(B \cap C)$$

$$x = \frac{1+3+3+6+8+9}{6} = 5$$

$$y = \frac{2+4+4+8+12}{5} = 30$$

$$z = \frac{4+7+1+6}{3} = 18$$



He = 4.002602  
Na = 22.989769  
Ar = 39.948



$$\log_b b = x$$
$$\log_a x = \frac{\log_b x}{\log_b a}$$
$$\log_{b^r}(x) = r \log_b x$$
$$\log_a(xy) = \log_a x + \log_a y$$
$$\log_a\left(\frac{x}{y}\right) = \log_a x - \log_a y$$



$$a(bc) = (abc)$$
$$a+b = b+a$$
$$a(b+c) = ab+ac$$

$$126 = 6xy$$
$$2x + 2y = 20$$

$$(100^2)a + 100b$$
$$10000a + 100b - 5$$

$$a_n = \frac{1}{2^{n-1}}$$
$$= \frac{1}{2^9} =$$

$$y = ax + b$$

$$|a| = |-a|$$
$$|a| \geq 0$$
$$ab = |a||b|$$





**Webinar**  
on  
**“Securing Pakistan’s Cyber Domain:  
Challenges and Opportunities”**

*March 16, 2022*

## Webinar

on

### “Securing Pakistan’s Cyber Domain: Challenges and Opportunities”



The Arms Control and Disarmament Centre (ACDC) at the Institute of Strategic Studies Islamabad (ISSI) organised a webinar on “Securing Pakistan’s Cyber Domain: Challenges and Opportunities” on March 16, 2022. The webinar was moderated by Malik Qasim Mustafa, Director, Arms Control & Disarmament Centre (ACDC).



In his welcome remarks, Malik Qasim Mustafa, Director, ACDC, said that the growing reliance on cyberspace has fundamentally transformed every facet of our lives. It has the potential to revolutionise our future including our national security as contemporary global communication and connectivity are becoming increasingly dependent on cyber technologies. This dependency has exposed and increased the vulnerability of the cyber domain for its misuse for criminal activities, cybercrimes and cyber warfare, including cyber security threats or attacks against critical infrastructures. Knowing such potential misuse of cyberspace, states are ensuring the protection of cyberspace from cyber threats and cyberwarfare to safeguard their social, economic and national security interests. States are introducing strong data protection laws and regulations to ensure secure access to such technologies, their application and the realisation of their true potential.

Pakistan has already embarked upon this path of digital transformation under the slogan “Digital Pakistan.” Pakistan envisions “having a secure, robust and continually improving nationwide digital ecosystem ensuring accountable confidentiality, integrity and availability of digital assets leading to socio-economic development and national security.” To materialise this digital transformation, Pakistan has taken several initiatives including drafting Pakistan’s Cyber Security Policy 2021 and attaches top priority to securing Pakistan’s cyberspace in its

National Security Policy 2022-2026. However, there is a need to raise awareness, promote cyber security culture, bridge the technological divide, develop cyberspace norms and address other related challenges at the national level. This requires a comprehensive and result-oriented discussion among all relevant stakeholders.



Dr Siraj Ahmed Shaikh, Professor of Systems Security, Coventry University, UK, shared his views on “Ensuring Cyber Safety and Security of Critical Infrastructure.” While talking about the strong national security and a critical infrastructure perspective on many cyber-physical systems, he laid out the premise of the problem at hand. There are two fundamental differences when experts talk about cyber security. One is the computer system that is right in front of us. It is all the data and the code. These are traditional computers and traditional IT equipment networks in some way. It may have a security implication because of any

malicious kind of manipulation but largely its impact is confined to either some data disclosure or some disruption.

The second part of this problem domain is the cyber-physical systems. These are usually safety-critical systems that have some physical manifestation so they could be smart home cameras. But more importantly critical infrastructure could be anything from transport infrastructure that could be maritime vessels that could be cars on the road health care infrastructure so that could be hospitals connected for some critical surgery delivery and so on military systems that could be used for all kinds of defensive offensive kind of capabilities. For a nation-state and several other infrastructures that could be rather scoped into that. Therefore, the security of those traditionally somewhat safely critical systems is then a completely different subject that requires of course an understanding of the threat actor because a very serious player usually with some state backing and some serious non-state backing poses any threat to that. It also involves a deeper understanding of not just traditional computer science and networking but engineering electronics, control systems, communication systems and a number of those technologies that may be relevant to the domain itself. This makes the subject very complicated.

There are two things when it comes to developing and maturing capabilities for security and safety-critical systems. They are much-related domains but they are fundamentally different domains. Therefore, for any nation-state, the first thing we want to think about is where the risk ownership and the operational ownership for these sectors are. For example, if we were talking about smart home systems or even automotive systems then the private sector usually would have many standards of best practices and regulatory authority that would look at traditional safety issues to comply so the systems would comply with certain safety regimes. Increasingly, they would set up bodies where they share threats or they would regulate various compliance regimes and so on to make sure that products are complying with some safety requirements so there are international standards.

In the context of Pakistan, how do we structure that kind of risk ownership and that sectoral ownership? It cannot be the one cyber body overlooking all of this, there may be which could facilitate but it needs sectoral knowledge. However, there are systemic risks that lie within those different sectors. The automotive industry has a different understanding of functional safety and road safety than the nuclear power industry would have. Therefore, there are

different levels of maturity. It is important to think about whether the state takes ownership in the case of energy systems and whether the private industry takes ownership when it comes to automotive systems. Before getting into regulation that kind of structure is very important. It is also important to make sure of a healthy structure and ecosystem. Safety is a much more established regime in terms of knowledge, certifications and standards. How do typical mature economies address this? The role of local adoption of standards and best practices is very important. Global standards may be very useful but an automotive security standard would be implemented differently in Japan and Germany, very mature economies than in developing regions such as South Asia. Therefore, in the safety world experts have acknowledged a reference architecture.



Dr Haider Abbas, Director, National Cyber Security Auditing & Evaluation Lab, Military College of Signals (MCS) – NUST, spoke on “National Information Security: Lessons for Pakistan.” He highlighted the increasing dependency of states on cybersecurity. He said that we are living in an era where most of the critical infrastructures are dependent on cybersecurity in which a big number of wired and wireless devices are making things extremely complex. The emerging critical threats in the cyber domain are going to affect the economy of a state. Cyberwarfare combined with electronic warfare becomes even more dangerous for nation-states.

While talking about the major categories of cyberattacks against Pakistan, he said that they could be divided into three categories: against people, against organisations and government. Due to the recent Pegasus attack that compromised several devices, there is a potential risk that critical information has been leaked. Dr Abbas also mentioned recent cyberattacks on the Careem and the FBI websites by the Indian hackers. The cyber threat landscape of Pakistan shows that these attacks affected people at all levels. One of the major reasons behind these successful attacks is the state’s huge reliance on the third party rather than on initiating national cyber security initiatives at a different level. The official data is being compromised due to weak cyber security mechanisms followed by the public sector organisations without any risk assessment mechanism. Additionally, the common use of pirated software and the same password by multiple users increases the security risks. Despite PTA’s restrictions, banned sites are still accessible through different software. Furthermore, there is a general careless attitude in people vis-a-vis data.

There is a need to raise awareness about cybersecurity to ensure good cyber hygiene. Moreover, there is a need to develop technical solutions and make them available at the organisational and individual levels. Every organisation must formulate its cybersecurity policy, perform a risk assessment of the organisation to figure out its vulnerabilities, install firewalls and anti-virus on their personal as well as official devices and use multi-factor authentication. Other measures include the establishment of national, development of indigenous tools to facilitate audit and compliance mechanisms, the introduction of indigenous software and training of human resources to ensure the physical protection of cyberinfrastructure and the establishment of national and sectorial CERTS for rapid crisis management.





Professor Dr Khashif Kifayat, Director, National Centre for Cybersecurity, Air University, Islamabad, presented his views on “Building National Cyber Disaster Recovery Model and Challenges for Pakistan.” He said that cyber security is not Pakistan’s problem only but it is a transnational phenomenon. Globally these attacks from malicious actors affect people. Pakistan is highly motivated to protect its critical assets and the public. To achieve that goal, Pakistan has introduced its National Security Policy and the National Cybersecurity Policy. If Pakistan is motivated to eradicate the cybersecurity issues, then it should develop a technical as well as a non-

technical skill set.

From the technical side, many public sector organisations are unaware of the actual magnitude of the cyber threat and data loss due to a lack of information and cyber security awareness. To enhance speed and quality of response, the government should first identify the critical assets and perform a comprehensive risk assessment. A heavy loss could be avoided by establishing a multi-layered defence mechanism and making the organisation aware of it. Most of the time, a cyberattack is not just about one time damage, it’s about the critical data theft that could be misused for several diverse attacks with serious consequences in future. On the non-technical side, the government should initiate proper alertness that includes a massive awareness campaign, especially in educational institutes. A human being is an asset that lies at the core of cyberspace. Therefore, the state should also work on building the technical capacity of the public to defend themselves from malicious attacks. The state should make the data protection measures mandatory for every organisation operating in Pakistan. The state should also make sure that everyone must be aware of cybersecurity from the top executives to lower employees.



Ms Aamna Rafiq, Research Associate, ACDC-ISSI, made a presentation on “Creating National Cyber Security Culture in Pakistan.” she said that cybersecurity culture is not a properly defined concept due to a difference in understanding of what demarcates a cybersecurity culture. Academic and industrial research has led to the development of a clearer definition of what a cybersecurity culture is. “Cybersecurity culture is the human behaviour that protects organisational information through compliance with the organisation’s security policies and procedures and an understanding of how to execute them as embedded through initiatives such as training, education,

awareness and communication.” Cybersecurity culture could also be described as a way that things are done. It consists of secure behaviours that have become habitual and require less cognitive effort. It is also known to be an effective tool that helps manage the human factors within cybersecurity because employee individual is known to either create or reduce vulnerabilities.

While highlighting the significance of cybersecurity culture, she said that managing cyber defences only through borrowed tactics from the annals of traditional warfare, with an increasing emphasis on securing all boundaries and delivering a knockout is no longer effective. In the contemporary interconnected world, the digital boundaries are becoming more and more porous. Furthermore, the civilian roles of cyber technologies are expanding. A growing number of essential business functions are being performed online. However, the

nature of cybercrime is also maturing and mutating. The increasing sophisticated cyberattacks require a coordinated team effort based on the principle of shared responsibilities. The security culture of the state has its specific dynamics and boundaries that decide what can be securitised. The national security culture is securitised at a general level in such a way that any new security issue automatically moves to the already securitised area of traditional security. In Pakistan, cybersecurity operated in the absence of relevant institutions or under the domination of the institutions established because of other types of securitisations. Furthermore, there is an absence of resonance between the public and national cybersecurity narrative. Presenting something like an existential threat to cybersecurity does not necessarily result in securitisation. Pakistan should focus on building the credible voices of cybersecurity for a resolute acceptance of cybersecurity policy, laws and culture. She also recommended measures to be taken in political, economic, legal, management, and monitoring domains.

**Table 1: Approaches and Measures to Strengthen Cybersecurity Culture in Pakistan**

Type of Approach	Recommended Measures
Political	<ul style="list-style-type: none"> <li>• Start National Awareness Campaign</li> <li>• Establish a Dedicated Body for Cybersecurity Culture</li> <li>• Allocate Dedicated Financial Capital</li> <li>• Design National Cybersecurity Curriculum</li> <li>• National Capacity Development Programme</li> </ul>
Legal	<ul style="list-style-type: none"> <li>• Draft Cybersecurity Policy, Strategy and Doctrine</li> <li>• Develop Cybersecurity Standards</li> <li>• Adopt Industry Competency Models</li> <li>• Establish Compliance Accreditations</li> </ul>
Management	<ul style="list-style-type: none"> <li>• Establish Cybercrime Units in Local Police Stations</li> <li>• Establish Specialised Cybercrime Courts</li> <li>• Establish Cybersecurity Inspection Programme</li> </ul>
Monitoring	<ul style="list-style-type: none"> <li>• Define Benchmarks</li> <li>• Define Success Indicators for Initiatives</li> <li>• Develop Acceptable Practices</li> <li>• Publish Periodic Process Reports</li> </ul>
Economic	<ul style="list-style-type: none"> <li>• Develop Stakeholder Engagement Plan</li> <li>• Promote Public-Private Partnerships</li> <li>• Design Cybersecurity Research Agenda – Increase Knowledge base</li> <li>• Increase International Partnerships</li> </ul>



While emphasising the importance of international legal infrastructure, Ambassador Aizaz Ahmad Chaudhry, Director General ISSI, in his concluding remarks said that there is a great deal of effort being made by Pakistan to develop legislation at the national level to prevent the misuse of cyberspace or regulate it for creating incentives for good uses. However, at the international level, there is a reluctance on the part of those who already have an advantage in the cyber domain to create an international legislative structure. In the absence of an international legal structure, every state is operating from a self-help approach. There is a need to make a

move for an international legal regime for cyberspace.



## “Artificial Intelligence and National Security”

*Aamna Rafiq,  
Research Associate, ACDC, ISSI*

## “Artificial Intelligence and National Security”

*Aamna Rafiq,  
Research Associate, ACDC, ISSI*

What constitutes Artificial Intelligence (AI) is a fundamental question, which is being debated for decades now. There is no universally accepted definition. However, simply AI refers to the “capability of a computer system to perform tasks that normally require human intelligence.”<sup>1</sup>

The field of AI is making progress by leaps and bounds. It has started to penetrate every facet of human life, ranging from cell phones, language translation, navigation systems and social media to autonomous aerial vehicles. AI like any other technology is a dual-use technology. It has a lot of potential to be used for beneficial purposes but it could be misused for various malicious purposes. This will not only generate new opportunities and facilities but also generate new types of threats and challenges for traditional/military security and non-traditional/human security or comprehensive national security.



### Impact of AI on Military Security

AI is one of those emerging technologies whose theoretical integration in military strategies and doctrines as well as its impact on the actual battleground in the latest conflicts is gradually gaining a certain level of prominence. Yet, the vast majority of its impacts in the military domain remain ambiguous due to the near future operationalisation of various applications. This has resulted in the conception of numerous assumptions, judgements and predictions. Regarding the impact of AI on military security, there exists a divide among experts. Some experts consider AI as the next big revolution in military affairs that would change the fundamental ways in which wars are being fought. Currently, states are competing with each other to dominate the technologies related to AI. On the other hand, some experts consider AI just a force multiplier just like many other military technologies in the past.<sup>2</sup>

The most widely discussed application of AI in the military domain is decision-making during a crisis or conflict. It is believed that AI systems accelerate the overall decision-making process, as they are capable of collecting, processing and analysing big data at an unprecedented high speed as compared to humans. This swift decision-making provides a strategic edge and narrows the time window for the opponent to respond accurately or explore creative alternatives. However, it should be taken into account that decision-making in crisis or conflict involves many other factors like troops and logistic movements, weather situation, geography, terrain, etc. Furthermore, the AI integration with space-based assets would enhance the object detection, image processing and recognition improving operation-specific imagery, precision targeting and Intelligence, Surveillance and Reconnaissance (ISR) capability of

<sup>1</sup> Definition from Defence Science Board, Summer Study on Autonomy, Washington, DC, June 2016.

<sup>2</sup> Forrest E Morgan et al., “Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World,” RAND Corporation, 2020, accessed date, April 26, 2022, [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RR3100/RR3139-1/RAND\\_RR3139-1.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR3100/RR3139-1/RAND_RR3139-1.pdf)

military forces. Although it decreases the probability and scale of collateral damage, the important factors like traceability and credibility of data used in AI decision-making and targeting should be taken into account as well.<sup>3</sup>

The introduction of automation in the military domain would resolve the issue of limited availability of human resources and finances. Militaries across the globe struggle with the issue of maintaining the specific numerical strength and budget. In addition to data analytics, the military robots on the battlefield could assist soldiers on the ground, reducing the need for extra or even required human resources for a specific operation. However, it could also result in exposing these military robots to the dangers of electronic warfare and physical attacks. Moreover, it would also endanger these systems to cyberattacks like jamming, hacking and unauthorised modification of algorithms, etc. AI is dependent on cyber technologies at a very fundamental level because the entire AI system relies on algorithms and big data. Therefore, protecting both and many other components from cyber interference is a prerequisite for any AI application. The militarisation of AI will give rise to various other threats and challenges like loss of escalation control, inability to differentiate between combatants and non-combatants, corruption of data, automation bias, the trigger of an arms race and lack of attribution resulting in third party interferences.<sup>4</sup> The dynamics could take a risky turn with the shift from the AI integration with the existing conventional weapons to AI integration with nuclear weapons. With the consolidation of military AI, oceans will become transparent. The introduction of maritime autonomous vehicles and submarines will affect the strategic stability among nuclear states, as it will reduce the significance of sea-based deterrence.<sup>5</sup>

## **Impact of AI on Human Security**

### *Economic Security*

The global economy has entered a new era of economic expansion based on the emerging technologies of the fourth industrial revolution like the IoT, AI, etc. However, there are notable ambiguities about the true implications of AI integration into national and international economies. AI is an uncertain territory that requires in-depth research to examine the potential negative implications and risks to national and global markets. The technological optimists believe that AI would enhance productivity resulting in a large-scale increase in global and national GDP revenues.<sup>6</sup> With an annual growth rate of approximately 121 per cent, AI will become a US\$90 billion industry in 2025 from the US\$7.3 billion industry in 2018. AI will add 20 per cent to the growth of developed economies while just adding 10 per cent growth to developing economies.<sup>7</sup> The implications of AI on the labour market would not be unidirectional as they greatly depend on the degree of synergy and speed of the integration process. The more competitive firms with greater reliance on technologies and creative human

---

<sup>3</sup> “Lethal Autonomous Weapon Systems (LAWS) and State Behaviour: Global and Regional Implications,” Institute of Strategic Studies Islamabad (ISSI), Arms Control & Disarmament Centre (ACDC) Webinar Report, April 7, 2021, [https://issi.org.pk/wp-content/uploads/2021/04/Report\\_Webinar\\_Apr\\_7\\_2021.pdf](https://issi.org.pk/wp-content/uploads/2021/04/Report_Webinar_Apr_7_2021.pdf).

<sup>4</sup> Morgan, et al., “Military Applications of Artificial Intelligence.”

<sup>5</sup> Aamna Rafiq, “Militarisation of Artificial Intelligence and Future of Arms Control in South Asia,” *Strategic Studies* 41, no. 2 (Summer, 2021): 49-63.

<sup>6</sup> E K Karpunina, et al., “Artificial Intelligence and its Impact on Economic Security: Trends, Estimates and Forecasts,” in: E Popkova, eds., “Scientific and Technical Revolution: Yesterday, Today and Tomorrow,” ISC 2019, Lecture Notes in Networks and Systems, vol 129. Springer, 2020, Cham. [https://doi.org/10.1007/978-3-030-47945-9\\_23](https://doi.org/10.1007/978-3-030-47945-9_23).

<sup>7</sup> “IDC Future Scope: Worldwide IT Industry 2019 Predictions,” accessed on April 24, 2022, <https://www.idc.com/getdoc.jsp?containerId=US44403818>.

resources will thrive while the traditional industries with manual labour and less reliance on technologies either will exit the market or ultimately take in by the bigger tech giants.<sup>8</sup> According to the World Economic Forum (WEF) report, AI and emerging technologies will introduce 133 million new job opportunities while reducing the 75 million existing jobs by 2025. Robots are expected to perform more than 50 per cent of existing jobs mostly in the area of repetitive manual jobs.<sup>9</sup> This indicates a major shift of economic opportunities from labour-intensive blue-collar jobs to creative and tech-savvy white-collar jobs.

### Food Security

According to World Food Programme (WFP), 11 million people went hungry in the year 2020-21 due to conflicts, economic slow-down, rapid depletion of natural resources, extreme Climate Change and increasing water scarcity. The COVID-19 pandemic increased the frequency and intensity of these challenges, resulting in further exacerbation of the ongoing global food crisis. With the world population reaching 9.8 billion by 2050,<sup>10</sup> the grave danger of a global hunger pandemic is on the horizon. Traditional farming techniques are also among the major challenges to sustainable and inclusive food security in today's world. All these challenges could be managed by introducing dual-use emerging technologies especially AI. AI-enabled smart sensors, autonomous unmanned ground vehicles and drone swarming would play a decisive role in enhancing the seed quality, yield and harvest optimisation, soil monitoring, disease mitigation and pest control. It would set in motion modern, smart, synergistic, precision and sustainable farming. As automated farming heavily relies on a huge amount of data about various types of soils, seeds, fertilizers, weather patterns, equipment and tools, the fundamental focus should be on developing effective data management infrastructures and mechanisms.<sup>11</sup>

### Environmental Security

As the depletion of the natural ecosystems and environmental disasters are intensifying, the global communities and governments are looking for new sustainable and eco-friendly ways to ensure environmental security. AI could enhance environmental security by facilitating an efficient and eco-friendly waste management system. Along with machine learning and quantum computing, AI can not only design low carbon next-generation power plants but also detect malfunction, anomalies and cracks in the existing nuclear, hydro and solar power plants at early stages. In the case of nuclear power plants, AI can widen the available options for nuclear waste disposal. Based on existing big data of weather patterns, the AI-enabled disaster response system can detect weather anomalies well before time and transmit natural disaster warnings. Using AI for creating pre and post-disaster maps could help in understanding the ecological and socio-economic damage caused by natural disasters. A similar mapping system can monitor the other effects of Climate Change like the speed and intensity of deforestation and glacier meltdowns. Moreover, AI contributes to better urban management. The new AI algorithms could facilitate the mechanisms of planning sustainable, greener and smart cities. It improves the architectural design for constructing environment-friendly and energy-efficient

---

<sup>8</sup> Karpunina et al. "Artificial Intelligence and its Impact on Economic Security," 218-220.

<sup>9</sup> "The Future of Jobs Report 2018," World Economic Forum, accessed on April 24, 2022, <https://www.weforum.org/reports/the-future-of-jobs-report-2018>.

<sup>10</sup> "Hunger Pandemic: Food Security Report Confirms WFP's Worst Fears," World Food Programme (WFP), last modified on July 12, 2021, <https://www.wfp.org/stories/hunger-pandemic-food-security-report-confirms-wfps-worst-fears>.

<sup>11</sup> Pradeep Tomar ed. *Artificial Intelligence and IoT-Based Technologies for Sustainable Farming and Smart Agriculture* (Pennsylvania: IGI Global, 2021).

buildings with automatic power controls. The smart city projects include automated traffic management systems, automatic transportation, improved vehicle efficiency, early detection of law and order situations and ground and aerial monitoring of cities through drones.<sup>12</sup>

### Health Security

The most common medical application is the integration of AI technology with radiology. The AI-enabled radiological system can detect extremely minute tumours and cancerous cells that cannot be detected by a human eye in traditional methods. Another common and widely used application of AI is “precision medicine.” Keeping in view the patient’s medical history, existing medical context and severity of symptoms, this application suggests suitable treatments. In the healthcare sector, the utmost complex and advanced function of AI and machine learning is neural network technology. In the light of provided patient’s medical data, this technology can predict what diseases the patient in question can get in future. This futurist application enables the patients and health care providers to take precautionary measures to minimise the likelihood of getting a particular disease. After diagnosis and precision medication, the next critical AI application is the medical robots. The AI-enabled surgical robots provide valuable assistance to surgeons. They enhance the human capacity to see and analyse the medical situation to perform minute surgical procedures with precision and detail. However, the health sector is aware of the critical dynamics of human-machine interaction. Therefore, human surgeons take all critical decisions while receiving relevant support from these robots.

Furthermore, AI algorithms are being used for various other administrative purposes e.g. maintenance and up-gradation of patients’ medical records, appointment assistance, billing as well as for monitoring the patient’s level of engagement and compliance. Despite all these beneficial applications, there are certain areas where AI cannot contribute to healthcare. AI can diagnose diseases based on physical data but cannot take into account the emotional and mental aspects of the disease. Furthermore, in case of any misdiagnose by the system, the absence of accountability and transparency will emerge as a major challenge. As big data is the basic component of all these systems and applications, its protection is the most critical responsibility on the part of healthcare providers. The hacking of systems and healthcare data could not only create horrific health care emergencies in the present time but also accelerate the creation of various dangerous bioweapons in future.<sup>13</sup> In recent medical research, the AI algorithm created 40,000 hypothetical biochemical weapons within just 6 hours of a trial run.<sup>14</sup>

### **Conclusion**


AI has generated a wave of socio-economic rejuvenation and an unprecedented shift in military security and warfare. Therefore, states and individuals should endeavour to develop an in-depth

---

<sup>12</sup> “Here’s how AI can Help Fight Climate Change,” World Economic Forum, last updated August 11, 2021, <https://www.weforum.org/agenda/2021/08/how-ai-can-fight-climate-change/>, Jackie Snow, “How Artificial Intelligence can Tackle Climate change,” National Geographic, last updated July 18, 2018, <https://www.nationalgeographic.com/environment/article/artificial-intelligence-climate-change> and David Rolnick et al, “Tackling Climate Change with Machine Learning,” accessed on April 23, 2022, <https://arxiv.org/pdf/1906.05433.pdf>.

<sup>13</sup> Thomas Davenport and Ravi Kalakota, “The Potential for Artificial Intelligence in Healthcare,” *Future Healthcare Journal* 6, no. 2 (2019): 94-8.

<sup>14</sup> News Centre, “Artificial Intelligence could be Repurposed to Create New Biochemical Weapons,” Kings College London, last modified on March 24, 2022, <https://www.kcl.ac.uk/news/artificial-intelligence-could-be-repurposed-to-create-new-biochemical-weapons>.



understanding of AI to be better prepared for AI dominated future. The pace at which AI is developing and integrating with day-to-day life is much fast as compared to the establishment of a regulatory regime at national, regional and international levels to deal with the traditional and non-traditional security issues. There is a need to develop a comprehensive tech ecosystem that minimises the misuse of AI but enables national security within the bounds of global normative order and peaceful uses of AI socio-economic development.





**Webtalk**  
on  
**“Artificial  
Intelligence for  
Socio-Economic  
Development in  
Pakistan”**

*April 26, 2022*

## Web Talk

on

### “Artificial Intelligence for Socio-Economic Development in Pakistan”



The Arms Control & Disarmament Centre (ACDC) at the Institute of Strategic Studies Islamabad (ISSI) organised a web talk on “Artificial Intelligence for Socio-Economic Development in Pakistan” by Dr Yasar Ayaz, Chairman, National Centre of Artificial Intelligence (NCAI), NUST, on April 26, 2022. Dr Munam Ali Shah, Associate Professor Department of Computer Science, COMSATS, Islamabad, was the discussant at the web talk.



In his welcome remarks, Ambassador Aizaz Ahmad Chaudhry, Director-General ISSI, said that Artificial Intelligent (AI) has helped humans perform tasks faster from recognising speech and using stored memory and responding to requests, to an ATM that interacts with humans to buying an airline ticket on a computer or machine, to the use of robots to do things with much greater speed and efficiency. AI can work at a phenomenal speed and make our workplaces more efficient. It has brought a revolution to the modern world. Ultimately AI can be used for tremendous socio-economic development. However, he expressed concern over the potential to weaponise AI technology for military purposes. AI is a dual-use technology that humans can choose to use for the betterment of humanity or for destructive purposes.

Earlier in his introductory remarks, Malik Qasim Mustafa, Director ACDC, said that AI is widely accepted as the major driving force of the fourth Industrial Revolution and it has the potential to bring socio-economic development to a country. The COVID-19 pandemic has

shown us how digital technologies and AI-based models have addressed public health management challenges. He said that AI could play a substantive role in achieving 17 UN Sustainable Development Goals (SDGs) that are the building blocks of the 2030 agenda for sustainable development. Hence, it is high time for Pakistan to harness AI for its Socio-economic Development, as AI can play a major role in urban planning and monitoring, smart cities, precision agriculture and food production, water resource management and the health sector.



Dr Yasar Ayaz said, “AI is as important as electricity.” There is no system hardly any system that works without electricity. So in the future, there will not be any systems that work without AI. He said that AI has many uses today and some potential dangers as well. He highlighted the achievements and ongoing efforts of various research labs in the field of healthcare, medical image analysis, disaster management, Urdu speech recognition, crowd management, vehicle recognition system, firearm detection system and advanced driver and training assessment system.

Talking about his research work in AI, he said his team created a humanoid robot that could play soccer and became Pakistan’s first team that qualified to become part of the robotics World Cup. He also talked about his work on creating prosthetic legs and arms as well as a wheelchair using AI technology. Emphasising that about one-sixth of the world population is disabled in one way or the other, he said that AI and Robotics Technologies could bring all these people into the mainstream where they can start working like normal human beings. Thus, AI has the potential to bring betterment to these people and contribute to a country’s socio-economic development.

Dr Ayaz highlighted the uses of AI in Pakistan in the judiciary, for example, to dispense justice faster and for law enforcement to make cities safer for the safe cities project. AI systems have resulted in apprehending actual suspected persons in crowded places, like cricket matches. It is also helping in anti-terrorist operations. AI is, thus, already made an immense contribution to Pakistan. He also highlighted the work of NCAI, NUST, which is working across Islamabad, Karachi, Lahore and Peshawar and has nine labs that are working in diversified fields such as diagnostics, healthcare, disaster management and environment protection, trends of the climate prediction, global Climate Change, traffic management, reducing electricity consumption, as well as the COVID-19 management and counterterrorism.

Talking about international trends in AI, he said that worldwide spending on AI systems would reach US\$77.6 billion in the year 2022. China has declared that it is investing US\$150 billion into AI, the US \$300 billion, the UK US\$1 billion and India US\$477 million by the year 2030. In comparison, Pakistan has modest resources and is only investing about US\$10 million. While talking about the access of developing countries to these technologies, he said that in terms of AI infrastructure, the developed world is leading the race. However, the developing states are actively contributing their part to software development.

He concluded by saying that AI is the way to the future. It has contributed to socio-economic development worldwide and it is contributing tremendously within Pakistan. There is a need to develop the AI sector, harness its potential as well as further invest in it.



While expressing his views on the importance of data for AI, Dr Munam Ali Shah, Associate Professor Department of Computer Science, COMSATS, Islamabad, said that AI systems in every field rely heavily on big data and data analytics. There is a need to develop a data management system at the national level for efficient and intelligent use of data. About two decades ago there were hardly any computers being used by ordinary people. Now everyone has a computer or a smart device. Now with the use of the internet, a large amount of data is being produced and it needs to be processed. With the COVID-19 patients, we have a lot of data. In addition, in

Pakistan with a population of over 200 million and almost 63 per cent of the population comprised of young people, there is potential for the development and processing of data. He said that there are a lot of opportunities here but there is also some decision making needed. During the COVID-19 pandemic, AI helped a lot and opened many doors. Many businesses have flourished including online shopping and video streaming.

Talking about future trends, Dr Shah said that there is a lot of potential for AI in education, employment and road safety. Also with a large young population on social media, the data can be used to assess trends and their education needs and the government can use that data to offer vocational training and other educational opportunities. In Pakistan, there is data and technology, what is lacking is the processing and use of data for the betterment of the country.

The presentations were followed by an interactive question and answer session. Questions included the tremendous potential for AI use in the future and how we can promote it in Pakistan. Especially how can we educate and train the youth; What are the prospects for international collaboration and whether the leaders in AI across the world are willing to share and collaborate in AI technologies; the possibility of misuse of AI; the major challenges in Pakistan's regulatory or policy framework about AI innovation and growth and Pakistan's gaps for promoting secure and reliable AI?

The speaker responded that there is disparity globally in access to AI technologies. Not all developing countries have equal access to facilities in which AI can be processed. However, they emphasised that the world is very closely knit today and each other progress benefits all countries. They suggest collaborative groupings like the EU where there can be collaboration. They said that we have to realise in our region that we have to promote peace and develop inclusive technologies, which enable people to work in a mainstream. In a closely-knit world, mutual collaboration and support are the way forward.

Speakers also said that there is a standardised curriculum for the AI Masters and PhD within the country that is applied throughout Pakistan. There are certification programmes to meet the need of the market, short-term training from five days to two weeks, then there is also training to convert conventional computer science professionals into proper AI professionals through four months diploma or certification programme. Pakistan needs to produce AI professionals at a fast rate. Hence quick certifications and conversions of computer professionals into AI

professionals. This is done in collaboration with the industry and many prominent companies are part of this initiative and working together.

As for the international regulatory regime to prevent the misuse of both cyber power and AI, speakers said that UNESCO is already developing a document, which is a standard-setting instrument for AI. This can serve as a guideline but it is not possible to make a central law for example, which can be implemented in all countries to follow.

Regarding the misuse of AI, the speakers said that there are the good and bad aspects of every technology. The important thing is to keep the flow of the technology in check and to make sure that they are in the right hands. AI if not in responsible hands can be misused.

In his concluding remarks, Ambassador Khalid Mahmood, Chairman BoG ISSI, stated that AI is a double edge sword. It could be used for military purposes or to accelerate the progress toward socio-economic development. He also highlighted the key concerns like human-machine interaction, protection of human rights and the global digital divide. AI like all technologies have its negative side if misused and its positive side. Overall, the impact of AI technologies is positive, as it is apparent in its use during the COVID-19. AI has been found beneficial in the field of energy, education, the financial and the health sectors. Greater use of AI technology will help progress toward reaching the 17 SDGs set by the UN. Talking about the downside of AI technology, he said that progress in AI is slow in developing countries and it is likely to accentuate the digital divide worldwide. Even within countries, there may be a disparity. He also expressed concern with the potential to weaponise AI technologies, which can be harmful to humanity. He emphasised the need to regulate AI technology.







**“Space Technologies for Socio-Economic  
Development in Pakistan”**

*Ghazala Yasmin Jalil,  
Research Fellow, ACDC, ISSI*

## “Space Technologies for Socio-Economic Development in Pakistan”

*Ghazala Yasmin Jalil,  
Research Fellow, ACDC, ISSI*

Space is increasingly becoming vital to countries' progress, prosperity and development. While space assets have been used both for civil and military purposes, the article focuses on the civil uses of space technologies. Today, space technologies have tremendous potential to contribute to the socio-economic development of a country. Satellites today are being used in a wide range of fields from navigation, agriculture, urban planning, disaster management, water resource management, health and industry. Space technologies can also contribute to the United Nation's Sustainable Development Goals (SDGs). Pakistan has a modest space programme and is increasingly using its space-based assets to achieve sustainable development goals and socio-economic development.



### **Pakistan's Space Programme**

Pakistan started its space programme in 1961 when it set up its Pakistan Space and Upper Atmosphere Research Commission (SUPARCO), which is responsible for the country's public and civil space programme and aeronautics and aerospace research. Pakistan has launched four satellites so far.

In 1961, SUPARCO launched its first-ever sounding rocket called Rehbar-1 for upper atmosphere research with the help of China. The technology for the rocket was developed with the help of the US, British and French space agencies. It continued working on sounding rockets in the ensuing years. During the 1970s, SUPARCO continued to expand research and development on remote sensing satellites, for imagery and telecommunication. It worked to develop its experimental satellites Badr-1 and Badr-B. Badr-1 was Pakistan's first digital communication satellite, which was launched into Low Earth Orbit (LEO) in July 1990 using a Chinese rocket. Badr-1 materialised due to the joint efforts of some Islamic countries under the Inter-Islamic Network on Space Sciences and Technology (ISNET), which was established in 1986.<sup>1</sup> Its headquarters were located within the SUPARCO headquarters in Karachi. Chairman SUPARCO was its head. The ISNET in collaboration with SUPARCO was responsible for the development, processing and launch of Badr-1. It was considered the Muslim world's first satellite and was a matter of great pride.

Badr-B or Badr-2 was launched in December 2001 with the help of Russia from Baikonur Cosmodrome, Kazakhstan. It was launched into a sun-synchronous circular orbit of 1018 km. It has an orbital period of 105 minutes and an inclination of 99.64 degrees.<sup>2</sup> The primary objectives of Badr-B were for the acquisition of earth imagery, for experimental uses and for encouraging the scientific community in the country.

<sup>1</sup> Ajay Lele, *Asian Space Race, Rhetoric or Reality* (India: Springer, 2013), 46.

<sup>2</sup> "Badr-B," SUPARCO, <http://www.suparco.gov.pk/pages/badrb.asp>.



China has helped Pakistan achieve many milestones in its space programme. China has shown a willingness to provide access to Chinese space technology and the use of its space infrastructure. Pakistan launched Paksat-1R, its first communication satellite, with Chinese collaboration on August 12, 2011. It has a capacity of 30 transponders. The satellite was launched in the Geo-stationary orbit (GSO). It replaced the existing satellite PAKSAT-1, which was leased by SUPARCO in 2002. With a design life of fifteen years, it provides broadcasting, internet and data communication services to regions outside Pakistan as well. These are primarily parts of South Asia and Central Asia, Eastern Europe and parts of East Africa.<sup>3</sup>

SUPARCO's greatest achievement so far is the launch of the two indigenously built satellites from a Chinese satellite centre. The foreign office confirmed that the Pakistan Remote Sensing Satellite (PRSS-1) and Pakistan Technology Evaluation Satellite (PakTES-1A) were launched using the Chinese SLV in 2018.<sup>4</sup> PRSS-1 weighs 1,200 kg while PakTES-1A weighs 285 kg. The satellites operate at 640 km and 610 km altitude, respectively.<sup>5</sup> In 2016, SUPACO and China signed an agreement for the development of the PRSS-1 system to monitor the China Pakistan Economic Corridor (CPEC).<sup>6</sup> This represents a new level of space cooperation between Pakistan and China.

### **Vision 2040**

The National Command Authority approved the Space Programme 2040 in July 2011. Under the Vision 2040, Pakistan plans to launch five GEO satellites and six LEO satellites by 2040. Pakistan also plans to send an astronaut into space in 2022 with the help of China.<sup>7</sup> It also has ambitious plans to build its launchers and be self-reliant in launching satellites. At present Pakistan mostly uses Chinese launching facilities. Pakistan has already launched Paksat-1R in August 2011.

### **Uses of Space Technologies in Pakistan**

Satellites are of immense importance for Pakistan's socio-economic development. The data and images gathered by the satellites would be vital for the efficient management of Pakistan's natural resources and water resources, which are already under tremendous stress due to improper management and Climate Change.<sup>8</sup> SUPARCO is the national body that deals with space technologies and applications it has done tremendous work in the fields of Earth Observation, remote sensing applications, earth and environment sciences as well as aerial remote sensing.

#### *Remote Sensing Applications*

PRSS-1 and PakTES-1A ground stations launched in 2018 contribute nationally and internationally. These satellites have applications in a vast number of fields like remote sensing

---

<sup>3</sup> <http://www.fab.gov.pk/article/the-paksat-1r-satellite.html>.

<sup>4</sup> "Pakistan Launches two Satellites from China," *The Nation*, July 10, 2018.

<sup>5</sup> Ibid.

<sup>6</sup> "Satellite to be Launched for Monitoring CPEC Projects," *Dawn*, April 21, 2016.

<sup>7</sup> Miqdad Mehdi and Jinyuan Su, "Pakistan Space Programme and International Cooperation," [https://www.unoosa.org/documents/pdf/psa/activities/2019/UNJordanWorkshop/Presentations/P.7\\_Poster\\_Jordan\\_Conference.pdf](https://www.unoosa.org/documents/pdf/psa/activities/2019/UNJordanWorkshop/Presentations/P.7_Poster_Jordan_Conference.pdf).

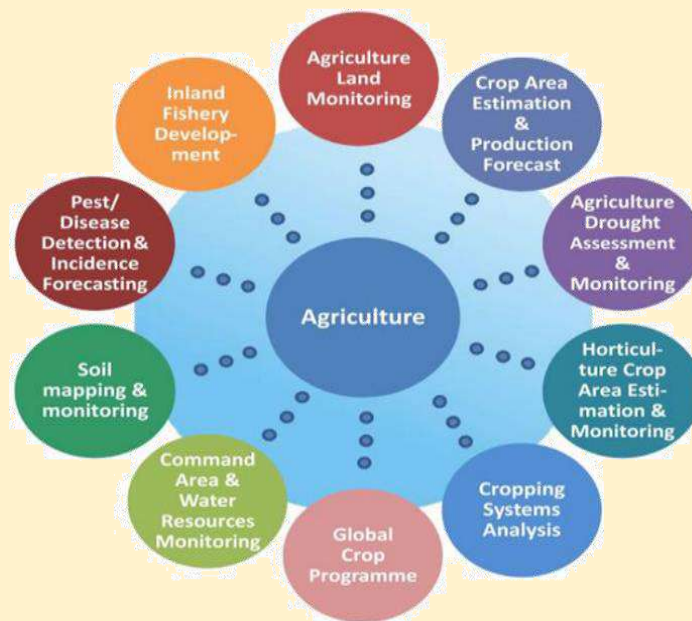
<sup>8</sup> Ahmad Khan, "From Badr-1 to PRSS-1: Pakistan's Journey into Space," *Pakistan Politico*, August 7, 2018, <http://pakistanpolitico.com/from-badr-1-to-prss-1-pakistans-journey-into-space/>.

data products, agriculture, forestry, disaster management, management of water resources, environment, urban planning and management, cryosphere modelling, managing coastal and marine resources, and geology & mineral prospection.

### Agriculture

Pakistan being a country that relies heavily on agriculture, space technologies are playing a vital role in the agriculture sector.<sup>9</sup> Remote sensing technologies are thus aiding in improving agriculture by classifying various crop types, providing crop area estimation, monitoring crop health and crop growth and assisting in crop production and yield estimations, drought monitoring, waterlogging, salinity and land degradation monitoring and precision agriculture. It helps in identifying and eliminating pests and diseases in farmland. Remote sensing technology also provides data about the soil moisture this helps in planning the irrigation needs of the soil. In addition, soil mapping is an important use of remote sensing technology by helping identify soils, which are not suitable for crops.<sup>10</sup>

Agriculture is an area where there is a lot of space technology applications are already in use by still there is room for further applications that will help in improving the socio-economic indicators in Pakistan.



**Source:** Mahvish Malik and Misbah Arif, “Managing Non-Traditional Threats by Using Space Technology: A Case of Pakistan,” *NUST Journal of International Peace & Stability II*, no. 2 (2019): 32-44.

### Disaster Management

These satellites would also help with natural disaster management such as floods and drought, forestation and deforestation. SUPARCO has a Space Applications Centre for Response in Emergency and Disasters (SACRED) established in 2013 to provide space-based technical support to National Disaster Management Authority (NDMA), Provincial Disaster

<sup>9</sup> “Space Technology Applications,” SUPARCO, <https://suparco.gov.pk/major-programmes/space-technology-applications/>.

<sup>10</sup> Mahvish Malik and Misbah Arif, “Managing Non-Traditional Threats by Using Space Technology: A Case of Pakistan,” *NUST Journal of International Peace & Stability II*, no. 2 (2019): 40.

Management Authorities (PDMAs) and other national bodies for natural disasters using satellite remote sensing technologies. It is also host to the UN Platform for Space-based Information for Disaster Management and Emergency Response (UN-SPIDER) Regional Support office in Pakistan since 2010 and provides natural disasters assistance to regional countries as well. Pakistan is also developing the National Catastrophic model and Disaster Management Information System in the first phase for disasters like floods, droughts, tsunami cyclones and storms, heatwaves and earthquakes.

In addition, SUPARCO is also collaborating internationally for disaster management. It is the Authorised User (AU) of the International Charter Space and Major Disasters on behalf of NDMA, a member of the JPTM-3 project of Sentinel Asia and has been registered as Data Analysis Node (DAN) since 2014 and it is a member of APSCO Disaster Management Framework.<sup>11</sup>

### Hydrology

Pakistan is essentially an arid country that relies on glacier melts and monsoon rains. RSS provide large-scale multidisciplinary information to monitor and manage water resources. RSS play a vital role in Pakistan by mapping and monitoring the health of watersheds and water bodies, check of dam sites, surface water resources estimation, snowmelt, rainfall and river runoff. Remote sensing also aids in assessing surface energy balance and evapotranspiration; hydrological modelling; mapping of Surface water resources and irrigation networks; ground-water prospection; wetland ecosystem modelling and soil moisture estimation.<sup>12</sup>

### Weather

SUPARCO has established a dedicated space weather facility known as Pakistan Space Weather Centre (PSWC). State of the art instruments installed countrywide helps to monitor space weather phenomenon in real-time. After processing, HF communication products are disseminated to national users

### Climate Change and Environmental Degradation

SUPARCO is working in the fields of Climate Change and environmental degradation with the use of integrated ground-based observation and satellite data. It is addressing Climate Change and environmental degradation issues through the integrated use of ground-based observations and satellite data, which helps in forecasting the environmental indicators across different spheres like Atmosphere, Biosphere, Cryosphere and Hydrosphere. Four centres help in doing that. They monitor and manage forest assets and operations, deforestation, detect change over time, monitoring of fog and Smog patterns and fire location identification.

### **International Cooperation**

At the international level, there has been tremendous success in space exploration and the use of outer space for peaceful purposes. There has also been a lot of international cooperation to better utilise space resources for peaceful purposes. Pakistan has also been actively cooperating

---

<sup>11</sup> “Disaster Management,” SUPARCO, <https://suparco.gov.pk/products-services/disaster-monitoring-and-mitigation/>

<sup>12</sup> “Water Resources,” SUPARCO, <https://suparco.gov.pk/products-services/water-resources/>

internationally. It had permanent membership in several international organisations, institutes, scientific committees and the United Nations bodies. SUPARCO also has bilateral and multilateral cooperation agreements/MoUs for collaboration in space-related activities. Pakistan is also party to five primary international treaties on outer space:

- The 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space. Pakistan joined in April 1968.
- The 1968 Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space. Pakistan joined in 1973.
- The 1972 Convention on International Liability for Damage Caused by Space Objects.
- 1976 Convention on Registration of Objects Launched into Outer Space. Pakistan became acceded in February 1986.
- 1979 Agreement Governing the Activities of States on the Moon and Other Celestial Bodies. Pakistan joined the Moon Treaty in February 1986.<sup>13</sup>



Source: “International Cooperation,” SUPARCO, <https://suparco.gov.pk/international-cooperation/>.

## The Way Forward

Pakistan has always maintained that space needs to be preserved for peaceful uses only. It has always opposed the militarisation and weaponisation of outer space. Pakistan has been a strong advocate of the Prevention of Arms Race in Outer Space (PAROS) and supports the International Code of Conduct for Outer Space. Pakistan has always maintained that space is a global commons and needs to be preserved for human benefit.

Internationally, Pakistan needs to further develop collaboration with many states on the peaceful use of space technology. Non-traditional security threats today are faced by a multitude of countries and thus there is a need to collaborate to meet the challenges.

<sup>13</sup> “United Nations Treaty Collection”, <https://treaties.un.org/pages/Treaties.aspx?id=24&subid=A&clang=en>

Pakistan has come a long way in the application of peaceful use of space technology. However, it has a very small space programme that needs to be developed. It is vital for Pakistan's policymakers to understand the need for a robust space programme. Pakistan needs to work towards the indigenisation of its national space programme. For this government support is vital. The private sector can also play a role in investing in and utilising space technologies. There is also a need to create awareness and sensitise the public on the importance of a space programme. Thus, Pakistan needs to still go a long way to keep pace with the latest technologies in the world and use innovative solutions like space technologies in overcoming challenges.

## **Conclusion**

Non-traditional threats are increasingly pressing. It is, thus, time to tackle them using the latest technologies like AI and space technologies. While Pakistan has robust traditional security apparatus, it is time to pay equal, perhaps more attention to non-traditional security threats like Climate Change, environmental degradation, hunger, poverty, health water scarcity and natural disasters. Only by overcoming these challenges will Pakistan achieve much needed socio-economic development. A robust space programme is essential to achieve economic progress today. Pakistan's space policy is focused on the peaceful use of outer space to achieve socio-economic development. Overall the South Asian region faces many non-traditional security threats like increasing population rate, illegal immigrants, poverty, social disparity, terrorism, arms trafficking and environmental disasters. The challenges are of great magnitude that all countries of the region need to come together and devise cooperative security mechanisms to tackle them.





Webinar  
on  
“Big Data for  
National Security:  
A Case of Pakistan”

*May 11, 2022*

## Webinar

on

### “Big Data for National Security: A Case of Pakistan”



The Arms Control & Disarmament Centre (ACDC) at the Institute of Strategic Studies Islamabad (ISSI) organised a Webinar on “Big Data for National Security: A Case of Pakistan” on May 11, 2022. Speakers included Dr Muhammad Ali Ismail, Principle Investigator, National Centre of Big Data & Cloud Computing (NCBC), Karachi, Dr Hussain Nadim, Executive Director (C &R), Islamabad Policy Research Institute (IPRI) and Ms Aamna Rafiq, Research Associate ACDC-ISSI.



In his welcome remarks, Ambassador Aizaz Ahmad Chaudhry, Director-General ISSI said that big data refers to a collection of data that is enormous and comes at you with great speed and continues to grow. Big data needs to be managed and analysed for it to be useful. This data explosion is touching every aspect of life human security, finance, stock exchange, banking, social media and the agricultural sector. The government, private sector as well as individuals are keen to use big data to their benefit. Big data is also playing a big part in the technological race between the US and China. The statistics are mindboggling where China is manufacturing 250 million computers annually, 25 million automobiles and 1.5 billion smartphones. China continues to focus on producing world consumer goods. Thus, there is a huge technological race going on that will be powered and fuelled by big data. Pakistan needs to be aware of how it can help or undermine our national security.



Earlier in his introductory remarks, Malik Qasim Mustafa, Director of ACDC, said that big data means a larger volume of a complex data set, which is received at a fast velocity rate and contains greater variety. According to experts, it can influence every aspect of individual human life and society and the global landscape. It enables everything from access to knowledge and global communication to the delivery of services and infrastructure. Big data analytics is positively transforming the ways of doing business, trade, governance, politics, communications and social services. However, its misuse can equally exacerbate existing national security threats and can create new and unpredictable ones.



Pakistan recognises the potential and reaches of big data for socio-economic development and national security challenges. Big data is an unexplored and uncharted territory in Pakistan. There is a need to identify the potential spectrum for designing the normative and legal framework at the national level for big data.

Dr Muhammad Ali Ismail spoke on “Big Data for Human Security in Pakistan.” He said that “Big data” is a big challenge and it becomes an emerging hot topic. The term was coined around 2014. At the time, the Pakistani government and HEC also took up the initiative to stay on top of it and create centres like NCBC. In 2018, the Centre started working and the idea was to tackle national-level problems. “Big data” is a huge data coming with a huge philosophy and has different types of varieties. It started with three Vs – velocity, variety and volume. Managing big data is a complete echo system, which means that people and systems are continually executing data. In an echo system, one has to store the data, evaluate it, execute it and analyse it. Thus, big data also needs the change of complete infrastructure. The use of cloud computing emerged for storing data. Data mining is the new gold. Then it needs to be analysed for which special computers and software are needed.



He said that National Centre in big data and cloud computing’s objective was to provide a platform for the development and deployment of cutting edge solutions related to big data using open source tools. The Centre is working on astrophysics, genomics, tsunami modelling and traffic modelling. Genomics will help understand the biology behind genetic abnormalities to train human resources for the processing of next-generation sequencing data. The astrophysics lab is working on the classification of celestial objects, and simulation of the observable universe using data from SUPARCO and international sources. Tsunami modelling is working on a digital elevation model for major cities along with coastal areas. Traffic modelling is working on traffic flow modelling and simulation. All these projects are working and contributing toward human and national security.

Dr Hussain Nadim presented his views on “Big Data Analytics and Information Warfare in Pakistan.” He talked about how data can be used to decipher patterns of suicide bombing and identify what people are at risk of radicalisation. He said that compared to 30 years ago now we have the data but not the ability to process it. There are over 40 million social media users alone in Pakistan and are projected to have 80 million social media users in the coming years.

These people are creating narratives as opposed to the state. The state does not have the ability to be in the fifth generation of warfare.

The information warfare domain has become more complicated. There may be billions of users tweeting in India or elsewhere about Pakistan. He said that information warfare is defined as actions taken to achieve information superiority by affecting adversary information, and information-based processes. He elaborated that the term information warfare is widely used in the contemporary discourse but it is often misunderstood. The goal of information warfare is to destroy the enemy's warfighting capability without firing a single bullet. He highlighted that information warfare does not use tanks, fighter planes, missiles, or nukes to wage war. The weapons in information warfare are computer viruses, malware and Trojan horses. It does not result in mass casualties but the damage it can do to one's critical infrastructure, such as nuclear power plants in case of a country or critical data in case of others is a matter of concern. Information warfare is not new but what has changed is the speed of data. The huge data available can be used to map the behaviour of a nation, leaders and individuals. It can also be misused. One can easily build a narrative to manipulate the people and disseminate fake information among the targeted audience based on behaviour and trends. State institutions are fighting fifth generation warfare with 3rd generation tools. Pakistan needs to invest in managing and regulating big data.



While expressing her views on “Building National Framework for Big Data: The Way Forward for Pakistan,” Ms Aamna Rafiq, Research Associate ACDC-ISSI, said that Pakistan is facing a major challenge of insufficient and fragmented legislative, policy and technical frameworks on the big data. The national data ecosystem is suffering due to the absence of effective institutional and technical coordination on data partnerships between the government and other relevant stakeholders. Other challenges include data fragmentation, data silos, limited financial and human resource, insufficient ICT infrastructure and indigenisation. “Pakistan should work

on fast data, privacy laws, data partnerships, data diplomacy, and new data service models,” she said.

The remarks by speakers were followed by a robust discussion and question-answer session. Questions included since the failure of “Big Data” in National Security lies in the human ability to embrace the par and mitigate the limits of algorithms. How can we policymakers at the missions develop this ability in the era of post-truth and what normative and legal framework is available in Pakistan at the national level to regulate “Big Data”?

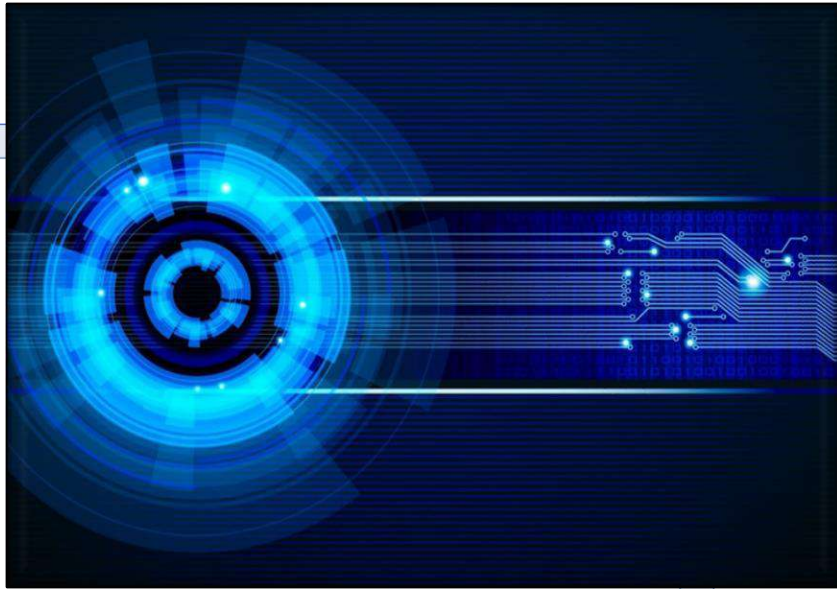
Speaker responded by saying algorithm development is all about the vision that you are having in your mind and what you want to execute. If we have the right policies and pre-defined objectives with us, these developments accordingly will lead to success. Algorithm designing and failure are all about a thing that you are processing. More importantly, you have clear objectives in your mind and the right policies.

Speakers also responded that at the national level, the normative framework is provided within the policy on a particular issue or area. As we do not have the “Big Data” policy right now. Thus, it is difficult to say what exactly norms the Government of Pakistan is trying to achieve in this area. Overall, Transparency, accountability and inclusiveness: these values exist in Pakistan. However, regarding the legal framework, we do not have any specific legal document or the act that deals with the “Big Data” issue and the Data Protection Privacy (DPP). The one proposal or the bill which is currently in the pipeline that is quite controversial and various drops are being discussed, is the personal data protection bill.

In his concluding remarks, Ambassador Khalid Mahmood, Chairman of BoG ISSI, stated that the world has been seeing the march of technology. Big data is also part of that technology march. All activities generate data. So far data has been kept in physical form but now it is stored and used in virtual space. This data is helping tackle challenges in many fields like national security, health, communication, education, industry, and disaster management. While there are advantages to utilising big data, there is potential for misuse like cyber-attacks on sensitive installations. There is also potential for misuse by the state as well as non-state actors. He said that there is a need to manage and eliminate and regulate the malicious use of data in Pakistan and at the international level. Efforts are afoot at the national, international and regional levels but much more needs to be done. Pakistan is the first country in the SAARC region, which adopted the e-government policy. Pakistan is also trying to make use of it under the CPEC to create a digital corridor. He emphasised the need for a public-private partnership to maximize the benefits of big data.







# Key Takeaways

## Key Takeaways

Following key takeaways have been drawn from this special report. These takeaways can serve as recommendations and a road map for achieving comprehensive national security through emerging technologies.

### *Role of Emerging Technologies in Achieving Comprehensive National Security*

- Emerging technologies are set to reshape the future of societies and economies and can play an important role in achieving the goals of comprehensive national security - social, economic, human and traditional security.
- States are utilising emerging technologies for battlefield dominance, altering the “balance of power” and fuelling up new regional and global arms races.
- For Pakistan, it is important to look at how India’s pursuit of emerging technologies is impacting strategic stability in South Asia.
- There is a need to raise awareness, promote cyber security culture, bridge the technological divide, develop cyberspace norms and address other related challenges at the national level.
- States must ensure the protection of cyberspace from cyber threats and cyberwarfare to safeguard their social, economic and national security interests. States should introduce strong data protection laws and regulations to ensure secure access to cyber technologies.
- It is high time for Pakistan to harness AI for its socio-economic development, as AI can play a major role in urban planning and monitoring, smart cities, precision agriculture and food production, water resource management and the health sectors.
- It is the collective responsibility of technologically advanced states to share and transfer technological expertise to the developing states for the greater good. In this regard, there is a need to develop an emerging technology sharing mechanism at the regional and international levels.

### *Cyber Technologies, Artificial Intelligence and International Security*

- A hybrid approach to deal with cyber threats is needed which would be a combination of education and effective security controls.
- The international community’s efforts at regulating cyberspace should be strengthened and there is a need for more international efforts to understand the consequences for the victim of cyber threats.
- There is a need to develop a legally binding international instrument, specifically tailored to the unique attributes of ICTs, to provide a regulatory framework that creates stability and security in cyberspace.
- There is a need to bridge the digital divide between developed and developing countries.
- There is a need for the formulation of a Vulnerability Disclosure Policy whereby all the relevant stakeholders could be involved in the creation of a safer digital space in Pakistan.
- There is a need for growing regulatory compliance and growing government efforts to ensure the security of supply chains, both on the industry side and the consumer side, and build into cyber defences.

- There is a need to look at autonomous systems beyond algorithms and also focus more on the availability of digitalised big data and improving computing power.
- There is a need to demilitarise emerging technologies.
- For AI to be used effectively and appropriately, there is a need to create a balance between extensive support and regulation for the use of AI.
- Hybrid military operations require a lot of teamwork and interactions involving a lot of human aspects, a key element missing in machine operating systems. Therefore, it is necessary to always keep humans in the loop.

### *Securing Pakistan's Cyber Domain: Challenges and Opportunities*

- The emerging critical threats in the cyber domain are going to affect the economy of a state.
- Cyberwarfare combined with electronic warfare becomes even more dangerous for nation-states.
- The role of local adoption of standards and best practices is very important for cybersecurity.
- There is a need to raise awareness about cybersecurity to ensure good cyber hygiene.
- Every organisation must formulate its cybersecurity policy, perform a risk assessment of the organisation to figure out its vulnerabilities, install firewalls and anti-virus on their personal as well as official devices and use multi-factor authentication.
- Encourage the development of indigenous tools to facilitate cybersecurity audits and compliance mechanisms, introduce indigenous software and train human resources to ensure the physical protection of cyberinfrastructure.
- Establish national and sectorial CERTS for rapid crisis management in case of a cyberattack.
- Pakistan should focus on building the credible voices of cybersecurity for a resolute acceptance of cybersecurity policy, laws and culture.

### *Artificial Intelligence and National Security*

- AI is dependent on cyber technologies at a very fundamental level because the entire AI system relies on algorithms and big data. Therefore, protecting both and many other components from cyber interference is a prerequisite for any AI application.
- The hacking of systems and healthcare data could not only create horrific health care emergencies in the present time but also accelerate the creation of various dangerous bioweapons in future. Protection of big data is the most critical responsibility on the part of healthcare providers.
- There is a need to develop a comprehensive tech ecosystem that minimises the misuse of AI but enables national security within the bounds of global normative order and peaceful uses of AI socio-economic development.

### *Artificial Intelligence for Socio-Economic Development in Pakistan*

- AI is a dual-use technology that humans can choose to use for the betterment of humanity or for destructive purposes.
- AI is widely accepted as the major driving force of the fourth Industrial Revolution and it has the potential to bring socio-economic development to a country like Pakistan.

- AI is contributing tremendously to Pakistan in the field of healthcare, medical image analysis, disaster management, Urdu speech recognition, crowd management, vehicle recognition system, firearm detection system, the judicial system and advanced driver and training assessment system.
- AI is as important as electricity. In the future, there will not be any system that works without AI. It is the way to the future since it has contributed to socio-economic development worldwide and it is contributing tremendously within Pakistan.
- There is a need to develop the AI sector in Pakistan, harness its potential as well as further invest in it.

### *Space Technologies for Socio-Economic Development in Pakistan*

- Space technologies have tremendous potential to contribute to the socio-economic development of a country. Pakistan's space policy is focused on the peaceful use of outer space to achieve socio-economic development.
- Pakistan is successfully using space technologies in the field of agriculture, disaster management and managing environmental degradation, Climate Change, water resources and urban planning.
- Internationally Pakistan needs to further develop collaboration with many states on the peaceful use of space technology.
- Non-traditional security threats today are faced by a multitude of countries and thus there is a need to collaborate to meet the challenges through space technologies.
- Pakistan needs to work towards the indigenisation of its national space programme and government support is vital for this.
- The private sector can also play a role in investing in and utilising space technologies.
- There is also a need to create awareness and sensitise the public on the importance of a space programme.

### *Big Data for National Security: A Case of Pakistan*

- Data explosion in the contemporary world is touching every aspect of life human security, finance, stock exchange, banking, trade, governance, politics, social media communications and social services and the agricultural sector.
- Its misuse can equally exacerbate existing national security threats and can create new and unpredictable ones.
- The goal of information warfare is to destroy the enemy's warfighting capability without firing a single bullet.
- The huge data available can be used to map the behaviour of a nation, leaders and individuals.
- Big data can also be misused. It is easy to build a narrative to manipulate the people and disseminate fake information among the targeted audience based on behaviour and trends.
- State institutions today are fighting fifth generation warfare with third-generation tools.
- Pakistan needs to invest in managing and regulating big data.
- Pakistan is facing a major challenge of insufficient and fragmented legislative, policy and technical frameworks on the big data.
- Pakistan faces challenges that include data fragmentation, data silos, limited financial and human resource, insufficient ICT infrastructure and indigenisation.







**ACDC**  
ARMS CONTROL & DISARMAMENT CENTRE

**Arms Control and Disarmament Centre (ACDC)  
Institute of Strategic Studies Islamabad (ISSI)**

Sector F-5/2, Islamabad, Pakistan.

Tel: 0092-51-9204423-24, 9205882, 9205886

Fax: 0092-51-9204658

Email: [acdc@issi.org.pk](mailto:acdc@issi.org.pk)

Website: [www.issi.org.pk](http://www.issi.org.pk)

*(Acknowledgement: Background images used in this report are downloaded from <https://suparco.gov.pk/> and <https://wallpapercave.com/>)*