ISSRA
INSTITUTE FOR STRATEGIC STUDIES, RESEARCH & ANALYSIS

REPORT - SEMINAR/ROUNDTABLES

EMERGING TECHNOLOGIES

IMPACT ON NATIONAL SECURITY

13th September 2023 – 1st October 2024

Institute for Strategic Studies, Research & Analysis (ISSRA)
National Defence University. Islamabad

EMERGING TECHNOLOGIES

IMPACT ON NATIONAL SECURITY

STRATEGY PAPER EMERGING TECHNOLOGIES: IMPACT ON NATIONAL SECURITY

Introduction

- In today's fast-paced technological age, emerging technologies like Artificial Intelligence, Robotics, Cyber Security, Quantum Computing, Cryptocurrency, the Internet of Things, and New Materials are driving economies forward. These technologies interact and converge, potentially transforming global development. The international economy, foreign policy, defense, diplomacy, conflict, and cooperation are now dependent on states' technological prowess.

- Major competitors like the US, China, and Russia use these technologies to boost economies and address complex challenges. However, the benefits of these technologies require investment and proactive policymaking. Pakistan has a promising future in this sector due to its strategic position, diverse diplomatic history, large youth population, natural affinity for STEM careers, and intrinsic socio-economic potential.

Methodology Adopted

- The paper is a crystallization of key takeaways compiled after a series of events held at ISSRA - NDU to deliberate upon and analyze the trends and trajectory of emerging technologies at the global as well as regional levels and understand how these may influence Pakistan's national security. Three emerging technologies were focused on a priority basis including:-

    - **Part I** - Artificial Intelligence (AI)
    - **Part II**- Cyber Security &
    - **Part III** -Synthetic Biology

The detailed plan that was executed is given as under:-

PLAN OF ACTIVITIES

Topic/Theme	Event	Date Conducted
Emerging Technologies: Impact on National Security	Mini Roundtable Discussion (Planning Phase)	26 Jul 23
Emerging Technologies: Impact on National Security	International Seminar (Initial)	13 Sep 23
Future of AI in Pakistan: Challenges and Opportunities	Roundtable Conference 1	11 Oct 23
	Roundtable Conference 2	23 Nov 23
Cyber Security in Pakistan: Challenges and Opportunities	Roundtable Conference 3	30 Nov 23
	Roundtable Conference 4	21 Dec 23
The Age of Synthetic Biology: Securing A Safer And Prosperous Bio Future For Pakistan	Roundtable Conference 5	27 Dec 23
Emerging Technologies: Impact on National Security	International Seminar (Final closing seminar)	30 Jan 24

- Multiple roundtable discussions were organized with participants including policymakers, representatives from academia, industry, technology related business organizations, research organizations, and students. Each discussion was digitally audio recorded, transcribed verb-atim, and, together with accompanying field notes, analyzed thematically to formulate the subsequent chapters of the paper. The research questions comprise the objectives of this study given below:

Objectives

- Comprehend where Pakistan stands (current state, gaps, challenges) vis-a-vis a range of emerging technologies – i.e. Where are we, today?
- Identify the end state (goals, aspirations, short and long-term) that we want to achieve as a nation – i.e. Where do we want to go?
- Strategize the path we may adopt to achieve the end state – i.e. How to achieve objectives?

Key Findings

- We live in an age of fast-moving and accelerating technological change today. Emerging technologies such as Artificial Intelligence (AI) and Robotics, Cyber Security and Quantum Computing, Cryptocurrency and Internet of Things, and New Materials and Synthetic Biology have the promise of propelling economies forward technologically and economically.
- These technologies are unique in the way that they interact or converge with older technologies in addition to enhancing one another. Some of these technologies (such as AI) are so foundational and multidisciplinary that they have been dubbed the “electricity” of our times. Others (such as Synthetic Biology) bestow upon the human race capabilities it never had before. Each of these, individually, has the potential to singlehandedly change the course of global development, and their coming together creates the perfect storm with possibilities of unparalleled prosperity but tremendous risks for corporations, nation-states, and humanity as a whole.
- Pakistan has a promising future in this sector if it can catch onto and follow through on some of these emerging technological waves because of its long-acknowledged strategic position, rich and diverse international diplomatic history of proximity to multiple centers of power, large youth population and a workforce with its natural affinity for STEM careers, and intrinsic socio-economic potential of a large and growing market.
- However, the tremendous possibilities of advancement and prosperity do not come without threats, risks, and challenges. As we continue to experience technology's transformative power, there is always the risk of being left behind at a time with the fastgrowing gulf between technological haves and have-

nots. It is, therefore, important to think strategically about emerging technologies and their implication on socio-economic and national security, prioritizing both state and human security and their interconnected nature, and develop a view and strategy for how to proceed forward.

- Pakistan must lay down a set of concrete priorities in these emerging technology areas to signal the critical importance these have for our socio-economic and military security.
- Artificial Intelligence in Pakistan is in preliminary stages and needs to be accelerated by focusing on the country's overall AI Readiness in public as well as private domains. Pakistan must adopt a liberal approach towards AI policy, preferring to regulate harmful use rather than the technology itself, that avoids overregulation that could stifle innovation.
- The country should also adopt a more private-sector-friendly policy that enables individuals and small firms to lead and create value rather than a public-sector-led policy paradigm that funds government and public bodies to lead the way.
- Pakistan must identify a small number of ambitious goals that advance prosperity, security, and the human condition with the help of AI (e.g. making education accessible to all out-of-school children, healthcare for all, and improvements in agricultural and human productivity) and as well quantifiable KPIs (outcomes and impact rather than inputs or outputs) and support multi-stakeholder partnerships to achieve those.
- Cyber Security is a clear and present danger that could quickly turn into a runaway threat for Pakistan due to a lack of properly coordinated policy and threats far outpacing investment in security infrastructure over the years. Only very recently has cyber security begun to receive policy interest with the rationalization and empowerment of the policy and oversight infrastructure and the creation of a National CERT.
- Much work remains to be done education, threat assessment, and sharing, bringing the country under action and response cyber security regime starting from the most critical and the most vulnerable actors, indigenous capacity building and technology development, and developing a framework of robust international cooperation and cyber diplomacy.

- While the National Cyber Emergency Response Team (NCERT) is the first step, providing effective cyber security may require the creation of a National Cyber Security Agency with a multispectral and countrywide mandate to arrest this runaway threat.
- Pakistan needs to embrace this new age of 'engineering biology' and take measures to establish a foothold in the field of synthetic biology by realigning its existing infrastructure and laboratories and retraining the workforce for this new era of biology.
- In this regard, the establishment of a National Center for Synthetic Biology could lead the charge in retraining, connecting, and laying out a research agenda for the country.
- Synthetic biology has the potential to address many of the country's challenges, the most important one being its narrow base of materials industry necessitating expensive imports that burden the economy and check economic growth, and its power, coupled with innovation and commercialization infrastructure, must be put to good use to address national needs and international competitiveness.
- Finally yet importantly, Pakistan needs to invoke its friendly diplomatic ties with developed economies such as the US, UK, Russia, China, Malaysia, and Singapore as well as KSA, UAE, Indonesia, Thailand, and others to build new knowledge corridors and scientific collaborations.

ISSRA COLLABORATION

SSRA COLLABORATION

PART I

ARTIFICIAL INTELLIGENCE IN PAKISTAN

Part I – ARTIFICIAL INTELLIGENCE IN PAKISTAN

Current State: Where We Are?

- Today Pakistan has some (preliminary) capability in the area of AI – some in the private sector, a bit in academia, and a negligible amount in the public sector. The country has largely missed the technology revolution of Generative AI. Except for the National Center for AI (NCAI) under the Higher Education Commission (HEC) and some (limited) capacity within the security establishment (such as with the PAF), there is hardly any public sector entity with worthwhile AI capability.
- On the application side of AI, the situation may be slightly better with smaller (private) players building applications in healthcare, education, agriculture, etc. There are also several companies (such as ADDO AI, Redbuffer, etc.) engaged in exporting AI software services to international clients and an even smaller number (such as Vyro.ai, Arbisoft, etc.) focusing on AI or AI-enabled products. The AI 'applications' opportunity may, therefore, still be within reach. However, AI, particularly Generative AI, is a very fast-moving target that is also evolving at a breath taking pace faster than anything we have seen since the Internet. As one of the participants in the AI roundtable pointed out: "There is an arena and a big match is going on, and we're not even present (as spectators) in this arena." Regardless of what our position is on the march of AI, globally, the choice for a country like Pakistan is clear. Pakistan needs to quickly catch up to at least get a seat on the table and be a spectator, if not a big player, in the arena.

The Structure of AI in Pakistan

- In Pakistan, the locus of policy is the Federal Ministries with the Ministry of Planning, Development, and Special Initiatives (MoPDSI) being entrusted with overall national, cross-governme-ntal, and long-term planning while the relevant line ministries are responsible for formulating and implementing individual policies. In 2023, the Ministry of Information Technology and Telecommunications (MOITT) launched a draft AI policy document for public review and feedback. Later, the Ministry of Planning, Development, and Special Initiatives

also launched a 15 member Task Force to fast-track the deployment of AI within the country In addition to these, other Ministries (such as MOI, and MOD) and entities (such as the Higher Education Commission) have launched their initiatives to take a closer look at AI in their respective spheres.

- The National AI Policy, however, remains a work in progress, as MOITT has not yet notified a revised draft and/or put something before the Federal Cabinet for approval.
- Once a policy is notified, the implementation will fall to several entities under the MOITT and other ministries as well as the Provincial Governments. There has also been no visible progress through the National AI Task Force notified by MoPDSI. Figure (below) outlines the current structure of AI within Pakistan.

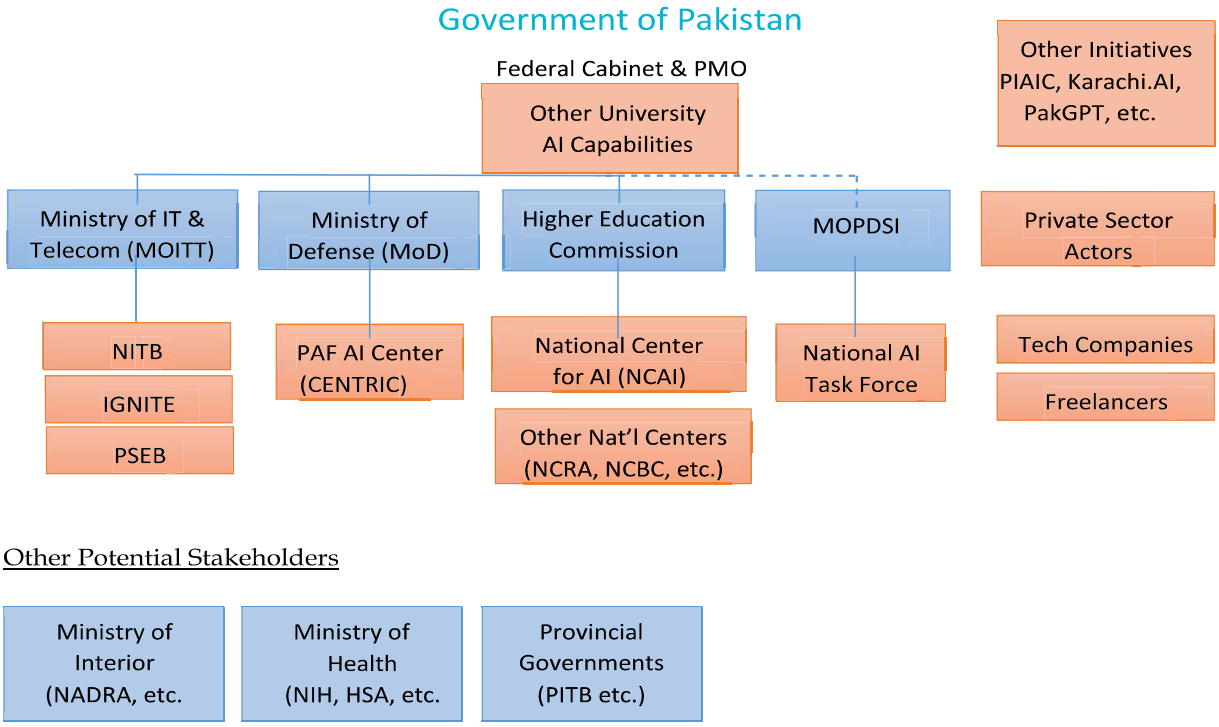


Fig: Structure of AI in Pakistan

Role of Different Sectors

The role of different sectors in AI is highlighted below:-

- **Role of Academia:** Academic institutions of Pakistan are offering bachelor as well as graduate and post-graduate level degree programs in Artificial Intelligence and its related subjects. Presently, there are 47 universities and colleges in Pakistan that offer bachelor-level courses in Artificial Intelligence, while 9 universities offer MS Artificial Intelligence. In 2017, a National Center for Artificial Intelligence (NCAI) was created to advance research and capacity building in various subdomains of AI including computer vision, surveillance, medical diagnostics, safe and smart cities, etc. Other initiatives in academia include the Center for Artificial Intelligence and Computing (CENTRIC) and the Sino Pak Center for Artificial Intelligence (SPCAI). Details are attached as Annex A.

- **Private Sector/ Industry:** Pakistan's private industry is leveraging AI technologies to boost innovation, improve efficiency, and tackle societal issues. Despite challenges, they are developing AI-based solutions, fostering a thriving AI-focused startup ecosystem. Startups are also working on innovative AI solutions and products, often leveraging technologies such as machine learning, natural language processing, computer vision, and robotics. Many of these startups have received funding from local and international investors to fuel their growth and development.

- **Private companies** are investing in skill development initiatives to address the shortage of AI talent in Pakistan. They offer training programs, workshops, and certification courses in AI-related fields to up skill the workforce and prepare them for careers in AI development, data science, and related roles. Top AIrelated companies are listed in Annex A.

Existing Policy Framework

- As part of its Digital Pakistan vision, Pakistan's Ministry of IT & Telecom unveiled a Draft National AI Policy in May 2023. This draft document reflects Pakistan's hopes to become a knowledge-based economy and establish an environment that would support the appropriate use of AI. It highlights the ethical and responsible use of AI as a policy objective, seeks to promote infrastructure investment for research and development, attempts to tackle the issue of job displacement, and talks about using AI to spur economic growth. The vision of the Policy is: "To Embrace AI by appreciating Human Intelligence and stimulating a Hybrid Intelligence ecosystem for equitable, responsible, and transparent use of AI." The policy framework is envisaged to provide a complete AI-enabling ecosystem in Pakistan, covering

all aspects of awareness, skill development, standardization, and ethical use" The government has also formed a National Task Force (NTF) on AI to develop a 10-year plan for the quick adoption of AI in the relevant industries.

- The establishment of the National Artificial Intelligence Fund (NAIF) and a series of Centers (s) of Excellence in AI and Allied Techno-logies (CoE-AI) have been proposed to leverage AI's potential for both societal good and private profit. The policy puts the onus of implementation of a range of AI initiatives – including the provision of public data on these COEs. This is something even the most powerful public sector IT organizations as well as Ministries themselves have been unable to do and is unlikely that COEs, as conceived in the policy documents shall be able to affect this.

- Similarly, the policy puts the considerable onus of implementation and execution on public

sector entities and not enough focus on the private sector and individuals who may have a first (and a fast) mover advantage in the emerging AI landscape. The draft policy, nonetheless, covers a very landscape and range of activities and seeks to build upon the Personal Data Protection Act the Pakistan Cloud First Policy, and other policy initiatives to advance AI forward in the country. This draft policy framework, however, has not yet been notified by the Ministry or presented before the Cabinet for approval and, therefore, remains largely non-operational. The detailed Policy Objectives, targets, and challenges are attached as (Annex B).

Objectives to be achieved– Where Do We Want to Go?

- Pakistan's draft National AI policy is a step in the right direction. However, Pakistan is good at making policies but is weak in their implementation. In the realm of technology and AI, policies and do uments exist, but do not have much ensuing practice to show for themselves. Meanwhile, AI is fast moving and is already taking the world by storm. Timely decision-making is the key to achieving results in this sector in Pakistan. As with the rest of the world, a major part of the development of AI shall happen within and with the support of the private sector in Pakistan. This will only happen if we create an AI-ready generation, invest in developing the right skills of both developing and deploying AI across the whole spectrum of socio-economic activity, and through public sector investment in infrastructure, enable the private sector to create value. Therefore, Pakistan should probatively facilitate and seek to create conditions and capabilities that would allow it to exploit the potential of AI to achieve, safeguard, and address economic well-being, governance, social development, and national security challenges. Given the above, a reprioritized set of goals is suggested, based on the two time frames below:

Short Term Goals (3-5 years)

In the short-run, Pakistan must target to quickly address the gaps within AI infrastructure and readiness by making foundational investments in AI readiness and capacity created through policy as well as public and private investments. This is necessary for providing the private sector and academia with the necessary environment in which they can begin executing meaningful programs and make additional investments for AI development and usage in various sectors.

Medium to Long-term Term Goals (10-15 years)

- In the medium to longer run, Pakistan could see that these foundational investments and policies are unambiguously beginning to pay off. For example, the following set of (hypothetical) targets may be possible within this time frame:
  - 10% of the country's GDP growth attributable to AI
  - 25% of Pakistan's IT exports come from AI services
  - 25% improvement in worker productivity and agricultural productivity due to AI
  - 100% of the country's out-of-school children (OOSCs) have access to educ-ation through AI and technology with improvements in literacy (with language barriers becoming a thing of the past!).
  - 100% of the population has access to special-ist healthcare (radiology, pathology, cancer, etc.) via an AI-assisted physician.

Strategy: How to Achieve Objectives

- This section lays out brief strategies/ steps for what needs to happen for Pakistan to get from where it is today (rudimentary capability but significant potential) to where it needs to go (significant capability and effective engagement). The strategy provides realistic and proactive policy recommendations for the promotion of AI in Pakistan. It takes a decidedly handsoff approach by charging the government with creating an enabling environment and addressing critical gaps in Pakistan's AI readiness.
  - Further, it leaves it up to the private sector to deliver value and socio-economic returns from this transformative technology. It also charges the government with ensuring that the benefits of AI – both social as well as economic, are widely shared.
  - Finally, it charges the government exclusively with ensuring and addressing that appropriate national security implications of AI are identi-fied, and efforts are made to achieve national security objectives and safeguard national security interests. This can be achieved via a policy of thoughtful guidance and enlightened regulation that is targeted, mission driven, and performance based, which encourages and accommodates the unique capabilities and incentives of all sectors across society. Details of the strategy are as follows:-
  - Pakistan's current socioeconomic landscape demands an exclusive strategy focused on the utilization of economic and human resources to create optimal outcomes with the least expen-diture. The government may provide financial assistance and grants to AI startups and companies looking to build AI capabilities to export AI products and services. More impor-tantly, the government should address the

gaps within the following domains to create the environment necessary for the private sector to create products and services in Pakistan:-

- AI Readiness
- Policy Domain
- Regulatory Domain
- National Initiatives

Short-Term Strategies(2-4 yrs) (AI Readiness)

Before a country can expect to realize socioeconomic returns, it must build foundational readiness for effectively developing, deploying, and utilizing a particular technology. AI Readiness for a country, at least in the short term, depends on three absolute essentials: people, public data, and infrastructure discussed below: -

- **People**
  - Access to talent/HR resources is the most vital ingredient in building an AI ecosystem. This talent can be divided into high-end talent (PhDs in Universities and Entrepreneurs in Industry), mid-level talent (Software Architects and ML/AI Experts), and low-level talent (Software programmers, coders, etc.). Conservative estimates of the available and/or transferable talent within each of these domains are:-
    - AI PhDs and Entrepreneurs – currently at ~200 needs to be pushed to ~500 in 5 years.
    - Mid-level Software Architects & ML/AI Experts – currently at ~100 to be pushed to ~500 in 5 yrs, and ~5000 in 10-15 yrs.
    - Low-level AI Talent (Programmers, coders) – currently at ~1000 to be pushed to 10,000 in 5 yrs, and 50,000 in 10-15 yrs.
  - Manpower investments require the most amount of time to become mature and the talent pipeline, at least in the short-run, may be quite inflexible. It takes 5-7 years to produce a freshly minted PhD, 5-10 years or more for an average entrepreneur to reach his/her most productive peak, 5-10 years for a mid-level ML/AI resource to be groomed through experience, and between 4-8 years for a low-level programmer/coder to be trained. It is, therefore, imperative that we develop and execute precise manpower capacity-building programs with clearly articulated output and outcome targets and do not miss a beat in engaging our best talent in these opportunities. The following strategies are suggested to strengthen the talent pool in Pakistan:

- University programs (PhDs, Masters, Bachelors), and industry talent development programs (certificate programs) be strengthened and scaled to provide the right quality and quantity of talent at each level. Some of this has already begun to happen, this needs to be improved and scaled.

- Critical skillsets like problem, solving, solution architecting, and critical thinking should be improved in future generations of technology students to increase their utility for the tech industry.

- Pakistan must focus on developing an employable workforce by reskilling and up-skilling generations ahead. The country's education system appears to be in tatters, computer science and software education being imparted does not meet the market demands. Redesigning the curriculum is required. AI has replaced and will continue to reshape the job market; therefore, skill development is the way forward. Fortunately, market signals have begun to move talent into AI/ML, this will help support the pipeline of future talent.

- While measures can be taken in the short-run to build an AI pipeline by attracting talent from other areas, Pakistan cannot overcome the challenges of creating a sustainable pipeline for AI talent in the long run without having access to quality and quantity of output from basic computer science programs or even further upstream - from schools themselves.

- Investments in K-12 education in the country are the single most important investment Pakistan can make in creating future competence in AI. While many may consider this too long-term an aspiration to be within the scope of an AI policy, it is something worth serious consideration if Pakistan aspires to become a moderate-sized player within the AI space.

- General societal awareness about AI also needs to be created. This means putting in place a conscious strategy for creating awareness among professionals of all ages and domains about AI and its potential uses across the professional spectrum. This should be a central element of the strategy to use AI to improve labor productivity in agriculture, industry, and services.

- **Public Data**

  - The availability of both structured and unstructured data sets in the public and private sectors is critical for developing and training AI models and applications. Clear data-sharing guidelines for making public and private sector data available for innovation, with appropriate controls and anonymization where required, must be an integral part of any AI policy. In short, AI cannot succeed unless there is data for it to learn from. In the absence of local data, researchers and startups are forced to build models and applications using foreign data sources, leading to contributions towards the development of somebody else's economy rather than their own. Open and public data, therefore, is an important element of an enabling environment for AI.

  - Pakistan must move from a closed data

mindset to a public data mindset starting from the government itself. Three very specific targets are being proposed for the first phase of implementation of this public data policy regime:-

- All government ministries and public bodies to release in public domain 50% of data by year 1, 75% by year 3, and 90% by year 5.
- All publicly funded data in the possession of academic institutions and private entities be made public (after appropriate anonymity, etc.) by end of year 1.
- All private actors must also commit to releasing all non-competitive data and a of competitive data (perhaps dated) within the public domain.
- Pakistan must develop a policy of classifying public data into critical, and non-critical and ensuring that the latter is immediately available in an anonymized manner. To keep data private, the government must petition a competent authority and prove why it is necessary to keep this data in away from the public domain to be allowed rarely and only on account of national security or similar implications. Public departments hold very large and relevant data that needs to be digitized and made available for research and development.
- Establishment and usage of a "National Cloud" based service at the federal as well as provincial level should be adopted. This service should be available for use by anyone (for a small fee) and must have all digitized data available for use.
- Expansion and strengthening of the role of Right to Information (RTI) Commissioners (or the creation of a Federal Data Ombudsman) should be undertaken to include adjudication on access to public data.

- Private sector entities such as those working in medicine, education, agriculture, retail, transportation, etc. must also be encouraged to make data interoperable (e.g. through the adoption of EMR/EHR systems) and, where possible, anonymized and available in the public domain.

- **Infrastructure**
  - Access to cloud and computing infrastructure – both centralized and decentralized is critical to the development of AI. This is an important area where public investment to create a public cloud and round-the-clock, remotely accessible computing facilities will help lower entry barriers for private sector actors. The Government may also consider lowering (or zero-rating) duties on computing infrastructure (GPUs, etc.) for private, academic, and public sector actors. For instance, the private sector may be allowed to spend up to (say) 35% of their annual increase in export earnings on importing GPU clusters for AI (and related

applications).

Medium to Long-Term Strategies (5-15yrs)

The following three aspects comprise the medium to long-term strategies for the future development of AI in Pakistan:-

- **Policy domain**
  - National AI policy (or strategy) is not just designed to move a country forcibly, and in a top-down fashion, in a particular direction. It can also signal a change in direction and a mild 'nudge' to organize a coordinated response to a particular challenge. In Pakistan, with a few exceptions, national policy of the first kind has been largely absent (or ineffective) due to a variety of reasons including lack of continuity, institutional and implementation capability, resources, etc. It is unlikely that this will be effective in AI in the short-to-medium term as well. The AI policy must take into account the nature of AI development taking place around the world and empower the various actors to do the same in Pakistan. In particular, the following broad principles of policy may be agreed upon before any detailed strategy or roadmap is developed or approved:-
  - The best policy course shall be one that is private-sector-driven and public-sector-enabled. The traditional approach, as also evident in the draft AI policy by MOITT, to burden and fund the public sector to do most of the policy execution hasn't worked out in the past and certainly not worked out for AI going forward as well.
  - The world over, AI is a fast-moving sector that is best addressed through the agility and profit incentive of the private sector (and individuals).
  - The policy must be implemented with a keen eye towards achieving clearly defined objectives and targets (milestones). Here it is important to focus on outcome and impact measures (e.g. productivity achieved, or exports generated) rather than input or output measures (such as money spent or people trained).
  - It is true that certain types of actions lead to outputs alone (e.g. manpower trained or awareness created) but these outputs are not the end in themselves but rather a means to an end (e.g. productivity or GDP growth achieved or exports generated). Our AI policy must focus on outcomes and impact and make individuals and organizations responsible for achieving these objectives.
  - Policy interventions and national initiatives are best achieved through incentivizing,

facilitating, or organizing multi-stakeholder partnerships that are private-sector-led and public-sector supported. This is to ensure that the private sector which is both a clear incentive and the required flexibility to act decisively to create value and be market responsive has the ability to do so. We must carefully address and strictly check the tendency of turf wars and duplication of effort between sectors.

- Pakistan should put in place a policy regime that largely focuses public sector energies on inputs (i.e. the actions outlined in AI readiness) and leaves the major outcomes to private initiative. The public sector should only intervene when there is a market failure that needs to be corrected or that cannot be addressed without direct provision.

- **Regulatory domain**

  - There should be no regulation on AI exports (software exports are already regulated or not regulated by the respective regulators of the importing countries) and Pakistan must not interfere in AI exports beyond what is necessary.

  - On the domestic front, there should be a serious and honest attempt to not regulate the technology but only its harmful applications. This should be done by building the capacity of existing regulators (such as SBP, PTA, SECP, HEC, etc.).

  - The approach towards new technology should be liberal rather than restrictive and regulation should only be adopted or strengthened once clear prospect or evidence of harm becomes established. An initially liberal approach towards new technology and innovation will give the necessary time and space for it to develop instead of overburdening or killing it in its infancy. (Here, for instance, the approach taken by SECP on the digital lending entities ('loan sharks') rather than SBP on crypto-currencies is the right way to go.

  - There is a need to build the capacity of current regulatory agencies to oversee and evaluate AI technologies and their applications -

  - A think tank or an entity to make public, an annual report on the State of AI in the country to help policymakers and regulators get a sense of where AI is heading, and what is needed to support its development.

  - We do not, therefore, support the creation of a separate regulatory agency with its additional teething problems, staffing, and burden on industry for AI at this early point.

- **National AI Initiatives.**

  A series of national initiatives are needed to help the country move the needle on certain key national objectives or challenges. These national initiatives must take the form of multi-stakeholder partnerships targeted, mission driven, and performance-based to help solve challenges. These could include:-

  - Development of Urdu and local language models (to address translation and availability of knowledge in local languages).

  - Development and use of small language models (for specific applications)

  - Use of AI in education and health (to provide 100% literacy to out-of-school children and access to specialized medical procedures and diagnostics)

- Use of AI for national security (to address its implications for warfighting and border security)
- Use of AI within NADRA, (to leverage NADRA's vast database for value creation). etc.
- The draft AI policy currently proposes the creation of one thousand initiatives costing PKR 1 million which is quite unrealistic under the current costs and efforts involved. While PKR 1 million may be enough to run a student project, any serious effort that makes a socioeconomic dent will require upwards of PKR 50 or 100 million each.
- A few carefully designed, properly funded, effectively implemented, and rigorously evaluated (national) projects that lead to socioeconomic impact are likely to be of much greater use than a large number of underfunded and ill-designed initiatives.
- Key operational areas/sectors within the government should be shortlisted through an AI Policy draft and government departments at federal and provincial levels, be given the annual ma ndate to invest 20% of their development budgets into AI-powered projects. In addition to local funding, Pakistan must also focus on partnerships with multinational groups and entrepreneurs to widen the scope of AI in Pakistan. Pakistan.

SUMMARY OF RECOMMENDATIONS/STRATEGIES ARTIFICIAL INTELLIGENCE ROADMAP FOR PAKISTAN

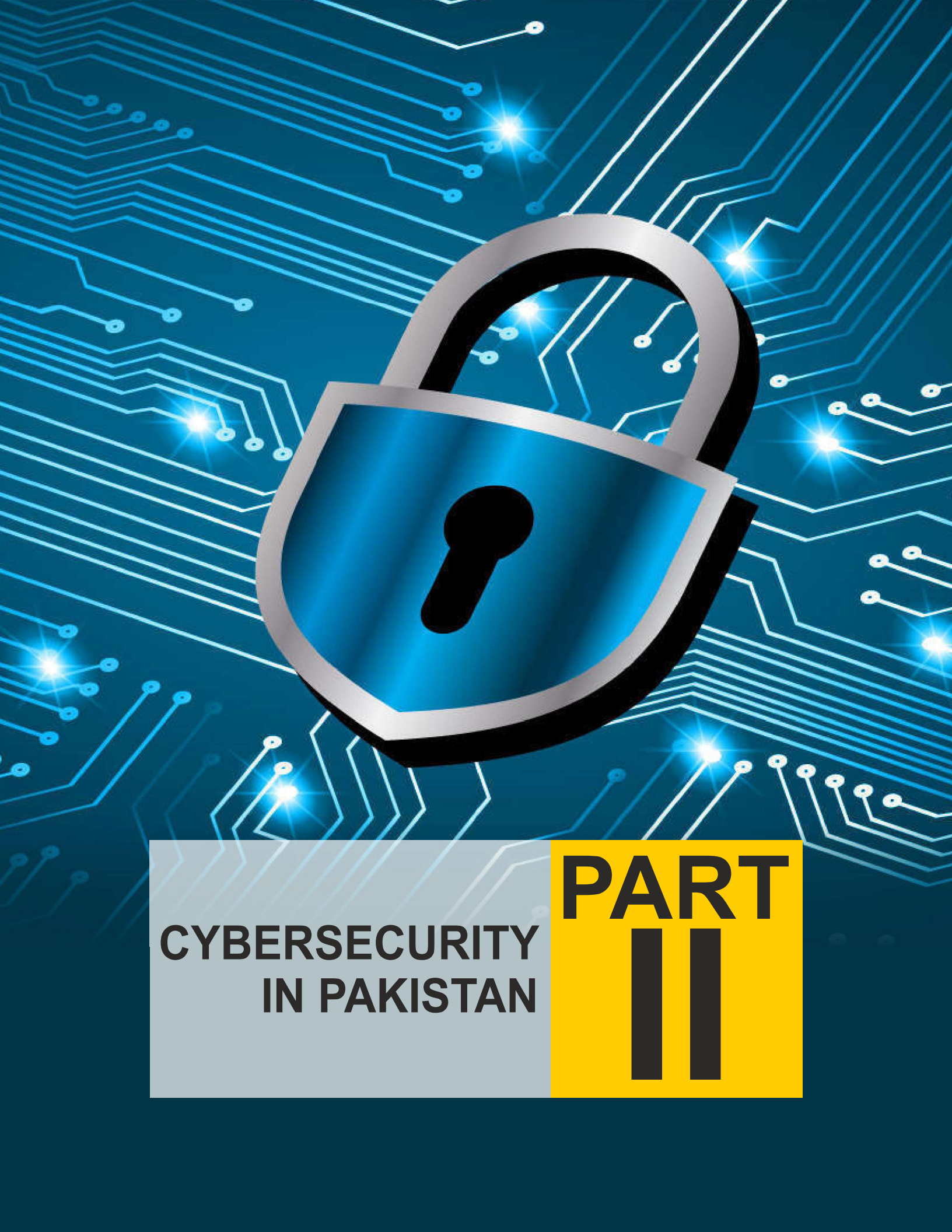
	Actions/Domain	***Expected Outcome***	***Key Implementers/ Stakeholders***
Short Term Strategy (2-4 yrs)			
AI Readiness (People)			
	• AI PhDs and Entrepreneurs – currently at ~200 needs to be pushed to ~500 in 5 yrs • Mid-level Software Architects & ML/AI Experts – currently at ~100 to be pushed to ~500 in 5 yrs, and ~5000 in 10-15 yrs • Low-level AI Talent (Programmers, coders) – currently at ~1000 to be pushed to 10,000 in 5 yrs, and 50,000 in 10-15 yrs.	• Access to talent/HR resources to build the required AI ecosystem	• Academia, Industry, MOITT
Public Data			
	• All government ministries and public bodies to release in the public domain 50% of data by year 1, 75% by year 3, and 90% by year 5. • All publicly funded data in the possession of academic institutions and private entities be made public (after appropriate anonymity, etc.) by the end of year 1. • All private actors must also commit to releasing all non-competitive data and at least 25% of competitive data (perhaps dated) within the public domain.	• The availability of both structured and unstructured data sets in the public and private sectors • Transformation from a closed data mindset to a public data mindset starting from the government	• All government ministries and public bodies
	• Establishment and usage of a "National Cloud" based service at the federal as well as provincial level • Expansion and strengthening of the role of Right to Information (RTI) Commissioners (or the creation of a Federal Data Ombudsman) • Private sector entities, including medicine, education, agriculture, retail, and transportation, should promote data interoperability, anonymization, and public domain availability through EMR/EHR systems.		

Infrastructure			
	• The Government may consider lowering (or zero-rating) duties on computing infrastructure (GPUs, etc.) for private, academic, and public sector actors. • The private sector may be allowed to spend up to (say) 35% of their annual increase in export earnings on importing GPU clusters for AI (and related applications).	• Access to cloud and computing infrastructure – both centralized and decentralized for the development of AI	• MOITT, Ministry of Finance, Planning Commission, FBR, and private sector
Medium to Long-Term Strategies (5-15 yrs)			
Policy domain			
	• Development of private-sectordriven and public-sector-enabled policies • Clearly define objectives and targets-milestones • Our AI policy must focus on outcomes and impact and make individuals and organizations responsible for achieving these objectives. • Policy regime that largely focuses on public sector energies on inputs, the public sector should only intervene when there is a market failure	• The policy of thoughtful guidance and enlightened regulation that is targeted, missiondriven, and performancebased, encourages and accommodates the unique capabilities and incentives of all sectors across society.	• MOITT
Regulatory domain:			
	• Removing regulation on AI exports • Building the capacity of current regulatory agencies to oversee and evaluate AI technologies and their applications	• An initially liberal approach towards new technology and innovation will give the necessary time and space for it to develop instead of overburdening or killing it in its infancy.	• SBP, PTA, SECP, HEC, etc

National AI Initiatives			
	• Development of Urdu and local language models • Development and use of small language models (for specific applications • Promote the use of AI in education and health to offer 100% literacy to out-of-school children and access to specialized medical procedures and diagnostics. • Use of AI for national security (to address its implications for warfighting and border security) • Use of AI within NADRA, (to leverage NADRA's vast database for value creation). • Any serious effort/project that makes a socioeconomic dent will require upwards of PKR 50 or 100 million each • Shortlisting of key sectors, and allocation of 20% of development budgets to AI-powered projects, partnering with multinational groups and entrepreneurs.	• Development of an enabling environment • The benefits of AI both social as well as economic, are widely shared. • Appropriate national security implications of AI are identified, and efforts are made to achieve national security objectives and safeguard national security interests.	• The government and all its related departments

SSRA COLLABORATION

ISSRA COLLABORATION



CYBERSECURITY IN PAKISTAN

PART II

PART II – CYBERSECURITY IN PAKISTAN

Current State: Where We Are?

- Cyber security measures play a vital role in protecting Pakistan's critical infrastructure, such as power grids, transportation systems, and communication networks. Pakistan's cyber security ranking, as per the National Cyber Security Index, stands at 85 out of 160 countries in 2023. This indicates a moderate standing in terms of overall cyber security preparedness. The Global Cyber security Index stands at 79 out of 194 countries and the 2022 Network Readiness Index (87 out of 130 countries) suggests challenges and considerable room for improvement. The Microsoft Security Intelligence Report Vol. 24 sheds further light on the cyber security landscape in Pakistan. According to the report, during the January–December 2018 period, Pakistan had a malware encounter rate of 18.94 percent, ranking second among the five locations with the highest rates. The top five countries with the highest malware encounter rates during this period were Ethiopia (26.33 percent), Pakistan (18.94 percent), the Palestinian territories (17.50 percent), Bangladesh (16.95 percent), and Indonesia (16.59 percent). This data underscores the significance of addressing cyber security challenges in Pakistan to mitigate the risks associated with malware encounters and enhance overall digital security.

- The potential impact of a cyber attack on critical infrastructure could have serious consequences for the country's national security and economy. Pakistan has witnessed several cyber attacks in the past. One of the most alarming cyber attacks targeted the National Bank of Pakistan between Friday, October 29th, and Saturday, October 30th, 2021. This cyber attack had a significant impact on the bank's backend systems, specifically affecting the servers that interlinked the bank's branches and the backend infrastructure responsible for controlling the bank's ATM network and mobile banking application

- Countries around the world have developed their cyber security infrastructures in line with their specific threat profiles as well as organizational and governance models. These cyber infrastructures usually involve key ministries such as ICT, Interior (or Home Affairs), Defense, and/or External Affairs. These cyber infrastructures usually have an implementation and execution arm (a key ministry such as Electronics and IT in India, Transport and Infrastructure in Turkey) and a

policymaking and/or oversight arm (e.g. National Security Advisor as in India or a National Cyber Security Board as in Turkey).

- In other countries, intelligence and security establishment players have a more direct role in managing cyber security (e.g. Revolutionary Guard in Iran). However, what is important is an effective legal and regulatory framework, a clear coordination between capacity and responsibility as well as demarcation of responsibilities (between Ministries), a robust mechanism for information sharing, and a singular chain of command running from policymaking, to oversight, for execution on the ground.

The Structure of Cyber Security In Pakistan

- The cyber security infrastructure in Pakistan has traditionally been fragmented and heavily reliant on intelligence services. The historical infrastructure can be described as 3-pronged dealing with the different nature of threats, namely: national cyber defense (critical infrastructure, etc.) being led by intelligence agencies and tri-services cyber commands; cybercrime being led by Federal Investigation Agency (FIA) under the Minister of Interior; and other private infrastructure protection being led by sectoral regulators (such as State Bank, PTA, SECP, etc.). While this infrastructure evolved, rather organically, because of perceived threats, it lacked central policymaking and oversight, a clear chain of command, effective information sharing, etc.

- Furthermore, the Ministry of IT and Telecom's role – which could be the natural home to high-quality IT manpower – was marginal in the overall scheme of things resulting in the mismatch between capacity and responsibility. Recognizing these gaps in the legacy infrastructure as well as the growing needs of the country, Pakistan's cyber security infrastructure has recently undergone a major upgrade. The following figure depicts the current state of the Cyber security structure in Pakistan:-

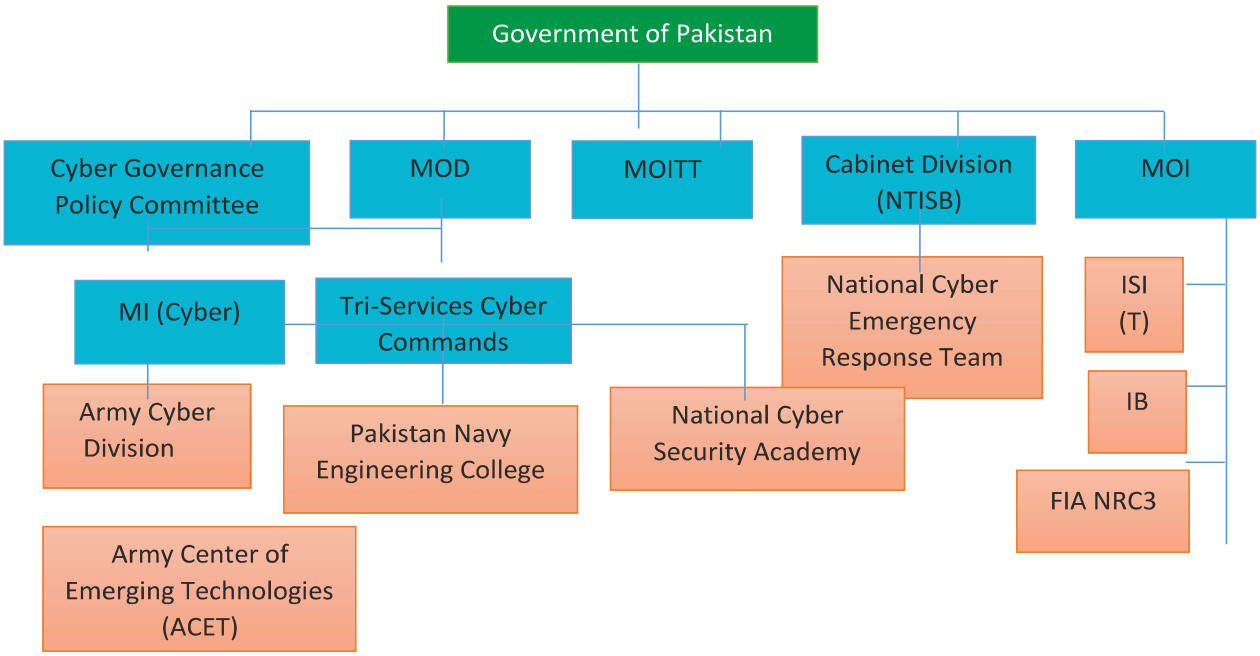


Fig: Structure of Cyber Security in Pakistan

- To begin with, a reorganized and reformed National Telecommunication and Information Technology Security Board (NTISB) under the Cabinet Division has taken over the national mandate for overall policymaking and oversight of cyber security. A National Cyber Emergency Response Team (NCERT) has been established by MOITT under NITSB to dev-elop and continuously update a national framework for cyber security, provide technical and operational capabilities, ensure coordination across different sectoral bodies and regulators, and provide cyber security services, training, and awareness to government, private sector, and the public at large.

- The NCERT has been a major gap in the country's cyber security infrastructure and is a welcome step in the right direction. In addition, the government has approved a National Cyber Security Policy in 2021. A major part of the cybercrime infrastructure rests upon the Prevention of Electronic Crime Act (PECA) Law introduced in 2016, though a recent development means this responsibility shall transition from FIA under the Ministry of Interior to a newly established National Cybercrime Investigation Agency (NCCIA) under the MOITT.

- Other important pieces of the cyber security infrastructure include the Pakistan Telecommunications authority (PTA) and its Technology, Vigilance, and Security Directorates responsible for, among other things, monitoring grey traffic and unauthorized access to telecom and internet networks. These recent developments have resulted in streamlining the nation's cyber security infrastructure and separating civilian cyber security from military cyber security leaving the latter to focus on its unique challenges. The roles of different sectors in this domain are discussed below: -

Role of Academia: Universities play an important role in the development of capacity – particularly human resources – for the country's cyber sec-urity

and defense. Several specialized program-mes and certifications exist to meet the requirements of the country though supply falls short of the perceived demand for such HR which in turn lags behind the actual need. In 2018, a National Center for Cyber Security was established at the Air University (Islamabad) to address the capacity to carry out research on critical areas of cyber security including cybercrime, malware, deep packet inspections, device security, and IoT security, among other things. (Annex - C)

Private Sector/ Industry: The cyber security industry in Pakistan has been growing steadily but is still relatively nascent compared to more established markets. However, it is gaining traction due to increasing digitalization, cyber security threats, and awareness among businesses and government entities. The cyber security startup ecosystem in Pakistan is gradually growing, with several startups focusing on developing cyber security solutions and services tailored to the needs of local businesses and organizations. These startups often leverage technologies such as artificial intelligence, machine

learning, and block chain to enhance cyber security defences.

Persisting Challenges:

- Despite the recent developments in the areas of cyber security, significant challenges remain in the way. These include reliance on third-party software, absence of security by design aspect in critical infrastructure security architecture, insecure government digital assets, overburdened National Response Centre For Cyber Crime (NR3C), lack of established cyber security technical procedures, etc.

- Although the empowerment of the National Telecommunication and Information Technology Security Board (NITSB) and the creation of NCERT has sought to address the lack of policy oversight and command, the infrastructure is still far from adequate and may require a National Cyber Security Agency to deal with the emerging threats in cyberspace. NCERT's work must also trickle down to the sectoral and organizational level via sectoral CERTs and other bodies for the organizational assets to be secure.

- The publication of CERT rules in September 2023 calls for the establishment of 3-tier CERTs at the national, sectoral, and organizational levels. The gazette notification of Pakistan Security Standards (PSS) for Cryptographic & IT Sec Devices in September 2023, with mandatory compliance from July 2028, reflects an effort to enhance cyber security standards. Adherence to these standards is crucial for securing critical infrastructure and sensitive information. There is still a considerable gap between what is mandated in various laws and regulations and what is available on the ground but serious effort is underway to bridge these gaps.

Objectives for Cyber Security: Where Do We Want to Go?

- **Proposed Objectives**

The National Cyber Security Policy of Pakistan 2021 is an important policy document that focuses on ensuring the security and resilience of cyberspace in Pakistan. The objectives of the policy are to protect critical infrastructure and information systems, raise awareness about cyber security in public, and establish mechanisms for enforcing and complying with the policy. Considering NCSP-2021 guidelines, a robust and comprehensive national cyber security program should include the following goals:

- Creation of a national cyber security threat and response system that works, both proactively and reactively, to ensure the country's most vital infrastructure and systems are properly protected against cyber threats, both domestic and foreign, through efficient, effective, and synergistic cooperation between various national (and international) entities.

- Develop an educated citizenry that is well aware of threats and vulnerabilities in the cyber sphere

and take appropriate and necessary actions to protect against these to ensure a safe and productive cyber presence for all

- To develop a cadre of cyber security professionals with both civilian and the defense sector – that can effectively address the exponentially growing cyber security threats from sources, domestic and foreign.

- Development and operation-alization of a differentiated threat and protection framework to ensure differentiated response and cyber security readiness across the country. For instance, 4 layers of cyber security readiness may be envisioned, namely:

  - List A: Critical Infrastructure (Utilities, Telcos, Aviation, NADRA, etc.), National Security appa-ratus (Tri-services, Strategic assets, Intellig-ence agencies, etc.), Government Ministries and Senior Leadership, and the Financial Syst-em (FBR, SECP, Stock Exchange, Banks, etc.)

  - List B: Important Infrastructure (Railways, Ports, Policing, Disaster Mana-gement Hosp-itals, Universities, etc.), Public sector bodies and connected government bodies, large private enterprises, and other hyper con-nected entities (such as Media, etc.)

  - List C: All remaining public infrastructure, isolated government departments, Hospitals, Schools, SMEs, etc.

  - List D: General population (all Individuals), irrespective of importance or priority.

- Complete (zero incident) Cyber security shall require a considerable expense, and may not even be feasible; therefore, achieving realistic levels of cyber security is always a balancing act between the level of protection achieved and the cost incurred in achieving it. Mission critical systems (List A) will require much higher levels of investment than successively less critical systems (Lists B, C, or D). A differentiated strategy shall allow these differing levels of

investments and security vs. cost trade-offs to be made systematically.

- It may be desirable to build cyber security capacity, infrastructure, and protection cover-age to:

  - 100% of entities in List A and 50% of entities in List B target within 3 years (2024-2027), and

  - 75% of entities in List B and 50% of entities in List C targets within an additional 3 years (2028-2030).

  - Risks to List D targets must be managed and minimized for example, to women, minors, or at risk religious minorities, are greater than others are but may still be tolerated due to their limited exposure and damage to the broader ecosystem.

Strategy: How to Achieve Objectives

Short Term Strategies (2-4 yrs)

- **Development of an appropriate legal framework for cyber security:** Pakistan must update its cyber security legal frame-work to protect citizens, balance freedoms and privacy, and create legislation tailored to its specific requirements and implementation paradigm. As the use of generative AI in social

media expands threats like fake news and digital impersonation. Pakistan must, therefore, catch up on laws and organizations required to protect its citizens in cyberspace. Balancing freedoms and privacy in cyberspace with specific legislation, it is crucial to create laws tailored to our specific requirements and implementation paradigm, rather than relying on foreign laws or external agendas.

- **Continuous Cybersecurity Education:** Promote continuous cyber security education at all levels to enhance awareness and preparedness. This involves developing educational programs, training modules, and awareness campaigns to instill a culture of cyber security across society. Mandatory Cyber security Programs should be introduced for all Govt/ Civil/ MoD Employees.

- **Crisis Communication and Public Trust:** Develop strategies for effective crisis communication and rebuilding public trust in the aftermath of cyber incidents. This goal involves establishing clear communication protocols, transparency, and proactive engagement with the public to mitigate the impact of cyber incidents. User data privacy protection standards and regulatory frameworks should be robust and not complicated in this regard.

- **Establishment of a National Cyber Security Agency (NCSA)**: Achieving the above may require the establishment of a dedicated National Cyber Security Agency (NCSA) to centralize monitoring and regulation of nationwide cyber security threats and a coordinated response. The NCSA shall be responsible For implementing the agenda and the key elements of the implementation plan outlined above. NCSA shall also work with, and oversee, sectoral cyber security strategies and plans as well as sectoral CERTs to address specific challenges within critical sectors such as defense and armed forces, classified organizations, law enforcement agencies, financial and economic sectors (such as banking, energy, and insurance), public services and utilities (including healthcare, education, IT and telecom, logistics, water management, housing and construction, and small and medium-sized enterprises), and environmental services. These sector-specific CERTs will help protect sensitive information, critical infrastructure, and operational continuity, addressing unique cybersecurity challenges in each sector

Medium Term Strategy (5-7 yrs)

- **Comprehensive Threat Sharing and Intelligence:** Establish mechanisms for comprehensive threat sharing and intelligence to enhance cyber security readiness. This goal requires the development of platforms and protocols for sharing timely and accurate information about emerging cyber threats.

- **National Threat Intelligence:** Platforms, STIX (Structured Threat Information Expression) and TAXI (Trusted Automated Exchange of Indicator Information Sharing and Analysis Centers (ISACs), and Information Sharing and Analysis Organizations (ISAOs) are to be considered at an immediate level.

- **Robust International Collaboration:** The Cybercrime Convention, also known as 'The Budapest has been adopted as a worldwide strategy to combat cybercrime. Pakistan, for a variety of reasons including a lack of appropriate laws, has been unable to sign the convention. Mobilizing international cyber security diplomacy, leading to signing the convention will enable Pakistan to address cyber threats originating from beyond the borders and protect the country's vital assets and infrastructure against threats domestic and foreign in nature.

Long-Term Strategy (10-15yrs)

- **Create Nationwide Cyber Security Strategies and Infrastructure:** Ensure (starting from List A, then B, and then C given in the above objectives) the development of appropriate nationwide cyber security strategies and infrastructures designed to work alone, or in alignment or synergy with other actors, towards a unified cyber security response. This involves creating partnerships, sharing expertise, building the infrastructure and capacity of organizations, and establishing joint initiatives to address cybersecurity challenges individually and collectively. Relevant bodies, including sectoral regulatory bodies, must launch initiatives to ensure enablement and compliance starting from the country's critical infrastructure down to the smallest SMES.

- **Self-Sufficiency in Technology:** Achieve self-sufficiency in cyber security technology to reduce dependency on external sources that may result in backdoors and other vulnerabilities. This requires investment in research and development, promoting local innovation, and maturing indigenous cyber security solutions. These may include national Firewalls, IDS, IPS, AV, National SIEM/SOAR, Encryption, etc. An exhaustive review of critical supply chains and their vulnerabilities to cyber attacks must be carried out and its recommendations. implemented to the latter.

SUMMARY OF RECOMMENDATIONS/STRATEGIES

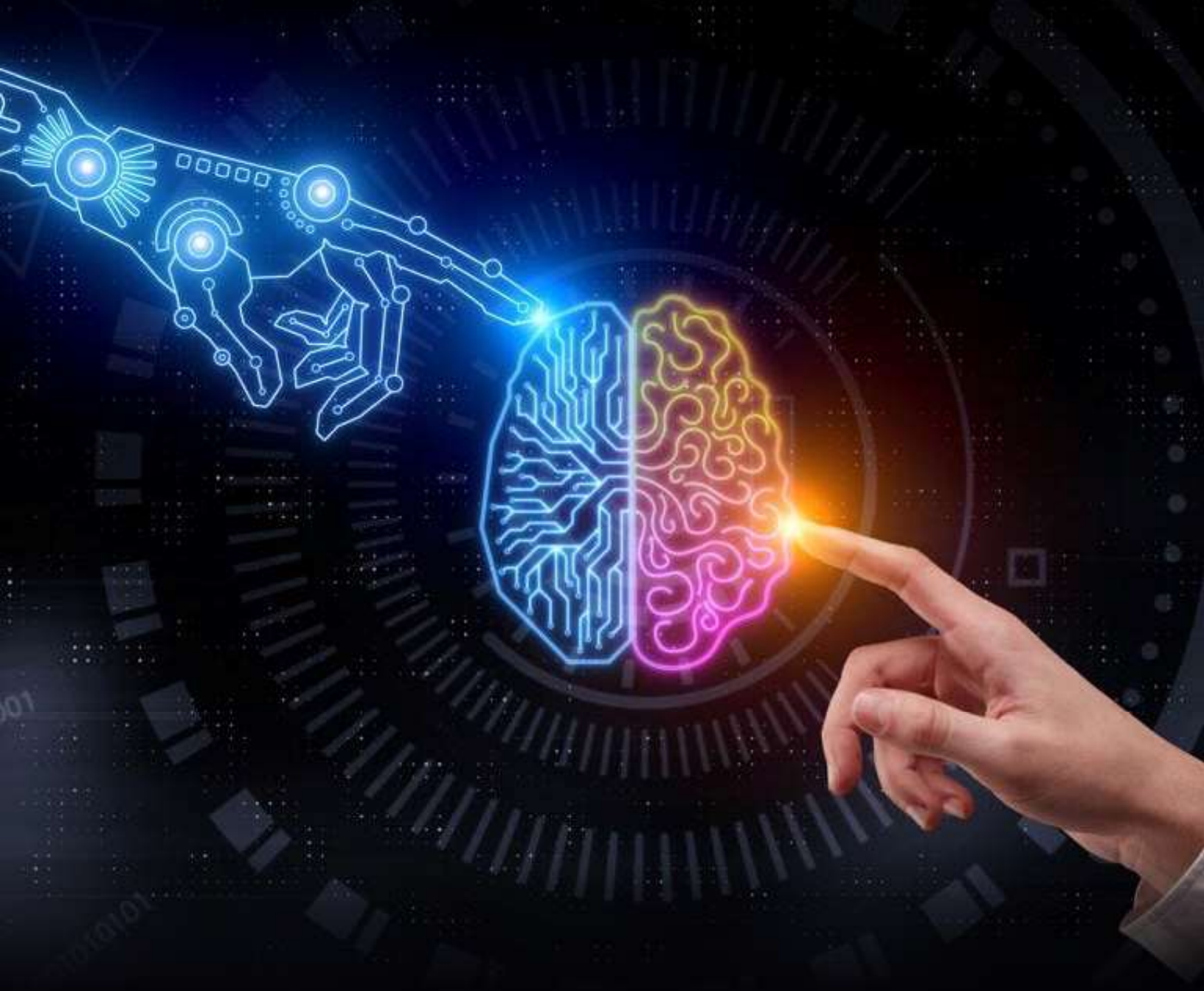
CYBERSECURITY STRATEGY ROADMAP: HOW ACHIVE OBJECTIVES

	Actions/Domain	***Expected Outcome***	***Key Implementers/ Stakeholders***
Short Term Strategy (2-4 yrs)			
	• Development of appropriate legal framework for cybersecurity • Cybersecurity Education • Crisis Communication and Public Trust Initiatives • Establishment of a National Cyber Security (NCSA)	• Laws tailored to our specific requirements rather than relying on foreign laws or external agendas. • Cyber Awareness of Govt/ Civil/ MoD Employees • Clear communication protocols, transparency, and proactive engag-ement with the public to mitigate the impact of cyber incidents • Protection of sensitive information, critical infrastructure, and operational continuity, addressing unique cybersecurity challenges in each sector	• National Cyber Security Agency (NCSA), MOITT & MOST
Medium-Term Strategy (5-7 yrs)			
	• Establishment of National Threat Intelligence Platforms, STIX (Structured Threat Information Expression) and TAXI (Trusted Automated Exchange of Indicator Information), Information Sharing and Analysis Centers (ISACs), and Information Sharing and Analysis Organizations (ISAOs) Signing of the Budapest Agreement	• Comprehensive Threat Sharing and Intelligence mechanism Robust International Collaboration along with protection of the country's vital assets and infrastructure against threats domestic and foreign in nature.	• NCSA

Long Term Strategy (10-15yrs)			
	• Establishing joint initiatives to address cybersecurity challenges by creating partnerships, sharing expertise, building the infrastructure and capacity of organizations • Initiatives to ensure enablement and compliance starting from the country's critical infrastructure down to the smallest SMEs	• Development of Nationwide Cyber • Security Strategies and • Infrastructure	• NCSA and relevant ministries along with media platforms
	• Investment in research and development, promoting local innovation, and maturing Indigenous cyber security solutions (These may include national Firewalls, IDS, IPS, AV, National SIEM/SOAR, Encryption, etc	• Self-Sufficiency in cyber protection and overall Technology	• Relevant Ministries and Government Departments

ISSRA COLLABORATION

ISSRA CO LAB RATION



SYNTHETIC BIOLOGY IN PAKISTAN

PART III

PART III – SYNTHETIC BIOLOGY IN PAKISTAN

Current State of Synthetic Biology: where we are?

- Synthetic Biology is the redesign of existing living organisms and their functions or the design of living organisms or functions that are otherwise non-existent, for various applications in medicine, agriculture, energy, and other industrial sectors. Synthetic Biology is different from preceding technologies such as genetic engineering and biotechnology in both its scale and potential. Traditional biotechnology, for example, was able to give us insulin by 'copying' the human insulin gene and 'pasting' it into a bacterium or yeast.
- "Synthetic biology aims to design and engineer biologically-based parts, novel devices, and systems as well as redesigning existing, natural biological systems," according to the Royal Academy of Engineering (2009). According to a World Economic Forum report on technology trends, one of the twelve innovative and destructive technologies of the future that would drastically alter industry, commerce, and life includes synthetic biology.
- What synthetic biology has done to the top-down discipline of traditional biology is nothing short of transformative, as it has reduced the cost and speed of making biological/genetic interventions by several orders of magnitude. For example, while in the past modifying varieties of plants and crops to achieve desirable properties would have taken a few years and several millions of dollars, with synthetic biology this can be achieved with laser-like precision, within weeks (if not days), and at a fraction of the cost. By modifying cells (fashioned as biological circuits), component-by-component, synthetic biology has made biology more like an engineering discipline rather than a traditional science. This has tremendous consequences, both opportunities and challenges for countries such as Pakistan.

Objectives: Where Do We Want to Go?

- **Existing Objectives**:

  Pakistan has a good amount of biotechnology infrastructure across the country from organizations like NIBGE in Faisalabad and NIFA in Peshawar under the PAEC, to university setups like the Centre for Excellence in Molecular Biology at Punjab University. Albeit small in

number at this stage, pockets of interest and/or excellence do exist in the new area of synthetic biology across the country, these include groups at LUMS, NUST, COMSATS Islamabad, Habib University, UIT University, and of course, CECOS University which hosted Pakistan's first two teams of undergraduate synthetic biologists that competed in the IGEM competition. Unfortunately, there are no national or provincial strategies or roadmaps that set any direction or objectives for the synthetic biology community in the country.

- **Proposed Framework:**
  - With clear goals and well-defined steps, the life sciences sector in Pakistan can be set on the right path. This has to be achieved by addressing the near term in a 'Five Year Plan' and addressing the medium and long term in a '15 Year Plan', but in parallel.

The Immediate to Short-term Goals (1-5 Years)
The following goals should be aimed at to be achieved in the short term:-

- Rally, align, connect, and upgrade active research groups in the country and set a direction for the future. This may involve hiring young researchers with systems and synthetic biology training into traditional biology and biotechnology departments and research groups.
- It may require sending researchers trained in these traditional fields on post-docs to upgrade their skillsets such that at least 25% of the workforce in the traditional biotechnology departments have upgraded themselves to the newer directions in these fields.
- Pool equipment and resources and establish 'foundry' infrastructure under a single roof in 2-4 key strategic locations declared across the

country.

- Identify 3-5 grand challenges that need to be solved in the immediate term. These may include the replacing of top-10 biological imports that can be bio-manufactured indigenously; creating active ingredients of pharmaceuticals and reagents for diagnostic tests, as well as developing new materials using biological rather than extractive or chemical processes.

Medium to Long-Term Goals (5-15 Years).

In the medium to short term, synthetic biology can revolutionize Pakistan's healthcare, climate remediation, and materials industries and have a substantial impact on Pakistan's foreign exchange situation. For example, 5-15-year targets could include:

- Replacing all diagnostics kits for all diseases with indigenously produced ones.
- Making testing for all communicable and non-

communicable diseases accessible to all Pakistanis.

- Replacing imports of 100% livestock and the top 50% of all human vaccines in Pakistan.
- Replacing imports of all off-patent biologics in Pakistan.
- Sequencing 1 million genomes across the population including the top 10 No communicable diseases (NCDs), top 10 infectious agents, and top 100 economically important plant and animal species.

Additional Strategic Objectives: Some additional strategic objectives are laid out below: -

- **Academia**
  - Pakistan needs to mobilize its higher education sector towards the development of a critical mass of highly skilled workforce in the field. This will require new programs and certifications to be established and involve the upskilling of graduates of biotechnology, molecular biology, biochemistry, microbiology, and related disciplines in the country.
  - Pakistan needs to establish a prioritized list of goals, or grand challenges, that can direct and channel the academic and intellectual interests and prowess of our academia and industry, especially our youth, towards solving the problem of lack of synthetic biology training and awareness, which is a problem of high significance for the economy and the country as a whole.
  - To be able to contribute internationally and be globally competitive, Pakistan will also need to strengthen its base of education and research in foundational technologies that underlie all the developments in the fast-moving field of synthetic biology. These include DNA sequencing technologies, DNA synthesis technologies, computer-aided bio-design software, the use of big data and AI, and all the underlying basic fields of science including physics, chemistry, biology, and mathematics.
  - The gap between academia (where the newest technologies are developed) and the industry (where they are deployed) needs to be reduced by incentivizing and helping both sides to come closer.
  - Most of the challenges facing the industry are indigenous. Indigenous resources need to be promoted and academia should be given incentives to promote research. This will create healthy competition and promote the local industry.
- **Regulations**
  - Regulatory reforms are needed to address bottlenecks in science, such as outdated public procurement rules, perishable reagents, and kits, as well as customs and taxation regimes that hinder rapid progress in experimental

work.

- Pakistan needs to engage in science diplomacy and develop renewed and long-lasting Scientific and technological bilateral collaborations and multilateral consortia.
- When it comes to policy formulation, the advisory board holds immense importance. The scientists and researchers should be advising policymakers as they have a thorough understanding of the subject.

Industry

- A major challenge that the sector faces in Pakistan is the lack of manufacturing by the industry. Industries that are not manufacturing should be penalized and their rebates should be taken away. The business community must be given a clear view of what can be achieved. This will minimize investor's risk and help attain more funds.
- For better results, synthetic biology should be divided into different tiers of a pyramid and each tier should be dealt with at the grass-root level. Skill development forms the bottom of the pyramid. Having requisite skills is of extreme significance, however, the development of skills is not being dealt with on a priority basis and this is affecting the growth of the sector.
- Scientists and researchers should take the lead role as they have knowledge and are aware of the needs of the field. Moreover, these individuals should be trained as per the needs of the market. The abovementioned steps are summarized in the figure below.

Strategy: How to Achieve Objectives

- Pakistan needs a fresh concerted effort to revitalize the life sciences community and ecosystem in line with the latest principles and best practices and build a foundational base for the inevitable synthetic biology transformation in the world. This could also warrant the notification of new departments, units, or sub-sections under science and technology ministries or departments in the federal and provincial governments that have the sole mandate of developing synthetic biology as a sector in the country. Pakistan needs to lay down a priority list of technolo-

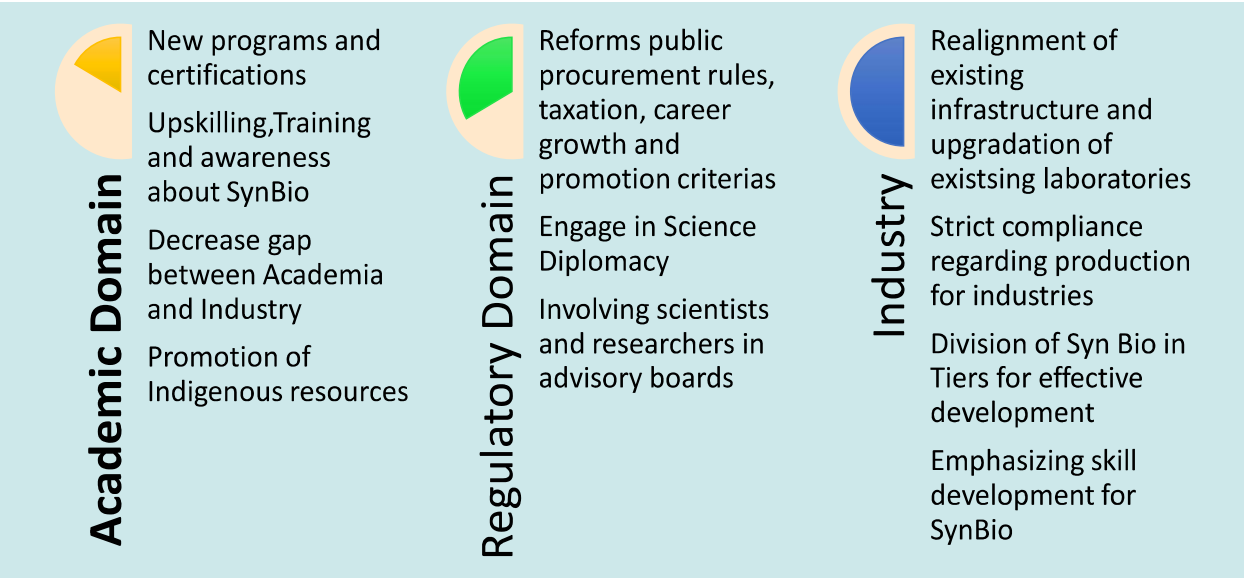


Fig: Strategic Objectives for Development of SynBio in Pakistan.

gies to signal to all institutions and their bureaucratic structures about the critical importance of these for our economy.

- A few strategic steps in this regard are given as follows in short, medium, and long-term strategies: -

Short-Term Strategy(1-5 yrs)

- **Establish a National Center for Synthetic Biology:** Establishment of a national structure or a group of top laboratories to put a dedicated focus on different aspects of research and development that will seed the Pakistani scientific ecosystem as well as our industry with ideas, inventions, prototypes, and products that will shape the first wave of synthetic biology in the country. A central body be introduced so that resources can be pooled at one point. This will allow a decision-making process.
- **Upgradation of Infrastructure:** Pakistan's biotechnology laboratory infrastructure is at best sparse, incomplete, and at worst obsolete. A zero-cost intervention could be to bring new rules and mechanisms for the following outcomes: -
  - To bring the most critical and expensive equipment under one roof in strategically chosen locations across the country.
  - To repair or auction broken pieces of equipment that are no longer needed.
  - To donate obsolete ones for teaching purposes.

Medium-Term Strategy (5-10 yrs)

- One of the biggest bottlenecks of a biology laboratory infrastructure is sensitive and perishable reagents and kits. This needs to be addressed with a multi-pronged strategy that includes improvement in supply chains by

inducing reforms within the Public Procurement Regulatory Authority (PPRA), taxation, and customs.

- Fostering strong relationships with top producers across the world to provide a shockproof supply line of required goods and development of an indigenous development plan for such consumables in the country will be beneficial for the sector.
- Faculty incentives need to be reworked to excite and reward them for time spent in industry doing startup companies or solving real-life problems for the country (and not being able to publish those works).
- There is a need to do a SWOT analysis of existing biotechnology centers to identify gaps and limitations.
- The Higher Education Commission (HEC) can create scholarships and give industrial placements to students to ensure that the graduates are trained and experienced in market needs.

- The landscape of synthetic biology in Pakistan needs to be reimagined through grassroots initiatives like capacity-building workshops, mentorship programs, and the creation of centralized resources and infrastructure. These initiatives will equip educators and students with the knowledge and skills to develop SynBio solutions to local issues, which will ultimately lead to the creation of a more inclusive and diverse bio-economy.

Long Term Strategy (10-20 yrs)

- Pakistan will need to develop a strategic workforce development plan in the SynBio space. That involves all stakeholders from the HECs and TEVTAs to Universities and Colleges as well as teachers and professors. A workforce is required at every tier level of every skill set.
- There needs to be a shift in Pakistan's overall educational programs. This includes curriculum, pedagogy as well as philosophy. There needs to be a shift from teaching biology as a science to biology as an engineering discipline.
- Formulation of policies is not an issue but their implementation is. However, policy language should be simple and to the point so that multiple interpretations are not deduced.
- To improve commercialization ratios and bridge the gap with the industry, new placement, and sabbatical programs can be launched for high-performing students and faculty to spend time in the industry.
- The government should help and enable the private sector to take up synthetic biology and partake in research in this area. Public-private partnerships (PPPs) need to be promoted. Startup incubation programs similar to National Incubation Centers (NICs) can be developed to spur a wave of startups in this particular space.
- Pakistan needs to invoke its friendly diplomatic ties with developed economies such as the US, UK, Russia, China, Malaysia, and Singapore as well as KSA, UAE, Indonesia, Thailand, and others as a part of science diplomacy to build new knowledge corridors and scientific collaborations.

SUMMARY OF RECOMMENDATIONS/STRATEGIES

SYNTHETIC BIOLOGY STRATEGY ROADMAP: HOW TO ACHIEVE OBJECTIVES

	Actions/Domain	***Expected Outcome***	***Key Implementers***
Short Term Strategy (1-5 yrs)			
	• Establish a National Center for Synthetic • Biology • Up gradation of Infrastructure	• Ideas, inventions, prototypes, and products that will shape the first wave of synthetic biology in the country • Resources can be pooled at one point. • Smoother decision-making process. • Critical and expensive equipment under one roof	• HEC, MOST & Relevant Departments
Medium Term Strategy (5-10yrs)			
	• Reforms within the Public Procurement Regulatory Authority (PPRA), taxation, and customs • Incentivizing faculty for problem-solving for national domestic issues • SWOT analysis of existing biotechnology centers • Grassroots initiatives like capacity-building workshops, mentorship programs Scholarships, and industrial placements to students.	• Improvement in supply chains • Identification of gaps and limitations. • Training of Human • Resources and capacity building • Creation of an inclusive and diverse bio-economy	• HEC, MOST & Relevant Departments

Long Term Strategy (10-20 yrs)			
	• Development of a strategic workforce development plan in the SynBio space • Shifting from teaching biology as a science to biology as an engineering discipline	• Development of workforce for promotion and utilization of SynBio for the national cause	• HECs and TEVTAs to Universities and Colleges as well as teachers and professors
	• Introduction of new placement, and sabbatical programs for high - performing students and faculty to spend time in the industry • Development of Startup incubation programs similar to National Incubation Centers (NICs)	• Improved commercialization • Ratios • Bridging the gap with the industry • Promotion of Public-private partnerships (PPPs)	
	• Promotion of friendly diplomatic ties with developed economies as part of science diplomacy	• Establishment of new knowledge corridors and scientific collaborations	

ISSRA COLLABORATION

CONCLUSION

The paper highlights the importance of developing, excelling, and sustaining progress in emerging technologies in Pakistan by addressing a gap between public policy formulation and implementation. It suggests combining responsibility with accountability, requiring structural and business reforms in public offices to make them more efficient and transparent. Experts also suggest that relevant departments should work synergistically to achieve objectives, using key performance indicators and tangible, quantified results. Government involvement in business should be limited and well defined, while the private sector should be more substantially engaged. A rules and standards based business culture is needed, as the private sector has proven successful with minimal regulations. The paper also suggests bridging the gap between academia and industry through policy interventions based on research commercialization, with the Higher Education Commission of Pakistan playing a vital role. The amalgamation of these efforts will prove to be a catalyst in the overall development of Pakistan's technology-driven knowledge ecosystem.

Anx A

COMPILED DATA ON GOVERNMENT POLICY, INSTITUTIONS, UNIVERSITIES, AND PRIVATE ENTITIES WORKING ON ARTIFICIAL INTELLIGENCE IN PAKISTAN

GOVERNMENT POLICY	OBJECTIVES OF THE GOVERNMENT POLICY
National Artificial Intelligence Policy	**Vision:** Owing to the impact of AI globally and its local adoption and implications, the Government of Pakistan envisions: ***"To Embrace AI by appreciating Human Intelligence and stimulating a Hybrid Intelligence ecosystem for equitable, responsible, and transparent use of AI."*** **Policy objectives:** • Training and up skilling human capital in AI at all levels to address the needs and demands of the market efficiently. • Integrating AI into the National Curricula at all levels is essential from a necessity, application, and use standpoint. • Ensure the ethical use of AI through inclusive and forward-looking guidelines. • Increasing public awareness to facilitate the adoption of AI sustainably. • Provide an enabling platform for AI with appropriate sandbox and agile regulatory arrangements to address societal and regulatory challenges (only • Where necessary). • To embrace research and innovation-based culture, offer fiscal/non-fiscal incentives to start-ups/SMEs investing in AI-based services/technologies. • Define data standards and invest in computational resources for the responsible use of organized datasets. • Strengthen international collaboration with both academia and industry

UNIVERSITIES OFFERING COURSES IN ARTIFICIAL INTELLIGENCE (AI)

- Department of Computer Science, Comsats University, Islamabad,
- Center of Excellence in AI, Bahria University, Islamabad,
- Department of Creative Technologies Air University, Islamabad,
- Department of Artificial Intelligence, National University of Science and Technology, Peshawar,
- Department of Computer Science, Shaheed Zulfiqar Ali Bhutto Institute of Science and Technology, Islamabad
- Department of Computing and Information Technology, University of the Punjab, Lahore,
- Department of Artificial Intelligence, National University of Computer and Emerging Sciences, Karachi,
- Department of Computer Engineering, University of Engineering and Technology, Taxila
- Department of Artificial Intelligence, University Of Management And Technology, Lahore
- Cholistan University Of Veterinary & Animal Sciences

RESEARCH CENTERS WORKING ON ARTIFICIAL INTELLIGENCE		
NAME OF THE DEPARTMENTS	**INITIATIVES OF THE DEPARTMENTS**	**AIM OF THE PROJECT**
Ministry of Information Technology and Telecommunication(MOITT)	High Impact Skills Boot Camp (MOITT): CDWP Approved05.04.2021	High Impact Skills Boot Camps for certain critical new ICT technologies will be established through service providers on the Train the Trainer (TOT) concept at different locations of Pakistan initially in Islamabad and Karachi. Boot Camp Training Service Provider will provide a model course work and methodology to be used as a guideline to universities and other institutions to train students in the future and prepare them for SOFTWARE DEVELOPMENT jobs in the fields of Cyber Security, Cloud Computing, Artificial Intelligence (AI) and Blockchain technology) for the next decade: 2020-2029.
Pak-Austria Fachhochschule Institute of Applied Sciences and Technology (PAF-IAST)	Establishment of SINO-Pak Center for Artificial Intelligence (PAF-IAST) **DDWP Approved** **21-01-2020**	PAF-IAST got approval to establish the Sino-Pak Center of Artificial Intelligence from public sector development funds. The core objective of the center is to build national capacity to carry out R&D in the emerging field of artificial intelligence by producing expertise through MS/PhD programs in collaboration with Chinese and Austrian universities. To solve local problems using AI and market them through the technology park. Provide high-value shared services to industrial partners. Develop an advanced workforce in AI and Data Science through training and applied work. Help in creating an ecosystem for startups and spin-off companies to make Islamabad an I the infrastructure and trained human resource.

Ministry of Information Technology and Telecommunication(MOITT)	National Center for Research Innovation and Entrepreneurship and AI and Allied Technologies. (MOITT) **DDWP Approved** **05-10-2020**	The Ministry of Information Technology and Telecommunication is evaluating the scope of AI from a global and local perspective about Pakistan's planned transition towards a technology-driven knowledge economy to assess the need for the establishment of such centers.
Ministry of Science and Technology	Establishment of the Centre For Artificial Intelligence (AI) In Health Sciences (Knowledge Economy Initiative) **CDWP 09-12- 2019** **Starting Date 06-01-2020**	To build up the national/provincial level center in AI for research and training purposes. • To raise awareness among the masses of people about the use of AI in daily life. • To establish a hub of innovation for the applications of AI and to create entrepreneurship in AI areas of research.
Ministry of Science and Technology	Advanced skills Development through international (Knowledge Economy initiative) Advanced Skill Scholarships **CDWP 03{3- 2020** **ECNEC 2141-2021** **Starting Date 1547-2021**	The prime objective is to provide international education of high standards to students at various academic levels. Providing opportunities to students to excel in emerging technology thrust areas such as AI, Block Chain, and other emerging technologies to become domain experts.

PAKISTANI PRIVATE COMPANIES WORKING IN THE FIELD OF ARTIFICIAL INTELLIGENCE (AI)

1.	Teradata Global	32.	Data Pilot
2.	LMKR Resources	33.	InvoZone
3.	CUBIX IT	34.	Kualitatem Private Limited
4.	AstroAlgo	35.	Xeven Solutions
5.	Ovex Technologies	36.	Devsinc
6.	Next bridge	37.	AlgoRepublic
7.	Hive WORX	38.	Arbisoft
8.	Sybrid Pvt Ltd	39.	Afiniti Pakistan
9.	Red Buffer Ltd.	40.	Five Rivers Technologies
10.	10Pearls	41.	TRG Global
11.	Genesis IT Lab	42.	AVAIL
12.	Zaytrics Ltd	43.	Salactsol
13.	Codeaza Technologies	44.	Innolytix Ltd
14.	National Incubation Center	45.	Metre 360
15.	Mozzine Technologies	46.	BlockApex
16.	SNSKIES Pvt Ltd	47.	KalSoft
17.	AbsoluIT	48.	based technologies
18.	DPL (Pvt) Ltd.	49.	Intelligence
19.	Arbisoft Islamabad	50.	WPExperts.io
20.	Ovex Technologies	51.	Liquid Techno
21.	I2c Pakistan		
22.	TECHNICS		
23.	FOCUSTECK		
24.	CLUSTOX		
25.	Dynamic Online Technologies		
26.	DATALATICS		
27.	Emblem Technologies		
28.	Phaedra Solutions		
29.	Mountains		
30.	Marriala Consultants		
31.	Ekkel AI		

Anx- B

NATIONAL AI POLICY OBJECTIVES AND TARGETS: The strategy paper provides a plethora of developmental activities required for awareness and uptake, redefining the fair and transparent use of personal data through AI and fostering innovation through partnerships between industry and academia as well as investments in AI-led projects. The following characteristics define the National AI Policy, which is designed with the fair distribution of opportunities and their responsible usage at its core.

- ✓ Evidence-Based and Target Oriented
- ✓ User-Centric and Forward-Looking
- ✓ Objective and Overarching

The AI policy further aims to augment AI and allied technologies through balanced demand and supply interventions, as briefly described below:-

- Market Enablement - Establishment of research & and innovation centers in AI for developing, test-bedding, deploying, and scaling AI solutions. This includes learning how to improve governance and manage the impact of AI.
- Progressive and Trusted Environment – Responsible use of AI to generate economic gains and improve lives. In addition, AI will raise the Government's capability to deliver anticipatory and personalized services.
- Enabling AI through Awareness and Readiness - Pakistan shall increase awareness and understanding of AI technologies and their benefits; our workforce will be equipped with the necessary competencies to participate in the AI economy.
- Transformation & Evolution - Transformation of sectors and industries towards effective use of AI, facilitated by national IT boards through creating awareness and offering training programs through sectoral cooperation.[1]

IMPLEMENTATION FRAMEWORK AND REVIEW PROCEDURE: The policy outlines a comprehensive framework with a steering/management committee, working groups, policy implementation cell, and review system. The committee, comprising representatives from the public sector, business, academia, and civil society, will oversee policy implementation and maintain it. Working groups will collaborate with academic institutions and international organizations for policy-relevant research.

[1] "Artificial Intelligence Law in Pakistan – Josh and Mak International," accessed January 5, 2024, https://joshandmakinternational.com/artificial-intelligence-law-in-pakistan/.

CHALLENGES: The following briefly describes the current state of challenges that exist in several different areas that are of importance in our quest for creating a future for Pakistan in the Age of AI:

- **Policy and Intent:** In Pakistan, today, the policy intent seems missing. The Draft AI policy which was widely circulated ago by the Ministry of IT and Telecom for comments, has received no follow-up. There is no clear sense of direction or urgency. Regardless of the political and economic challenges at home, AI is fast-moving but it has not (yet) become a priority at home.
- **Awareness:** Moderate level of awareness within academia. Low to moderate awareness within Industry and policy circles, and rudimentary awareness within the broader society.
- **Data and Public Access:** Pakistan currently stands at a low-to-medium level in the generation of data. And a low level of providing public access to data. Pakistan does not have an Open Data Policy and an Open Data Portal created 5 years ago remains under-populated and under-subscribed.
- **AI Infrastructure:** Pakistan, today, will score low on public infrastructure for AI (compute+cloud). There is no publically accessible cloud or computing capacity within the country. There is some capability in academia (at NUST, NED, LUMS, etc.) but these are not accessible outside of academia (or even to each other).
- **Manpower and Talent:** Pakistan, today, will score a low-to-medium on manpower and talent. There is a large base of young people within the country but their access to quality educational programs – particularly at the higher end – is limited. A few AI-focused training efforts are underway (such as Karachi.AI, PIAIC, etc.) and a few bachelor's/masters programs have sprung up in the last few years, but the supply of manpower and talent remains grossly undersupplied.
- **Industry:** For the last many years, there has been much talk of AI within the industry – particularly the startup community. Most companies that claim to be using AI use it as a “fashionable” thing to say about what they’re doing. However, there is some legitimate AI activity within the Industry – with probably 30-40 companies actively involved in building AI applications, mostly in retail, marketing, health, and education for both export and local deployment.

Overall, the above will probably place Pakistan, currently, at a low level of capability and development of AI. There are several areas with promise and some capability, particularly on the application side, but there are many areas of considerable gaps and weakness, particularly on the infrastructure and policy side, and these need to be addressed if Pakistan must proactively seek a future for itself in this fast-moving space of opportunities.

Anx- C

COMPILED DATA OF GOVERNMENT POLICY, DEPARTMENTS, UNIVERSITIES, AND PRIVATE ASSOCIATIONS WORKING ON CYBERTECHNOLOGY

Govt Policy	Objectives of the Government Policy	Universities CYBER SECURITY	Government departments dealing with Cyber Security		Private sector on Cyber Security
			Name of the Departments	Initiatives of the Departmentson Cyber Security	Name of the Company/organization
National Cyber Security Policy 2021	**Policy Vision:** The vision is for Pakistan to have 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. **Objectives:** • To establish governance and institutional framework for a secure cyber ecosystem. • To enhance the security of national information systems and infrastructure. • To create a protection and information-sharing mechanism at all tiers capable of monitoring, detecting, protecting and responding against threats to national ICT/ CII infrastructures. • To protect National Critical Information Infrastructure by mandating national security standards	COMSATS Institute of Information Technology, Islamabad **DEPARTMENT Computer Science**	Ministry of Information Technology and Telecommunication(MOITT)	High Impact Skills Boot Camp (MOITT): CDWP Approved 05.04.2021	Nextbridge
		Air University, Islamabad **DEPARTMENT** Cyber Security	National Telecommunication and Information Technology Security Board (NTISB).	Cyber Security for Digital Pakistan (NTISB) DDWP Approved 31.03.2021	Sybrid Pvt Ltd
		National University of Computer and Emerging Sciences, Islamabad **DEPARTMENT Fast School Of Computing**	National Information Technology Board (NITB)	President Initiative for Cyber Efficient Parliament (NITB) DDWP Approved27-05-2021	PanaceaLogics
		Quaid-i-Azam University, Islamabad **DEPARTMENT** Department of Electronics	Ministry of Information Technology and Telecommunication(MOITT)	High Impact Skills Boot Camp (MOITT): CDWP Approved 05.04.2021	10Pearls
		Bahria University, Islamabad	National Telecommunication and Information Technology	Cyber Security for Digital Pakistan	Genesis IT Lab

	and processes related to the design, acquisition, development, use, and operation of 13. information systems. • To create an information assurance framework of audits and compliance for all entities in both public and private sectors. • To ensure the integrity of ICT products, systems, and services by establishing a mechanism of testing, screening, forensics, and accreditation. • To protect the online privacy of the citizens by provisioning the required support and system to all the concerned institutions and organizations National Cyber Security Policy 2021 7 that are dealing with citizens' data-related matters be more equipped and able to render their services, accordingly. • To develop public-private partnerships and collaborative mechanisms through technical and operational cooperation. • To create a country-wide culture of cybersecurity	**DEPARTMENT** Leadership and Professional Development Center	Security Board (NTISB).	(NTISB) DDWP Approved 31.03.2021	
		University of Engineering and Technology, Taxila **DEPARTMENT** Department of Computer Science	National Information Technology Board (NITB)	President Initiative for Cyber Efficient Parliament (NITB) DDWP Approved27-05-2021	Zaytrics Ltd
		Sir Syed University of Engineering and Technology **DEPARTMENT** Department of Cyber Security	Ministry of Information Technology and Telecommunication(MOITT)	High Impact Skills Boot Camp (MOITT): CDWP Approved 05.04.2021	Codeaza Technologies
		University of Management and Technology, Lahore **DEPARTMENT** School of Systems and Technology	National Telecommunication and Information Technology Security Board (NTISB).	Cyber Security for Digital Pakistan (NTISB) DDWP Approved 31.03.2021	Multinet Pakistan
		Ghulam Ishaq Khan Institute of Engineering Sciences and Technology **DEPARTMENT** Computer Sciences and Engineering	National Information Technology Board (NITB)	President Initiative for Cyber Efficient Parliament (NITB) DDWP Approved27-05-2021	Tier3 Cyber Security
		Riphah International University, Islamabad **DEPARTMENT** Riphah Institute			Trillium Information Security Systems

	awareness through mass communication and education programs. • To train skilled cybersecurity professionals through capacity building, skill development, and training programs. • To encourage and support indigenization and development of cybersecurity solutions through R&D Programs involving both public and private sectors. • To provide a framework on national-global cooperation and collaborations on Cyber Security. • To Identify and process legislative and regulatory actions under the mandates of relevant stakeholders assigned in the policy. • Risks related to Cyber Security need to be managed continuously. Encourage adoption of a risk-based approach to cybersecurity through frameworks including those for regulation, assurance, threat management, and incident management.	of Systems Engineering			
					Mozzine Technologies
					Delta Tech Cyber Security Company
					SNSKIES Pvt Ltd
					Arbisoft Islamabad
					Lahore Based
					NEXLINX
					Systems Limited
					NETSOL Technologies
					InvoZone


NATIONAL DEFENCE UNIVERSITY
PAKISTAN

ISSRA
INSTITUTE FOR STRATEGIC STUDIES, RESEARCH & ANALYSIS

National Defence University
Sector E-9, Islamabad Pakistan

www.ndu.edu.pk