Center for Security, Strategy
and Policy Research

Supercomputers & Decision Advantage:

A Peculiar Arms Race between Pakistan and India

NUCLEAR FELLLOWSHIP
PUBLICATION

THE
UNIVERSITY OF
LAHORE

Author

Palwasha Khan is a CSSPR Nuclear Scholars Fellow of the 2021 cohort. Palwasha has an MPhil in Strategic Studies from the National Defense University (NDU), Islamabad, with her dissertation focusing on nuclear signaling patterns in South Asia. She has secured a certificate of merit in academic excellence from NDU in MSc. Strategic and Nuclear Studies. Her areas of interest are nuclear deterrence, strategic stability, and nuclear security.

© The Center for Security, Strategy and Policy Research 2021

The opinions expressed in this publication are those of the author and do not necessarily reflect the views of CSSPR or UOL.

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical including photocopying, recording or any information storage or retrieval system, without the prior written permission of the copyright holder.

Please direct all enquiries to the publishers. All imagery in this report is licensed under Creative Commons 2.0 from Unsplash.com, with thanks to all the photographers.

CSSPR

The Centre for Security, Strategy and Policy Research (CSSPR) is an autonomous policy research center housed in the University of Lahore (UOL), Lahore. It aims at generating research on issues relating to contemporary security and strategic aspects that affect Pakistan's domestic security environment and its international relations with other countries of the world. The Center aims to generate research-driven and nuanced discourses on how best to address security and strategic challenges that deny Pakistan the opportunity and ability to play its role as a responsible seventh Nuclear Weapon State in the world.

The Center conducts research, publishes, and holds conferences on a broad range of regional and international security, strategic, peace and conflict issues. Through this Center, we aim to establish national, regional and international linkages and collaborate with universities, think tanks, research institutes and eminent scholars from around the world, enabling national and international scholars and our students to use CSSPR's platform to deliberate upon issues that carry a global impact.

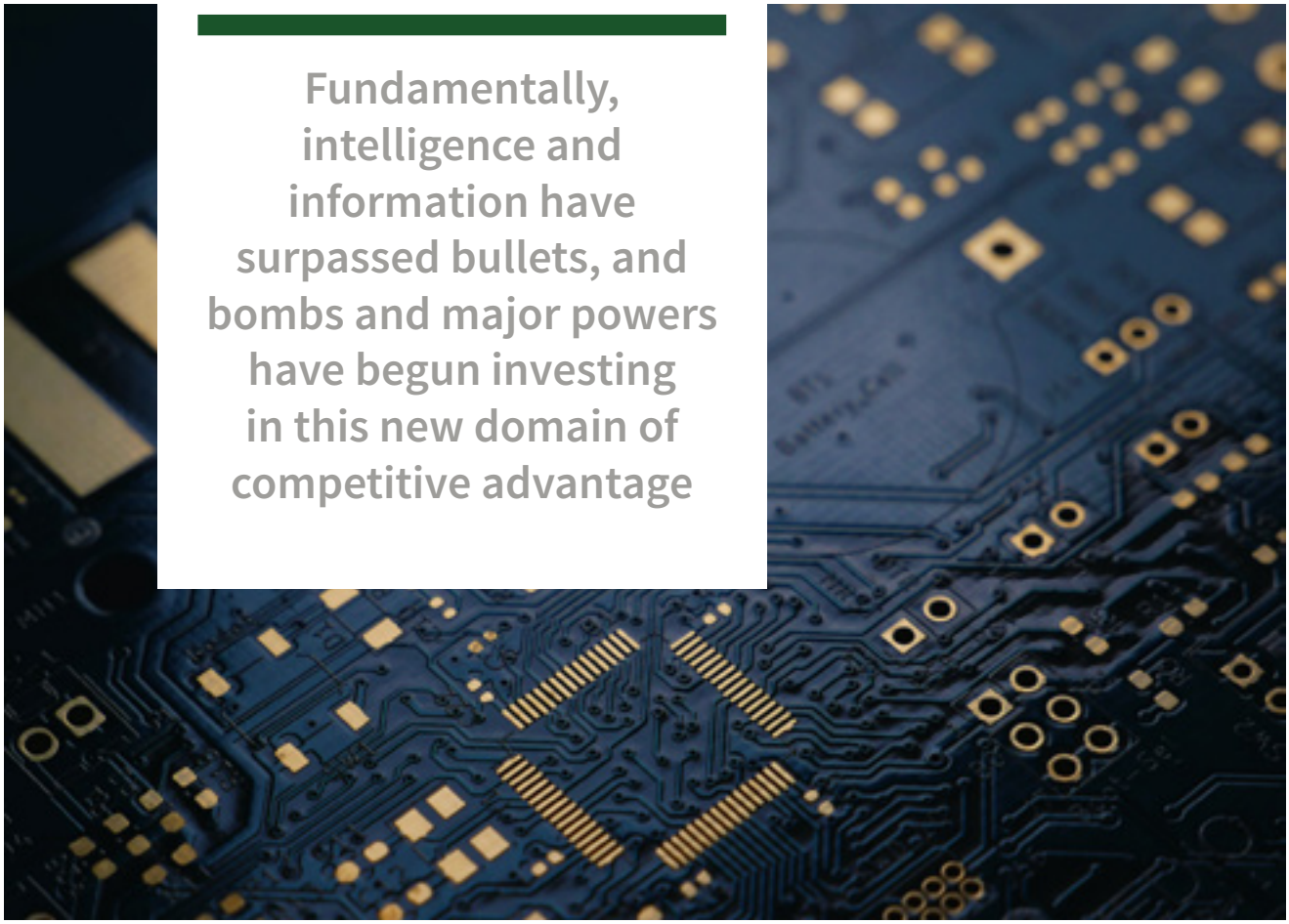
Center for Security, Strategy and Policy Research (CSSPR)
1-Km Defence Road
Lahore
Email: csspr@siss.uol.edu.pk
www.csspr.uol.edu.pk

University of Lahore (UOL)
1-Km Defence Road
Lahore
Email: info@uol.edu.pk
T: +92 423 2233888
www.uol.edu.pk

Supercomputers and Decision Advantage: A Peculiar Arms Race between Pakistan and India

Traditionally, a modernized military was one that had acquired enormous stockpiles of sophisticated equipment and technologies that enhanced its warfighting capabilities. However contemporary trends privilege the use of a stable internet connection and software to cripple entire defense organizations of the adversaries. The world has already started working extensively on Artificial Intelligence (AI), to fight an unseen, inexpensive yet very devastating war. While world powers move to induct supercomputing, quantum computing, and cloud computing to augment their capacities to manage and process information, they have also started testing these technologies to see how they work. From social media platforms to backdoor accesses to applications and software, data has become a key element in warfare. Fundamentally, intelligence and information have surpassed bullets and bombs, and major powers have begun investing in this new domain of competitive advantage and warfare. Close to home, New Delhi, too, took advantage of this paradigm shift and constituted the Defense Artificial Intelligence Council (DAIC) to work on its most robust arm: Defense Artificial Intelligence Project Agency (DAIPA).

As India hails success of its supercomputer PARAM Siddhi-AI, it causes concerns for the future of warfare in South Asia. Supercomputing, merged with Artificial Intelligence (AI) would mean that not only would Indian forces be able to take decisions more quickly but also would be able to manage information from its adversaries to plan and execute preemptive countermeasures more effectively. The Centre for Development of Advanced Computing (C-DAC), along with DAIPA, gives India an advantage in sophisticated warfighting and conduct of operations. As Unmanned Aerial Vehicles (UAVs) and other emerging technologies make their way into arsenals of both Pakistan and India, having an advantage over Pakistan allows India to transform warfighting strategies much quicker than Pakistan could counter. Battlefield management during crises and conflicts would be transformed as India would be able to effectively maneuver the fog of war and cause tactical or operational latency, a strategy that tilts scales of war in its favor. High Performance Computing (HPC) not only allows India to manage data and information more effectively



but also technologies like Pratyush and Mihir supercomputers can be used as dual-use platforms for information processing.

Decision advantage, AI with HPC, and a consistent hack-probe strategy would be the key consideration for Indian strategists once India is able to rationalize geospatial intelligence sharing with its strategic partners. This effectively allows India superior scaling and mapping techniques, which are critical to conducting successful preemptive/surgical operations. This is a prerequisite in cyberwarfare and cybersecurity as information processing through HPCs allows better securitization by accelerating decision making and calculating potential vulnerable factors. Induction and investment in such technologies by New Delhi through combining C-DAC, DAIPA, and DAIC implies that India might divert its civilian supercomputing systems for military learning so that it can be improved upon. Pakistan would have to follow suit if it aims to neutralize the possible Indian supremacy. Cybersecurity is not just about hacking your adversary's websites or stealing confidential data. It is about winning a war before the stage is even set by achieving supremacy in decision-making. Though Pakistan entered the realm of supercomputing close to India's forays , it has not been able to achieve the 'Pratyush and Mihir benchmark' in terms of computing performance. The difference is significant and with India investing heavily in associated technologies like AI platforms, cloud

Cybersecurity is not just about hacking your adversary's websites or stealing confidential data. It is about winning a war before the stage is even set by achieving supremacy in decision making

computing, software management, and cryptography, Pakistan cannot afford to lag behind in this competition.

Pakistan would have to develop interconnected and interdependent organizations and institutions alongside its cyber command. Artificial Intelligence, Machine Learning, supercomputing, and cloud computing are not things that can be compacted in a cyber command, as that would complicate its processes. Establishing relevant organizations for all such supplementary services would allow Pakistan to achieve accelerated learning that is crucial against New Delhi's DAIC. Academic institutions dedicated to such learning need to be established to revive Pakistan's knowledge base on HPCs and supercomputing. A similar set of organizations also need to be set up for developing indigenous learning on cloud computing and blockchain learning. Learning from the architecture of C-DAC, Pakistan can utilize Defense Science and Technology Organization (DESTO) and institute new Research and Development platforms to achieve parity of learning with its longstanding adversary. Cybersecurity architecture plays a vital role in contemporary warfare, but it requires sustainable cultivation of knowledge, research and development, and institutions to test its efficacy. India is progressing in supercomputing and fast-paced data processing and is doing so by engaging its platforms in civilian domains. This not only minimizes risks that might emerge in the military domain but also allows sufficient technological support to future projects that will be a core component of DAIPA.

The future of warfare, conflicts, and crises between Pakistan and India will be different in terms of strategies and machines that are employed to implement them. They will be unique in the sense that non-kinetic engagements will be structured to inflict strategic damage and compellence will take a whole new meaning once decision-making is AI-regulated. For this, India is currently ahead of the game and Pakistan might be under a 'technology gap' which needs to be filled. Recent hack-probes are just a start, what lies ahead requires thorough preparation in advance. The world has not yet laid down any rules or guidelines on how cyberspace competitiveness will be regulated nor is there any international mechanism to separate attributable and non-attributable activities to prevent crises. Pakistan and India are experiencing their own technological Cold War, one where Pakistan has sufficient ground to cover. India has significantly invested in emerging technologies by not only incubating it at the national level but also by using its diaspora by focusing on companies and institutions that deal with emerging technologies. Such investments are now venturing into more complex domains of quantum computing and with DAIC leading this domain, India will seek out a militarized or even a weaponized version of such investments. For Pakistan, this acceleration is an early warning to not only predict the trajectory of this tech-race but also to broaden its own horizon about this emerging competition.