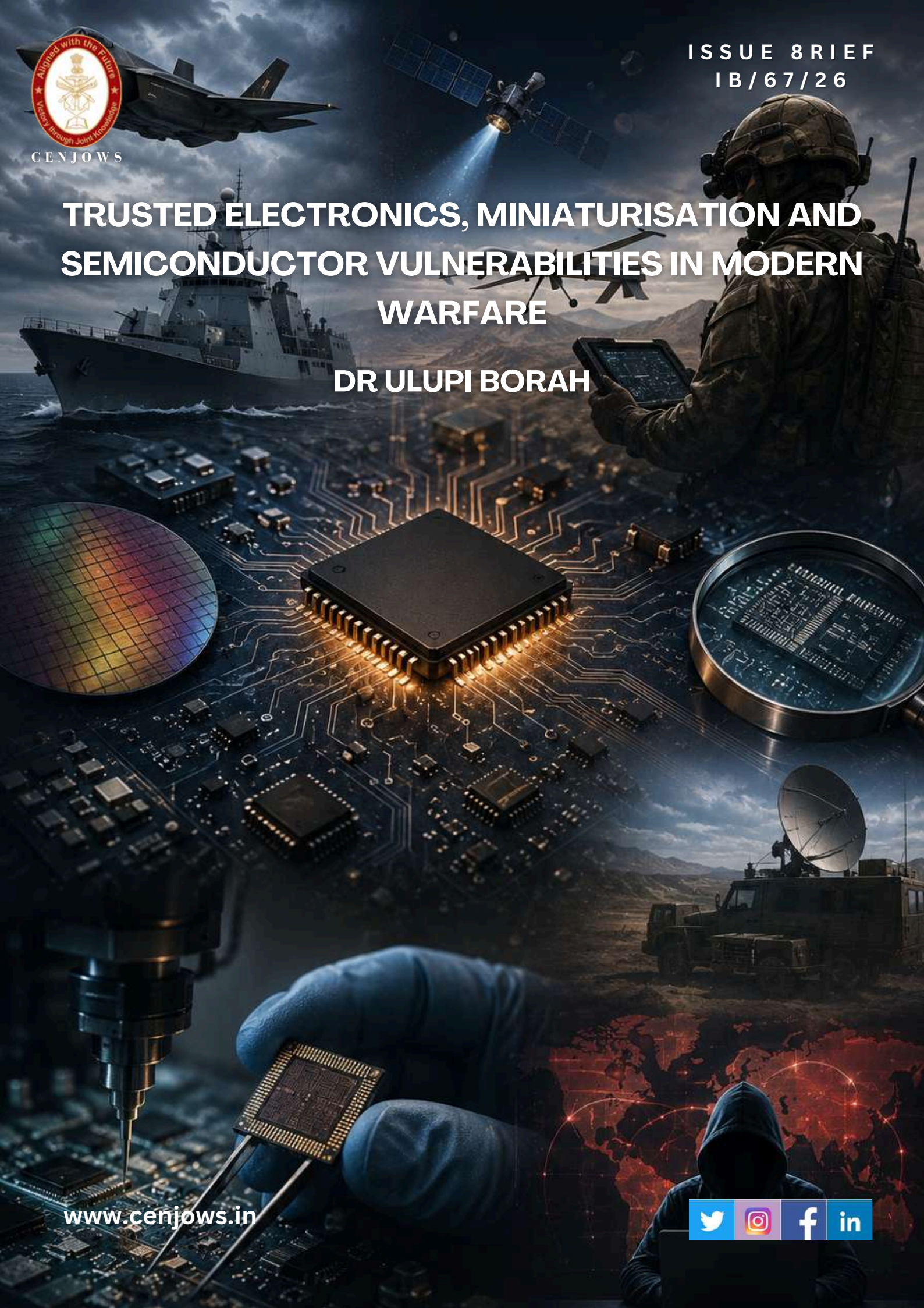

ISSUE 8RIEF
IB/67/26

TRUSTED ELECTRONICS, MINIATURISATION AND SEMICONDUCTOR VULNERABILITIES IN MODERN WARFARE

DR ULUPI BORAH

www.cenjows.in

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

Trusted Electronics, Miniaturisation and Semiconductor Vulnerabilities in Modern Warfare

Dr Ulupi Borah is a distinguished fellow at CENJOWS

Abstract

Modern warfare is increasingly decided not by firepower alone, but by the integrity of the electronics that underpin every weapons system, platform, and command network. Semiconductors today drive everything, from missile guidance and battlefield communications to autonomous drones and satellite intelligence. The armed forces of the 21st century run on silicon as much as they run on strategy. Yet the very supply chains that deliver this capability globally are fragmented, commercially driven, and geopolitically contested. A chip designed in America, fabricated in Taiwan, packaged in Malaysia, and integrated in India carries with it layers of trust assumptions that modern adversaries are actively working to exploit. This growing dependence on advanced semiconductors, sourced beyond the control of any single nation has introduced a new class of strategic vulnerabilities that are as consequential as they are invisible.

This article examines what it means for military electronics to be genuinely "trusted" in an era of globalised semiconductor supply chains and how relentless miniaturisation has simultaneously enhanced battlefield capability while multiplying the vectors through which adversaries can compromise critical hardware. It further highlights whether existing detection, assurance, and policy frameworks are adequate to

address vulnerabilities that are systemic, state-sponsored, and often undetectable through conventional means.

Introduction

The semiconductor chip has quietly become the defining variable in modern military power. From the guidance logic of a precision missile to the signal processor of an airborne radar, from the on-board controller of a satellite to the cryptographic module securing a battlefield network, every decisive military capability today rests on a foundation of silicon. If oil was once black gold, chips are now digital diamonds.

What makes this dependence acutely dangerous for India is its current structure. Over 70 percent of defence-grade semiconductors are sourced from geopolitically sensitive regions, Taiwan, South Korea, and China, creating supply chain vulnerabilities that no amount of tactical ingenuity can entirely offset. Export control regimes such as International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR**),** at a stroke, deny Indian defence platforms access to critical components for electronic warfare, signals intelligence, and Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems. Meanwhile, China's semiconductor investment, exceeding one hundred and fifty billion dollars, continues to widen a technology gap that is narrowing India's window to respond.

Yet the problem goes far beyond the supply chain alone. As transistors have shrunk down to just a handful of nanometres, whole new categories of risk have come into being. Radiation effects that used to be a concern only for satellites and other space-based electronics now show up in systems operating at ground level. Hardware security flaws, Trojan circuits, tampered intellectual property, and counterfeit parts making their way into the supply chain are threats whose sophistication is outpacing our ability to even detect them. An adversary no longer has to destroy a system outright; quietly compromising the chip inside it can achieve just as much, if not more.

This chapter highlights the three connected imperatives: building trusted electronics with verifiable provenance, achieving miniaturisation that expands operational capability without compromising reliability, and systematically closing the

vulnerabilities that India's dependence on foreign semiconductors has embedded within its warfighting architecture.

Trusted Electronics: The Foundation of Military Reliability

Trust in military electronics extends beyond performance and reliability; it concerns the assurance that a semiconductor component will function exactly as intended without hidden vulnerabilities, unauthorised modifications or malicious code. Unlike software, which can be updated, patched or replaced after deployment, hardware vulnerabilities become embedded within the physical architecture of the device and are often impossible to remove without replacing the entire component. This distinction between hardware and software trust has become increasingly important for modern defence systems that rely heavily on processors and memory devices.[1]

A critical aspect of trust is provenance, the ability to establish where a semiconductor was designed, fabricated, packaged, assembled and tested. The semiconductor value chain spans multiple countries and organisations, involving design houses, foundries, packaging facilities, testing centres and system integrators. Each stage represents a potential point of compromise, making complete traceability essential for defence applications. DRDO's hardware-security framework emphasises trusted sourcing, component screening and integrity verification throughout the lifecycle of military electronics, while the SCL highlights the complexity of the semiconductor value chain from design and fabrication to testing, packaging and system integration.[2]

The trust challenge is further complicated by the highly globalised nature of semiconductor supply chains. Rear Admiral D.S. Pathania, Director General, Weapons and Electronics Systems Engineering Establishment (WESEE), notes that a substantial proportion of defence-grade semiconductors originate from geopolitically sensitive regions such as Taiwan, South Korea and China, creating supply-chain vulnerabilities and operational risks. Dependence on single-source suppliers for critical components used in Active Electronically Scanned Array (AESA) radars, sonar systems, submarines and guided munitions creates strategic chokepoints that may be exploited during periods of geopolitical tension. Export-control mechanisms and technology-denial regimes add another layer of uncertainty for countries dependent on imported defence electronics.[3]

For many defence platforms, what matters is not just whether a component works correctly but whether it can actually be trusted. A commercial-off-the-shelf (COTS) component might be "known good" in the sense that it clears performance and reliability tests, but that alone does not make it "trusted". That label only applies once its origin, manufacturing history, and supply-chain integrity have been independently verified. The United States has tackled this through trusted-foundry programmes run under the Defence Microelectronics Activity (DMEA), but India currently has no equivalent defence-specific trusted semiconductor ecosystem of its own. DRDO's analysis also points to the need for dedicated validation, verification, and authentication mechanisms, including secure boot procedures and digital signatures.[4]

An equally serious concern is the possibility of hardware Trojans and embedded backdoors within procured devices, firmware, and hardware systems. These can sit hidden without any visible trace during standard testing, only surfacing once activated at a later stage.[5] Such modifications may be introduced during design, fabrication, packaging or assembly and can remain dormant until activated under specific conditions. Once triggered, they may leak sensitive information, alter performance parameters, degrade system effectiveness or disable critical functions. Unlike conventional malware, hardware Trojans operate beneath the software layer and are therefore extremely difficult to detect using traditional cybersecurity measures.[6]

Counterfeit semiconductors represent another significant threat to trusted electronics. The complexity of global supply chains and the widespread use of third-party suppliers create opportunities for counterfeit or recycled components to enter defence procurement channels. These components may initially appear functional but often exhibit reduced reliability, degraded performance and uncertain security characteristics. Detecting counterfeit devices requires extensive testing and verification procedures, including electrical characterisation, X-ray inspection, decapsulation and destructive analysis. However, such methods are costly, time-consuming and difficult to implement across large inventories. Consequently, trust in military electronics increasingly depends not only on indigenous manufacturing but also on robust verification, authentication and lifecycle assurance mechanisms.[7]

Viewed collectively, these challenges demonstrate that trusted electronics is not solely a manufacturing issue but a comprehensive assurance problem spanning design,

fabrication, testing, packaging, deployment and sustainment. For India, achieving genuine semiconductor self-reliance in defence will therefore require more than fabrication capability alone.

The Physics and Engineering of Miniaturisation

The semiconductor industry's relentless pursuit of node shrinkage (reducing the size of transistors on a chip) is not merely a commercial imperative; it is increasingly a military one. The journey from 800nm to 45nm technology nodes has enabled an extraordinary increase in computing power by packing far more transistors into a much smaller area.[8] Looking ahead, the 2030 horizon targets approximately 2 trillion transistors on a single chip operating at speeds of up to 50 GHz. Semiconductor miniaturisation has made it possible to integrate greater computing power into smaller and lighter devices, a capability that is critical for modern military systems. However, achieving such miniaturisation requires highly sophisticated manufacturing processes that only a few countries currently possess.[9]

For defence applications, this semiconductor miniaturisation is reflected in the growing adoption of System-on-Chip (SoC) technology, where multiple computing functions are integrated onto a single chip, and System-in-Package (SiP) technology, where several chips are combined into one compact package. A notable example is the Mixed-Signal System-on-Chip (SoC), which integrates computing, data processing, encryption, memory and security functions onto a single semiconductor chip measuring only 10mm by 15mm. By combining multiple functions that would traditionally require several separate components, the chip demonstrates how miniaturisation can significantly reduce the size, weight and complexity of military electronic systems.[10]

The Miniaturisation-Vulnerability Paradox

While miniaturisation delivers significant operational advantages, it also introduces new vulnerabilities. Radiation susceptibility stands out as one of the most significant challenges tied to advanced semiconductor technologies. As transistors keep shrinking, the electrical charge needed to store and process information keeps dropping along with them. As a result, even tiny amounts of radiation can throw off normal operation by flipping the stored value in a memory cell, a phenomenon known

as a Single Event Upset (SEU). Notably, these radiation-induced disruptions are no longer limited to satellites and spacecraft. They can now occur at ground level in advanced semiconductor nodes too, leaving military systems such as missile guidance computers and command-and-control processors increasingly exposed. This also threatens the reliability of critical military systems that must operate in harsh environments, including space, high-altitude terrain, deserts and other extreme climatic conditions.[11]

India's Miniaturisation Gap: Deficits in IP

India possesses approximately 400-700 semiconductor patents in defence-related domains, compared with more than 100,000 patents in the United States and over 150,000 in China. India possesses "precision IP" rather than "scale IP". In other words, India has demonstrated excellence in specific niche technologies, such as Gallium Nitride (GaN) radar systems, but lacks the large-scale intellectual property ecosystem enjoyed by major semiconductor powers. The challenge extends beyond manufacturing capability. A useful way to understand this progression is through the "Make to Own" model. In this framework, ‘Make in India’ refers to assembling products, 'Design in India' to developing indigenous technologies, 'Patent in India' to protecting innovations, and 'Own in India' to exercising long-term control over critical technologies. While India has made considerable progress in assembly and design capabilities, ownership of patents and core technologies remains relatively limited.[12]

Semiconductor Vulnerabilities in the Military Context and Threat Actors

The semiconductor threat landscape in modern warfare is not a single attack vector but a layered ecosystem of vulnerabilities spanning design, fabrication, supply chain, and deployment. At the hardware system design phase, the challenge lies in screening basic components for authenticity and verifying that intelligent components, including microcontrollers and processors, originate from trusted sources. At the design and verification phase, IP trust must be enforced through Electronic Design Automation (EDA)-based validation, and without specialised testing schemes, malicious logic inserted at the IP vendor or foundry stage remains undetectable through conventional functional testing. At the deployment phase, originality and integrity must be continuously re-established using boot sequence verification, checksums, digital

signatures, and increasingly, machine learning models capable of flagging anomalous hardware behaviour in the field.[13]

Hardware Trojans represent the most strategically consequential threat in this taxonomy. Hardware Trojans can find their way into a chip at various points along the semiconductor supply chain. They might be inserted during the design phase, through the software tools used to develop the chip, during manufacturing at the fabrication facility, or even at the testing and verification stage. Because of this, a malicious function or hidden backdoor can sit undetected inside a chip until it's triggered at some later point.[14]

Strategic sectors run into a number of hurdles when sourcing semiconductor components, lengthy testing and certification processes, difficulty replacing parts that have gone obsolete, and a growing risk of counterfeit or unauthorised components slipping into the supply chain. To tackle these concerns, the Semiconductor Laboratory (SCL) has built chip verification capabilities that rely on advanced imaging and inspection techniques to examine semiconductor devices and confirm both their authenticity and their construction.[15]

Geopolitical concentration elevates all of these risks to a systemic level. As discussed earlier, more than 70 percent of defence-grade semiconductors are sourced from Taiwan, South Korea and China. This creates a significant strategic vulnerability. An adversary may not need to directly target Indian military platforms to disrupt their functioning. Instead, compromising or disrupting the semiconductor supply chain at the manufacturing stage could produce the same effect while making it much harder to identify the source of the interference. The single-point-of-failure in EUV lithography, concentrated entirely in ASML, means that any conflict scenario involving the Netherlands or its logistics chain could freeze advanced node production globally.

Detection, Assurance, Mitigation, Policy and Future Outlook

There are several strategies for detection, assurance and mitigation policy frameworks for future preparedness in trusted military electronics. Some of them are discussed below:

- **Design-for-Trust and Hardware Assurance Techniques.** These techniques serve as the first line of defence against semiconductor compromise. One way to strengthen chip security is to split the manufacturing process across multiple facilities rather than producing the entire chip in one place. Additional security measures can also be layered in to conceal the more critical parts of the design. This means no single manufacturer ends up with full knowledge of how the chip actually functions, cutting down the risk of tampering or of malicious features being slipped in. Modern chips incorporate security features such as Physical Unclonable Functions (PUFs), unique digital fingerprints for chips and True Random Number Generators (TRNGs), tools that generate unpredictable random numbers for security. These support secure boot, which ensures that a device starts only with trusted software, and authentication chains that verify the identity of a device or user help to protect systems from unauthorised access and tampering. In addition, formal verification, which is rigorous testing to ensure a chip behaves exactly as intended, is used to confirm that the final design accurately reflects its original specifications and does not contain hidden errors or malicious modifications.

- **Supply Chain Security** is about knowing exactly where every component comes from and making sure it stays trustworthy throughout its journey, from the semiconductor wafer stage all the way to the final weapon system. Approved Vendor Lists (AVLs), backed by supplier audits and independent testing laboratories, help keep counterfeit and grey-market components out of defence systems. Newer technologies such as blockchain-based provenance tracking and digital twins create secure, tamper-proof records of a component's manufacturing, testing, and integration history. On top of this, bonded storage, tamper-evident packaging, and strict chain-of-custody protocols add an extra layer of physical security, helping reduce the risk of components being altered, replaced, or intercepted along the way.

- **Domestic Trusted Foundry Capability**. The most enduring strategic solution is building a trusted foundry at home. India's semiconductor push through ISM, DRDO's chip design programmes, and investments by Tata and Micron could be shaped into dedicated defence electronics vertical, mirroring the US DoD's

Trusted Foundry programme run through the DMEA. DMEA is the agency responsible for providing trusted microelectronics solutions and services to the US military. It is worth noting that most military electronics do not actually need cutting-edge nodes; mature processes in the 28 nm to 90 nm range cover the overwhelming majority of defence applications, which makes this a realistic target without having to chase TSMC-level technology. Sovereign packaging facilities add another layer of insulation from geopolitical chokepoints. The United Kingdom, Israel, and South Korea illustrate the strategic value of indigenous semiconductor capabilities, and their experiences show that even modest domestic production can meaningfully strengthen security, resilience, and technological self-reliance.

- **Policy, Partnerships, and the Future of Trusted Electronics.** Policy and international partnerships are essential to building a trusted electronics ecosystem. The US CHIPS Act and the EU Chips Act offer useful models that India could adapt through DAP reforms and a dedicated 'Trusted Electronics Policy'. Frameworks such as the Quad Semiconductor Supply Chain Initiative, NATO's defence innovation ecosystem, and Five Eyes hardware assurance mechanisms could help India strengthen its own standards and supply chain security. Looking further ahead, quantum computing, AI-generated chip designs, and neuromorphic computing will bring new security challenges of their own. Trust and security, therefore, need to be built into every stage of the semiconductor lifecycle, making trusted electronics a core element of India's national security strategy.

Conclusion

In modern warfare, the most dangerous vulnerabilities are not always visible on the battlefield; they are etched into silicon. As military systems grow inseparably dependent on semiconductors, the integrity of hardware has become as strategically vital as the platforms it powers. Miniaturisation amplifies this reality; the smaller and more capable a chip becomes, the harder it is to inspect, verify, and trust.

No software-layer defence can fully compensate for compromised hardware beneath it. The response must therefore be structural, spanning design philosophy, supply

chain governance, and sovereign fabrication capability. For India, this is not merely a technological challenge but a test of strategic seriousness. A nation cannot credibly pursue defence autonomy while remaining dependent on foreign foundries of uncertain alignment for the semiconductors at the heart of its weapon systems.

Trusted electronics is not a niche engineering concern; it is a foundational pillar of national security. Until it is treated as such in policy, procurement, and industrial strategy, the vulnerabilities documented in this article would remain not hypothetical risks but quiet, waiting liabilities.

ENDNOTES

[1] Jindal Mohan ". Hardware Security Products: Chipspirit Technologies Pvt Ltd", Presentation delivered at the "02nd Workshop on Energizing Semiconductor Ecosystem for Defence Applications," hosted by CENJOWS & HQ IDS, YouTube video, accessed April 19, 2026, URL: https://www.youtube.com/live/k-HtmRoH3u8

[2] *P Balasubramanian, "Resilient Computational resources for Defence Applications: Past, Present and Future - A Researcher's Perspective",* Presentation delivered at the "02nd Workshop on Energizing Semiconductor Ecosystem for Defence Applications," hosted by CENJOWS & HQ IDS, YouTube video, accessed April 19, 2026, URL: https://www.youtube.com/live/k-HtmRoH3u8

[3] DS Pathania, "Whole Nation Approach for Achieving Self-Reliance in Semiconductors", Presentation delivered at the "02nd Workshop on Energizing Semiconductor Ecosystem for Defence Applications," hosted by CENJOWS & HQ IDS, YouTube video, accessed April 19, 2026, URL: https://www.youtube.com/live/k-HtmRoH3u8

[4] *P Balasubramanian, "Resilient Computational resources for Defence Applications: Past, Present and Future - A Researcher's Perspective",* Presentation delivered at the "02nd Workshop on Energizing Semiconductor Ecosystem for Defence Applications," hosted by CENJOWS & HQ IDS, YouTube video, accessed April 19, 2026, URL: https://www.youtube.com/live/k-HtmRoH3u8

[5] Kwame Nyako et al., "Building Trust in Microelectronics: A Comprehensive Review of Current Techniques and Adoption Challenges," *Electronics* 12, no. 22 (2023): 4618, https://doi.org/10.3390/electronics12224618

[6] Jindal Mohan,"Hardware Security Products: Chipspirit Technologies Pvt Ltd", Presentation delivered at the "02nd Workshop on Energizing Semiconductor Ecosystem for Defence Applications," hosted by CENJOWS & HQ IDS, YouTube video, accessed April 19, 2026, URL: https://www.youtube.com/live/k-HtmRoH3u8

[7] P Balasubramanian, "Resilient Computational resources for Defence Applications: Past, Present and Future - A Researcher's Perspective", Presentation delivered at the "02nd Workshop on Energizing Semiconductor Ecosystem for Defence Applications," hosted by CENJOWS & HQ IDS, YouTube video, accessed April 19, 2026, URL: https://www.youtube.com/live/k-HtmRoH3u8

[8] Kamaljeet Singh, "*Challenges & Relevance of the self-reliance in Microelectronics & SCL Achievements*", Presentation delivered at the "02nd Workshop on Energizing Semiconductor Ecosystem for Defence Applications," hosted by CENJOWS & HQ IDS, YouTube video, accessed April 19, 2026, URL: https://www.youtube.com/live/k-HtmRoH3u8

[9] Kamaljeet Singh, "*Challenges & Relevance of the self-reliance in Microelectronics & SCL Achievements*", Presentation delivered at the "02nd Workshop on Energizing Semiconductor Ecosystem for Defence Applications," hosted by CENJOWS & HQ IDS, YouTube video, accessed April 19, 2026, URL: https://www.youtube.com/live/k-HtmRoH3u8

[10] Ibid

[11] P Balasubramanian, "Resilient Computational resources for Defence Applications: Past, Present and Future - A Researcher's Perspective", Presentation delivered at the "02nd Workshop on Energizing Semiconductor Ecosystem for Defence Applications," hosted by CENJOWS & HQ IDS, YouTube video, accessed April 19, 2026, URL: https://www.youtube.com/live/k-HtmRoH3u8

[12] Lalit Ambastha, "Patent to Platform", Presentation delivered at the "02nd Workshop on Energizing Semiconductor Ecosystem for Defence Applications," hosted by CENJOWS & HQ IDS, YouTube video, accessed April 19, 2026, URL: https://www.youtube.com/live/k-HtmRoH3u8

[13] P Balasubramanian, "Resilient Computational resources for Defence Applications: Past, Present and Future - A Researcher's Perspective", Presentation delivered at the "02nd Workshop on Energizing Semiconductor Ecosystem for Defence Applications," hosted by

CENJOWS & HQ IDS, YouTube video, accessed April 19, 2026, URL: https://www.youtube.com/live/k-HtmRoH3u8

[14] Ibid

[15] Kamaljeet Singh, "*Challenges & Relevance of the self-reliance in Microelectronics & SCL Achievements*", Presentation delivered at the "02nd Workshop on Energizing Semiconductor Ecosystem for Defence Applications," hosted by CENJOWS & HQ IDS, YouTube video, accessed April 19, 2026, URL: https://www.youtube.com/live/k-HtmRoH3u8