

Defence Technology Security Architecture in India

Comparative Analysis and Strategic Roadmap

*Khyati Singh**

Three convergent trends, that is, the weaponisation of technology, the escalating great power competition and the ongoing necessity for nations to attain strategic autonomy through ‘self-reliance’, have resulted in the current strategic landscape. Due to this, the security of defence technology has become an issue of utmost importance for national security policy. Furthermore, contemporary conflict now takes place in the non-kinetic realm rather than the specified physical area. Therefore, protection of advanced weapon systems, critical infrastructure and proprietary research is as crucial as governing the sovereign territory.

This commentary advances the central argument that India’s defence technology security challenge is not one of capacity, intent or partnership, but of institutional fragmentation and legal insufficiency. Unlike the United States (US) and the United Kingdom (UK), which anchor defence technology protection in unified authorities backed by enforceable statutory regimes, India relies on a dispersed constellation of agencies and procedural manuals. This institutional–legal gap undermines technology protection, constrains high-end defence collaboration and, ultimately, weakens India’s pursuit of strategic autonomy.

* Ms Khyati Singh is a Research Analyst at the Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA), New Delhi, India.

The commentary, therefore, argues for the creation of a unified, legally empowered National Technology Security Authority, supported by a standalone strategic technology law, as a prerequisite for India's defence modernisation and credible international partnerships. The effective security of defence technology involves a holistic, comprehensive and integrated framework that secures the entire cycle of critical military components. This cycle includes intellectual property rights (IPR), critical research, assured security during technology procurement and transfer, proliferation control, along with preventing espionage.

Few countries, like the US and the UK, have served as global benchmarks for securing defence technology. These nations had the first-mover advantage, which has allowed them to define the contours of framework and implement it over time. Their example serves as a case study for India, allowing us to identify systemic gaps in institutional frameworks and policy designs. The following sections unpack the practices and protocols of the aforementioned developed nations with respect to securing defence technology.

INTEGRATED SECURITY ARCHITECTURE OF THE US

The US follows a 'whole-of-government' approach, which is multi-layered and inducts specialised agencies with clearly defined and legally binding mandates operating within a powerful regulatory framework. It is designed not only to prevent technology leak but also work as an active instrument of national power.

The central idea is to avoid centralisation of responsibility and distribute it amongst various organisations, thereby creating a comprehensive security net. This includes:

- *Department of Defense* (DoD): It serves as the apex body responsible for providing military forces for national security. It sets the tone for policy direction and oversees the entire security ecosystem, which includes defence industries and military breaches.¹
- *Defense Technology Security Administration* (DTSA): The DTSA is the primary agency under DoD that is in charge of developing and implementing policies related to defence technology security, including transfer of technology, defence goods and services. The main agenda of the DTSA is to identify and mitigate risks associated with any such transfers, keeping the technological edge of the US intact.² Though it was born during the peak of the Cold War to forestall technology transfer to the Soviet Union, it has rapidly adapted to the needs of modern era

and evolved accordingly. Therefore, it now focuses on facilitating secure sharing of technology with critical partners.

- *Defense Counterintelligence and Security Agency (DCSA)*: This agency is often referred to as ‘America’s Gatekeeper’ as it is meant to protect both physical and human elements of the defence architecture. It conducts crucial background checks for personnel clearances and looks after the security of approximately 10,000 companies that have been cleared under the defence industrial base (DIB), thereby ensuring that both the people and the facilities involved in dealing with sensitive technologies are trustworthy.³
- *Intelligence Community*: The US intelligence community is a combination of 18 organisations, including the Defense Intelligence Agency (DIA), the National Geospatial-Intelligence Agency (NGA) and the National Security Agency (NSA). The intelligence community supplies crucial information regarding the capabilities and intentions of the adversary, which is then utilised for threat assessments, transfer policies and counter-intelligence efforts.⁴

The regulatory cornerstone of the defence ecosystem includes the following:

1. *International Traffic in Arms Regulations (ITAR)*: It is administrated by the Department of State’s Directorate of Defense Trade Controls (DDTC). These regulations govern the import and export of defence equipment and services which are enlisted in the United States Munitions List (USML). This list is an exhaustive account covering 21 categories of military items, from basic firearms to advanced spacecrafts. It possesses extra-territorial power, that is, despite the items being exported, it still has the rights over regulations and data.⁵
2. *Export Administration Regulations (EAR)*: This is managed by the Department of Commerce’s Bureau of Industry and Security (BIS) and governs ‘dual-use’ technologies. All the items are listed in the Commerce Control List (CCL). This allows them to be entitled to an Export Control Classification Number (ECCN), which decides the conditions and requirement for licensing. The control logic of the EAR is less simple than that of the ITAR as it depends on a combination of technical specification of the item (ECCN), the destination, the end-user and the ultimate end-use. This risk-based practice ensures protection of even commercially accessible technologies which are potentially a threat to national security in a balanced way. The items that are not contained on the CCL are classified as EAR99, which, unless they are being shipped

to an embargoed state or to a prohibited final user, do not need a licence in most cases.⁶

In addition, the US completely understands that modern technology is inseparable from the ambit of digital world. Hence, it has developed a mature, multi-layered network for securing the same.

1. *National Cybersecurity Strategy* (2023): This Biden administration strategy marks a significant shift in the state's approach towards cybersecurity. It aims at rebalancing the burden of security away from small users, and onto the big businesses, which are better positioned to reduce risks. It relies on five pillars: (i) safety and defence of critical infrastructure; (ii) disrupting and dismantling threat actors; (iii) investing in resilient future; (iv) making market forces work towards security resilience; and (v) forging international partnership for shared goals.⁷
2. *National Institute of Standards and Technology (NIST) Cybersecurity Framework* (CSF): The CSF has been developed by the NIST and offers a framework for organisations to manage and bring down cybersecurity risk. Although voluntary in nature, it is widely in use. It organises best practices into five main categories: identify; detect; protect; respond; and recover.⁸
3. *DoD-specific Initiatives*: The DoD Cyber Workforce Framework (DCWF) harmonises the roles, responsibilities and desirable knowledge, skills and abilities (KSAs) of the whole cyber workforce, thus providing a consistent and high standard of expertise.⁹
4. *Cybersecurity Maturity Model Certification* (CMMC): This programme is mandatory in nature and is designed to ensure protection for unclassified information, like the Controlled Unclassified Information (CUI). Strong systemic safety is a requirement for any organisation doing business with the DoD, and the framework directly links security compliance to contract eligibility by guaranteeing that all DoD contractors are audited and certified at a specific cybersecurity level.¹⁰

The system deployed in the US is not merely a collection of a set of scattered policy steps but a highly woven, legally enforceable system. Its efficacy derives from a systematic sequence of reinforcement. Together with the severe criminal and civil penalties embedded in the ITAR and the EAR, the DoD Technology Surveillance Act aims to assist in mitigating the risks that technology transfers have created. As a result, the policy recommendations of the department and its licensing decisions have serious gravitas. At the

same time, the DCSA protects people and physical resources that are part of the DIB through a rigorous vetting and facility clearance programme; and the CMMC framework strengthens the digital base using compulsory certification.

The result of such a function of refinements is a plurality of defence architecture: the technology, in its turn, is put under statutory (ITAR/EAR) control; the staff, to which it is trusted, is thoroughly vetted and authorised (DCSA); and information networks on which it all occurs are also certified and audited (CMMC). Therefore, technology cannot be effectively safeguarded by institutional actions or policy tools alone; rather, institutional actions ought to be supported by clearly defined, strict legislative processes which will authorise the existing agencies as well as compel the entire industry to adhere to the legislation.

COORDINATED APPROACH OF THE UK

The approach of the UK is based on a centralised model operated through its Ministry of Defence (MOD). The country has recently modernised its legal framework, putting a strong emphasis on the domestic defence industry.

1. *Ministry of Defence* (MOD): The MOD serves as the central agency with the onus of implementing the national defence policy. It is also the headquarters of the British Armed Forces, and has a range of specialised units to manage cyberthreats.¹¹
2. *Defence Digital*: This organisation is crucial for the technological advancement of the armed forces and is operated under the MOD. It is primarily responsible for the development and deployment of crucial technology and cyber strategy.¹²
3. *Defence Science and Technology* (DST): This wing gives directions for science and technology in defence, and operates under the MOD's chief scientific advisor. It ensures maximum investment for military advantage and shapes science and technology policies for critical aspects, like cyber and space.¹³

The UK has also worked to reform its legal and strategic framework, succinctly incorporating measures to counter new-age threats.

1. *National Security Act 2023*: The Official Secrets Acts of 1911, 1920 and 1939 were repealed following this major Act. It creates specially designed measures meant to counter state-sponsored adversaries, including protection of critical information and trade secrets, along with assisting

intelligence services. The provisions include hefty penalties, at times reaching up to life imprisonment in serious offences. It also provides intelligence agencies and law enforcement institutions tools required to perform the range of functions.¹⁴

2. *Defence and Security Industrial Strategy* (DSIS): The DSIS (2021) aims to curate better relationship amongst stakeholders, that is, the government, the defence forces and the security industries. Furthermore, realising that domestic industrial capacity is crucial for national security, it commits significant investment to research and development (R&D). It also advocates for increased transparency in the government's functioning, along with taking measures to build confidence amongst industries.¹⁵
3. *UK Strategic Export Controls*: The Export Control Joint Unit (ECJU) manages export control of the UK. It directly controls the export of items included in the UK Strategic Export Control Lists, covering both dual-use goods and military systems. The licence applications are reviewed based on the 'Strategic Export Licensing Criteria', elaborating criteria covering national security and regional stability, along with assessing any potential violation of the international humanitarian law. Moreover, the MOD Form 680 application is mandatory in order to share classified military information beyond the borders.¹⁶

The most distinguished aspect of the UK's approach is its collaborative model that considers industries a crucial partner in the country's security landscape.

1. *Defence Cyber Protection Partnership* (DCPP): This is a joint initiative between the industry partners and the MOD to enhance cybersecurity of the defence supply chain. It serves as a forum for sharing threat information and building common security standards together.¹⁷
2. *Cyber Security Model* (CSM): The DCPP created this architecture to guarantee cybersecurity on the supplier side. It requires certification for all suppliers handling MOD Identifiable Information (a specific data classification in the UK defence sector).¹⁸
3. *Cyber Essentials Scheme* (CES): This is a common cybersecurity measure supported by the government. According to the MOD cybersecurity standards, suppliers who are more vulnerable to cyberattacks must put additional measures in place.¹⁹
4. *Defence Standard 05-138*: This employs a more layered strategy, guaranteeing the bare minimum of security at every level, while also putting strong procedures in place where they are needed.²⁰

The UK's strategy is not focused on top-down rules, instead, it seeks to create an ecosystem that views industries as equal strategic partners through the DCPD and the DSIS. In the context of national security, they are regarded as important stakeholders rather than just suppliers. They are appropriately positioned as essential components for 'long-term capability advantage' in the DSIS framework. Similar to this, the CSM makes use of pre-existing cyber standards and simplifies and eases compliance, especially for small- and medium-sized enterprises, which are crucial for fostering innovation. The idea of shared responsibility encourages industries to voluntarily engage in security architecture.²¹

This paradigm is crucial for India, which is advocating for 'Atmanirbhar Bharat' or self-reliance in defence. It implies that the state ought to advocate for an atmosphere based on the shared responsibility culture, rather than a compliance-driven strategy.

INDIA'S DEFENCE TECHNOLOGY SECURITY ARCHITECTURE

India's defence technology security is ensured by a constellation of bodies with mandates that are, at times, overlapping, loosely defined and not exhaustive to the level of governance that is required in the current ecosystem. The major players in this system include:

1. *Ministry of Defence (MoD)*: It is in charge of the defence policy, resource distribution and overall supervision of the armed forces and allied organisations. However, unlike its counterparts in the UK and the US, it does not have empowered sub-agencies with specific mandate for developing, implementing and ensuring security policy across the entire supply chain.²²
2. *Defence Research and Development Organisation (DRDO)*: The DRDO works as the R&D wing of the MoD. Its primary goal is to develop critical defence technologies and state-of-the-art systems for the armed forces.²³ It has a sub-unit called the Directorate of Information Technology and Cyber Security (DIT&CS), which only ensures security for DRDO's projects and networks.²⁴
3. *Defence Cyber Agency (DCyA)*: The DCyA was established in 2019 with the mission of handling cyberthreats for the Indian Armed Forces. It is majorly concerned with offensive and defensive cyber operations, safeguarding military systems and evolving a joint cyberwarfare understanding. Its scope does not include larger challenges of technology security in industrial partnerships, procurement or technology transfer.²⁵

4. *Indian Computer Emergency Response Team (CERT-In)*: This unit operates under the Ministry of Electronics and Information Technology (MeitY) and serves as the nodal agency for responding to cyber breach incidents and leakages. Despite being a crucial agency for national cybersecurity, it mainly focuses on civilian issues. This often creates a vacuum for military-specific DCyA, which requires far more complex coordination.²⁶

CHALLENGES IN INDIA'S SECURITY STRUCTURE

There are many difficulties with the current institutional structure. There is not a single organisation in India, like the US DTSA, with the knowledge and power to enforce technology security and supervise its appropriate application throughout the public and private sectors, military forces and the MoD. Similar to this, cybersecurity is divided across multiple organisations, such as DCyA, National Critical Information Infrastructure Protection Centre (NCIIPC) and CERT-In, which makes response efforts more difficult and time-consuming in times of national emergency. A region of 'overlapping responsibilities' is produced by this fragmentation. A single cyber command that can expedite authority and action is necessary for India.²⁷

Furthermore, the desire to co-produce and co-develop advanced technologies with different partners that have strict regulations in place frequently makes the endeavour more difficult. For example, to encourage technology cooperation, India has entered into bilateral frameworks with the US, such as the Roadmap for US–India Defence Industrial Cooperation and the US–India Initiative on Critical and Emerging Technology (iCET). One of the requirements under these frameworks is that India fully execute the 'Industrial Security Annex', a crucial agreement allowing firms to share classified technology.

The US administration and its defence industries abide by legal frameworks on technology transfer and sensitive military information. In order to protect it from any diversion or compromise, they majorly partner with nations that have equally robust protection mechanisms in place. The current system of technology protection operational in India, however, is a patchwork of agencies that often have overlapping mandates, and are largely governed by mere policy guidelines rather than strict laws. There is thus a lack of legal guarantees and unified institutional oversight in the country, which is a precondition of many developed states for sharing advanced technologies. This, in fact, becomes both a foreign policy challenge and

a defence modernisation obstacle to fully realise agreements with other nations.²⁸

INDIA'S LEGAL AND REGULATORY LANDSCAPE

India's legal and regulatory framework is a mix of several agencies, procedures and general-purpose laws, clubbed with sector-specific policies, that fall short of effectively providing the comprehensive umbrella required for securing defence systems. This, in turn, creates significant loopholes and vulnerabilities that are exploited by adversaries for their gains. The legal and regulatory mandates are discussed next.

Defence Acquisition Procedure (DAP)

The DAP, which succeeded the Defence Procurement Procedure (DPP) in 2020, serves as the principal document for military procurement in India. It is crucial for creating a hierarchy that pushes for indigenously designed, developed and manufactured (IDDM) equipment to meet the self-reliance goal. It also includes offsets and technology transfers in its mandate.²⁹

Despite the DAP performing a prominent function, it lacks legal standing. It is merely a procedural manual and not a security law. This leaves considerable scope for frequent amendments, creating an environment of 'policy unpredictability', which has often been cited as a deterrent to foreign collaboration. Moreover, breaches of its provisions are matters of administrative action and do not fall under criminal offence, fundamentally weakening its role as a security instrument.

Intellectual Property Rights (IPR)

The IPR laws are often considered the biggest roadblock for the smooth transfer of technology. Indeed, the IPR indicators, including the one published by the US Chamber of Commerce, often give a low ranking to India. They have repeatedly cited challenges in copyright enforcement, trade secret protection and patentability. This perception, whether completely justified or not, often creates a bias amongst foreign firms that are looking at collaboration with India.³⁰

In addition, the domestic IPR framework suffers from enforcement issues, high costs of litigation and delayed legal resolution, thereby affecting small businesses and innovators. The government did try to address these challenges with the National IPR Policy in 2016, along with initiatives like

‘Mission Raksha Gyan Shakti’ to instil the culture of intellectual property (IP) within the defence ecosystem. Still, there remain significant implementation challenges.³¹

The most pertinent issue that remains is regarding the legal ambiguity that surrounds the security of military innovation. The law currently applicable in India empowers the government to revoke patents on broadly defined grounds, like national security, without giving any clear guidelines, transparency or compensation to the parties involved. This can demotivate private players, particularly in R&D, as innovators fear expropriation of their IP without due process. Moreover, the policy of the DRDO to allow the use of its patents by Indian players without any cost or royalty, at times, inadvertently devalues the IP and ends up disincentivising the private industries from investing in their own R&D.

Digital Personal Data Protection (DPDP) Act, 2023

This act serves as the legal document for data privacy in India. It places onus on data fiduciaries to have in place reasonable security safeguards to prevent any data breaches, and also immediately report any incident to the Data Protection Board of India, along with the individuals that are affected, following the breach.³²

However, the Act’s cover of the defence sector is complicated. It majorly focuses on ‘personal data’, which does not adequately cover the sensitive, operational, technical and design data on which the defence technology thrives. Likewise, it allows the government to exempt any of its agencies from the provisions listed in the Act on vaguely defined grounds, like security of the state or maintenance of public order. While being a standard feature of data protection laws across the globe, the loosely defined components often raise concerns regarding the casual bypassing of security protocols.³³

The cumulative outcome of all procedural manuals, IPR and data protection laws, with several exemptions for the state, works more as a legal framework that is obsessed with procedure than security. Despite ardently complying with each of the prescribed mechanisms, the sensitive technology and data of a company may still be vulnerable to theft, compromise and espionage due to overwhelming lacunas. This divide between procedural compliance and actual, stringent security application is the greatest legal challenge in India’s security of defence architecture. The gaps also end up deterring foreign companies from actively engaging with India, while creating ample opportunities for adversaries to exploit them. Hence, fixing

these issues would require a fundamental shift from mere procedural follow-ups to a more stringent security-oriented legal framework that is built on clearly defined, enforceable and acceptable standards.

The preceding comparative analysis demonstrates that effective defence technology security rests on two foundational pillars: institutional centralisation of authority, and legally enforceable control mechanisms. India's current framework lacks both. Fragmented mandates dilute accountability, while the absence of a statutory security regime weakens deterrence, compliance and partner confidence. The following roadmap is, therefore, not a menu of optional reforms, but a sequential strategy designed to close these structural gaps and align India's defence technology governance with international best practices.

ROADMAP FOR SECURING DEFENCE TECHNOLOGY

Institutional Consolidation: Establishing a National Technology Security Authority

To address the problem of fragmented authority and inconsistent enforcement identified in the commentary, India must establish a single, statutory National Technology Security Authority, with the mandate of enforcing and overseeing technology security. In order to cut on approval delays and ministerial silos, it must be formed within the National Security Council Secretariat and must directly report to the National Security Advisor. It can be designed on the lines of the US DTSA, serving as the nodal agency for all inter-agency coordination and policy formulation, thereby directly dealing with the issues of institutional fragmentation.

Its functions should include the role of technical and security review authority, overseeing transfer of technology, co-production and co-development projects under the DAP. Coordination with the Directorate General of Foreign Trade and the Ministry of External Affairs must come under its ambit, along with maintaining a national strategic technology control list. It must have the responsibility of export licensing and managing end-user monitor programme for technology exported from India. In addition, it should oversee national counter-proliferation efforts related to sensitive technologies, as well as act as the single point of contact for all international partners on crucial matters related to security of technology, communication and confidence building.

Legal Foundations: A Standalone Strategic Technology Law

For fixing legal loopholes, a comprehensive, standalone law must be enacted. This law can be dubbed the Bhartiya Strategic Technology Act, with the key purpose of providing unambiguous legal foundation for the aforementioned unified technology security agency. It can be inspired by the legal structure and stringent deterrence penalties prescribed in the US ITAR, or the elaborated threat focused in the UK's National Security Act 2023.

It must create an Indian Munitions List and an Indian Dual-Use List, clearly defining technologies and equipment which are subject to control. It must also prescribe mandatory licensing requirement for any exports, re-exports or transfer of technology, services, critical data to any foreign entity, or to any foreign national within India. Moreover, it must elaborate upon severe civil and criminal penalties for violating the security laws.

Industrial and Cybersecurity Certification of the Defence Supply Chain

To secure the defence industrial base to boost the spirit of 'Atmanirbhar Bharat', an Indian defence supplier certification framework must be created. The government must mandate such certification clubbed with cybersecurity certification. It should be a prerequisite for industries that are willing to be a part of any defence contract that involve sensitive information.

Its formation should be on the grounds of approaches deployed by the US CMMC or the UK's CSM. It should include self-assessment of suppliers that are not in charge of any sensitive data; a high level of certification for those dealing with more nuanced, sensitive and strategic projects; and a third-party audit for industries involved in handling controlled but unclassified information.

Gradation policy for defence design organisation can be considered as well to distinguish the design capacities, quality standards, safety and security policies and mechanisms of micro, small and medium enterprises (MSMEs) and start-ups in the defence sector. Moreover, there must be a validation of indigenous content in IIDM and transfer of technology to bring more transparency in the system.

The MoD and the DRDO must also formulate a policy for spiral development to prevent semi-developed or complex technologies. The user consent may be obtained for enhancing potential employment options and success rate of spiral development projects. For professional screening and quick approval of spiral development initiatives, an independent expert committee of the DRDO, user, academic and domain specialists' representatives may be established, as necessary.

Protecting Knowledge Flows: IPR, Academia and Consulting Firms

There are currently no special provisions in the policies for international consulting firms doing business in India. For consultations, studies, creation of vision statements, roadmaps and other projects, the union government, state government ministries, organisations and other entities frequently hire foreign consulting firms, such as PricewaterhouseCoopers (PwC), Klynveld Peat Marwick Goerdeler (KPMG) and McKinsey, among others. They, thus, have access to private data, aircraft, regulations and vital infrastructure information. The consequences of this data sharing for national security are not sufficiently addressed by the regulations in place. Clear ownership structure disclosure rules, financial transparency standards for parent companies, mandatory background checks for overseas consulting firms and strict measures to stop illegal technology transfer through data access need to be in place.

There is also a substantial amount of research conducted by academic institutions that can be categorised. However, these institutions have little knowledge of IPR. Therefore, it is necessary to set up specialised IPR offices with trained patent lawyers at all universities, as also set up professionally run technology transfer offices, and connect IPR protection with the growth of start-up ecosystems. The IPR courses are required for all technical and research programmes, and university institutions can submit applications for patents more quickly.

Operationalising Compliance: Non-disclosure Agreements, Personnel Vetting and Enforcement

There should be clearly defined confidentiality template for employees in critical roles and specialised units that combine technical experts and law enforcement. There must be a common non-disclosure clause (NDC) template for varying levels of technology sensitivity. The NDC should cover industry, researchers, sub-contractors, vendors, academia, start-ups and affiliated entities. The viability of requiring vital technology NDCs to register online with a designated government entity could also be investigated.

CONCLUSION

This commentary argues that India's defence technology vulnerability stems less from technological inferiority than from institutional and legal fragmentation. India is standing at a critical juncture as it transitions from a middle power to a great power, with an increased role of providing regional

stability. This would be realised with the country becoming a global military power, with strong indigenous base for defence manufacturing. In order to achieve this ambition, India must overhaul the architecture of its defence technology security. The system currently in place is fraught with challenges and suffers from fragmented approach, procedural complications, ill-defined guidelines and redundant mandates. They do not support the complexities of 21st century warfare, and the challenges that come with it. Piecemeal reforms and small tweaks will not support the safety required for creating an indigenous and robust defence ecosystem. It needs a systemic transformation, clearly defined policies, laws with stringent penalties and improved implementation.

NOTES

1. 'Defense Department', *Federal Register*, 1994.
2. 'Defence Technology Security Administration', Office of the Secretary of Defense, US.
3. 'Defense Counterintelligence and Security Agency', US, 2025.
4. 'Members of the IC', Office of the Director of National Intelligence, US, 2025.
5. 'International Traffic in Arms Regulations (ITAR)', America's Seed Fund, 2025.
6. 'An Introduction to the ITAR and EAR', Gan Integrity, 2024.
7. 'The National Cybersecurity Strategy', The White House, March 2023.
8. 'Cybersecurity Framework', NIST, 2025.
9. 'The DoD Cyber Workforce Framework (DCWF)', US Department of War, 2025.
10. 'DoD Defence Industrial Base', Cyber Crime Center, 2025.
11. 'Ministry of Defence', UK, 2025.
12. 'Defence Digital', Ministry of Defence, UK, 2025.
13. 'Defence Science and Technology', *Gov.UK*, 2025.
14. 'National Security Act Factsheet', *Gov.UK*, 2025.
15. 'Defence and Security Industrial Strategy', HM Government.
16. 'UK Export Controls and Licensing', UK Government, 2025.
17. 'UK Government & UK MOD Cyber Security Requirements', GE Aerospace, 2025.
18. Ibid.
19. Ibid.
20. Ibid.
21. 'Defence and Security Industrial Strategy', n. 15.
22. 'Transformation of India's Defence and Internal Security Posture', Press Information Bureau, Government of India, 20 August 2025, available at <https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155066&ModuleId=3®=48&lang=2>.
23. 'DRDO', Ministry of Defence, Government of India.

24. 'Directorate of Information Technology and Cyber Security (DIT&CS)', DRDO, MoD, Government of India.
25. Nikhat Parveen, 'India's Framework for Cyber Security Since 2014 and its Significance for Armed Forces', *International Journal for Multidisciplinary Research*, Vol. 6, No. 4, August 2024, available at <https://www.ijfmr.com/papers/2024/4/26605.pdf>.
26. 'CERT IN', Ministry of Electronics and Information Technology (MeitY), Government of India.
27. Dhruva Jaishankar, 'The Indigenisation of India's Defence Industry', Brookings India, August 2019, available at <https://www.brookings.edu/articles/the-indigenisation-of-indias-defence-industry/>.
28. Ibid.
29. 'Understanding the Defence Procurement Procedure: A Comprehensive Guide for Stakeholders', *Tender18*, 2025, available at <https://tender18.com/blog-details/Understanding-The-Defence-Procurement-Procedure-A-Comprehensive-Guide-for-Stakeholders>.
30. 'India Country Commercial Guide', International Trade Administration, 12 January 2024.
31. 'Promoting Intellectual Property Rights in Defence', Press Information Bureau, Ministry of Defence, Government of India, 4 February 2019, available at <https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1562585®=48&lang=2>.
32. 'Draft Digital Personal Data Protection Rules, 2025 Receive 6,915 Inputs from Citizens and Stakeholders', Press Information Bureau, Ministry of Electronics and Information Technology (MeitY), 26 July 2025, available at https://www.dpo-india.com/Resources/privacy_laws_in_India/Draft-Digital-Personal-Data-Protection-Rules,20256,915-Inputs-Citizens-Stakeholders.pdf.
33. 'The Digital Personal Data Protection Bill, 2023', *PRS Legislative Research*, 12 August 2025, available at <https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023>.