Countering rogue drones

FICCI

EY
Building a better working world

About the report

FICCI, in collaboration with EY has developed this paper as a deep-dive into the Counter Unmanned Aircraft Systems (C-UAS), covering its various facets. Considering the status of UAS policy and operations in India, the paper emphasizes the need for counter-UAV systems to be deployed. It contains an overview of the fundamentals of C-UAS and various sub-technologies. Further, the paper discusses the challenges with respect to policy, market and operations for law enforcement agencies, organizations and the government before they leverage C-UAS and its associated technologies for the safety and security against dangers arising from UAS used with maligned intentions. The paper concludes by charting out the next steps based on the secondary research conducted and proposes recommendations on next steps in the Indian context.

Table of contents

I. Executive summary 04

II. The need for counter-UAS technology: Gold rush in the wild west 06

A. The potential drone applications 07

B. Possible misuses of UAS 07

C. Counter-UAS solutions: A US$1.2 billion market by 2025 08

D. What are the risks from UAVs? 09

III. Counter-UAS in the Indian context: The law of the land 12

A. Knowing the landscape: Overview of UAS operating framework in India 13

B. C-UAS in the Indian context 14

1. Land of the People – India's demographic situation 14

2. Increasing air traffic: Growth in aviation sector 15

3. Latent population of unregistered drones 15

4. Civil Aviation Regulations 2.0 15

IV. Strategies for defense: Tools of trade for the marshals 16

A. Types of cUAS systems 17

1. Detection and tracking C-UAS 17

2. Interdiction 18

V. Use cases: Current approaches: Enabling our marshals 20

A. How are military personnel using anti-drone systems? 21

B. Anti-drone systems in our backyard: Police operations 21

C. Event specific measures 22

D. Measures taken by private entities 22

E. Challenges 23

VI. Path ahead in India: Taming the wild west 24

A. Empowering the homeland security forces 25

B. Risk and asset profiling 25

C. Boost to allocation for indigenous R&D and Make in India 25

D. Liquidating the threat of legacy UAVs 25

E. Citizen participation 25

I Executive summary

The gold rush of the 19th century brought together people from all economic strata. It brought investors, opportunists, miners, entrepreneurs, law enforcers and law breakers together to a single location. There was a law of the land but implementation of that law was a challenge. The modern drone industry portrays a similar lay of the land. There is a gold mine of potential applications and business opportunities. This has attracted participants from multiple industries to provide business solutions. We have the law of the land in terms of regulations for drone (UAS) ownership and operations, we also have the entrepreneurs and large firms - the law abiders and law breakers – the entities who wish to misuse technology.

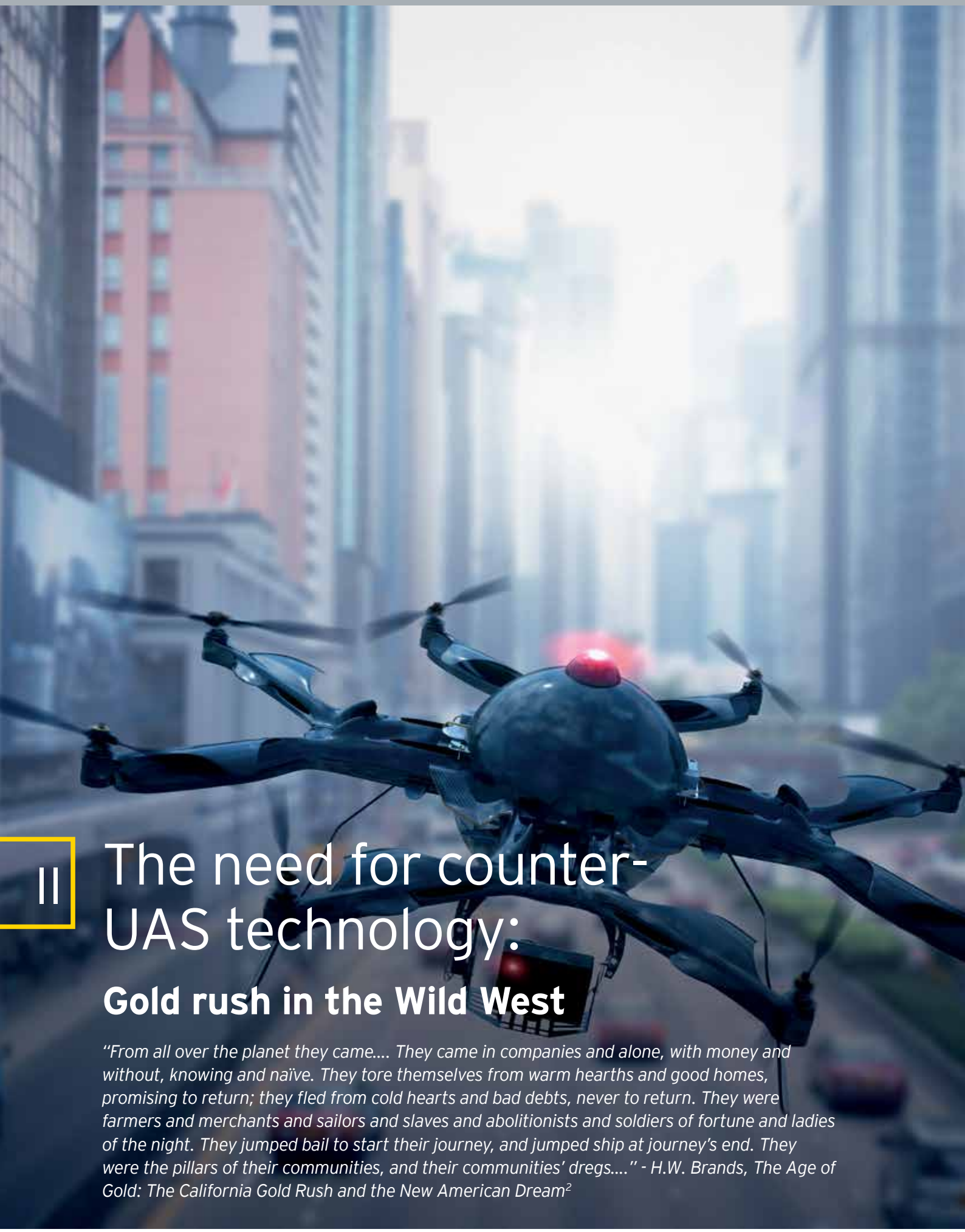
This report aims to capture the "yin–yang" of UAS technology and counter-UAS (cUAS) technology. The report explores the need for counter-UAS technologies given the current explosion in the UAS or drone applications in the civilian space. The market for drone applications is expected to accelerate to US$100 billion by 2020 [1]. As the market booms, there are multiple instances of misuse of technology by adverse entities which has heightened the sense of risk and security disruption from drones. UAS technology and applications typically pose three types of risks – privacy risk, security risk and penetration risks. The need to mitigate risk has given rise to adoption of counter-UAS technologies.

Section 3 of the report explores the need for counter-UAS technologies in the Indian context. It is important to understand the current drone regulatory framework to get a sense of the need for counter-UAS technologies. The section provides the key features of the Indian Civil Aviation Regulations (CAR), e.g., the permits required, policy of "No Permission No Take off" and the Digital Sky platform. The need of the hour here is to ensure enforcement of the regulations. The need for counter-UAS in the Indian context is further enhanced given the demographic intensity, increasing air traffic and the evolution of CAR in India.

Sections 4 and 5 of the report identifies the "tools of the trade" to help entities like law enforcement agencies to identify, interdict and mitigate the impact of rogue drone usage in civilian situations along with a few real-world use cases of applications of counter-UAS technologies, including some of the challenges in the current defense technologies.

Section 6 of the report encapsulates the way ahead in adopting the counter-UAS technologies in India and the way ahead for mitigate and manage the risks from rogue UAS applications. During the report the terms UAS, UAVs and drones are using synonymously and interchangeably and so are the terms counter UAS, counter-UAV and anti-drone technologies.

[1] Drones: Reporting for Work – Goldman Sachs - https://www.goldmansachs.com/insights/technology-driving-innovation/drones/



II

The need for counter-UAS technology:

Gold rush in the Wild West

"From all over the planet they came.... They came in companies and alone, with money and without, knowing and naïve. They tore themselves from warm hearths and good homes, promising to return; they fled from cold hearts and bad debts, never to return. They were farmers and merchants and sailors and slaves and abolitionists and soldiers of fortune and ladies of the night. They jumped bail to start their journey, and jumped ship at journey's end. They were the pillars of their communities, and their communities' dregs...." - H.W. Brands, The Age of Gold: The California Gold Rush and the New American Dream[2]

A. The potential drone applications

It is a Gold rush…

The first commercial drone was demonstrated at the Consumer Electronics Show (CES) 2010[3]. Since then, drones or unmanned aircraft systems (UAS) have demonstrated significant potential in the commercial applications across industries. Today, drones are being used for different use cases across construction, agriculture, oil and gas and law enforcement, amongst others. Trials are being performed to try out drones for applications like pizza delivery, medical supplies and emergency assistance. Over the past nine years drone applications have significantly grown in terms of the depth of capabilities and applications. Experts estimate that the drone market would show a hockey stick growth to reach US$100 billion by 2020[4]. The applications of drones are further fueled by the adoption of technologies like cloud computing, Artificial Intelligence and Machine Learning. Globally, the total addressable market for drone applications is expected to be US$11 billion for construction and US$6 billion for agriculture alone.

The trajectory in India is expected to be in line with the global trends. UAS have seen an exponential growth in demand in India over the past five years. Primarily being used by law enforcement agencies (LEAs), UAS have seen more usage by other PSUs (Public Sector Undertakings) and government agencies. A specialized force constituted for the purpose of specialist response to a threatening disaster situation or disaster has been using UAS for locating victims of natural disasters, the national railway system in India is using UAS for inspecting and tracking progress of its mega projects and the largest state-owned natural gas processing and distributing company has implemented UAS for surveillance of its network of gas transmission pipelines. Adoption of UAS is increasing in India and it is projected that the value of industry and market would be around US$885.7 million[5].

B. Possible misuses of UAS

…But requires marshalling

Every technology has the potential for misuse and this is applicable to drones as well. In 2013, Germany's Pirate Party flew a small multirotor drone in close proximity to Angela Merkel at an open-air rally, leading many to speculate about the ease with which a drone could attack an otherwise highly secured area[6].

This incident highlighted the ease with which drones can disrupt our current way of working. Since then there have been multiple scenarios where drones have disrupted the security and privacy and aided in penetration where otherwise difficult. Given below are a few examples:

- In August 2018, a failed assassination attempt against Venezuelan President Nicolás Maduro was mounted with explosive-armed drones in Caracas during a televised national event. The drones detonated explosives above the audience which led to a few injuries.[7]
- In July 2018, in the UAE, terrorists claimed to have sent an armed drone to attack the international airport in Abu Dhabi, the capital of the United Arab Emirates. While the authorities deny the claims, the Caracas incident provides sufficient evidence that this can be done.[8]
- In January 2015, a drone crashed onto the White House lawn after its operator lost control, prompting concerns that the US President's residence may be vulnerable.[9]
- Also in 2015, a man protesting Japan's nuclear policy dropped a drone carrying radioactive sand from the Fukushima nuclear disaster onto the Prime Minister's office premises, though the amount of radiation was minimal.[10]

Apart from the security risks posed by drones, there have been consistent concerns of privacy regarding the video, images and data collected by drones. In some cases, there have been flagrant violations of privacy which have been enabled by using drones. Some of the instances are as below:

- In November 2016, a husband used drones mounted with cameras to catch his wife cheating— and then posted evidence of the alleged affair online.[11]
- In March 2017, a woman in Washington spotted a drone outside her window and tried to shoot it down initially using stones and then using a gun.[12]

There have been instances where drones can be used for penetrating secure areas and capture data through remote signals which can be received through drones with camera payloads. Some examples of using drones for penetrating systems are:

- Leaking data through LED lights in hard drives which is read through light sensitive remote operating systems (drones, say outside a window)[13].
- Research shows that one can leverage the light sensitivity of a multi-function printer and use different light sources to infiltrate and place malware in a system. These attacks can be carried out through laser on drones or a laser on a tripod from a remote system.[14]

[2] From the Book: The Age of Gold: The California Gold Rush and the New American Dream by H.W. Brands

[3] CES: iPhone-controlled drone unveiled at tech show curtain-raiser - https://www.theguardian.com/technology/2010/jan/06/ces-iphone-controlled-drone

[4] Drones: Reporting for Work – Goldman Sachs - https://www.goldmansachs.com/insights/technology-driving-innovation/drones/

[5] ET - India fastest growing market for unmanned aerial vehicles - https://economictimes.indiatimes.com/news/defence/india-fastest-growing-market-for-unmanned-aerial-vehicles/articleshow/63466658.cms

[6] Gettinger, Dan, "A Pirate Drone in Germany," Center for the Study of the Drone, September 19, 2013- https://dronecenter.bard.edu/tag/pirate-party/

[7] Terrorism by joystick - https://www.post-gazette.com/opinion/2018/08/07/Terrorism-by-joystick/stories/201808070022

[8] Terrorism by joystick - https://www.post-gazette.com/opinion/2018/08/07/Terrorism-by-joystick/stories/201808070022

[9] With drone attacks, the era of joystick terrorism appears to have arrived - https://www.scmp.com/news/world/article/2158380/analysis-drone-attacks-prove-era-joystick-terrorism-has-arrived-and-world

[10] Man arrested for landing 'radioactive' drone on Japanese Prime Minister's roof- https://www.independent.co.uk/news/world/asia/man-arrested-for-landing-radioactive-drone-on-japanese-prime-ministers-roof-10203517.html

[11] Husband uses drone to catch cheating wife - https://nypost.com/2016/11/16/husband-uses-drone-to-catch-cheating-wife/

[12] Not in my backyard - https://www.dailymail.co.uk/news/article-4283486/Woman-grabs-gun-shoots-nosy-neighbour-s-drone.html

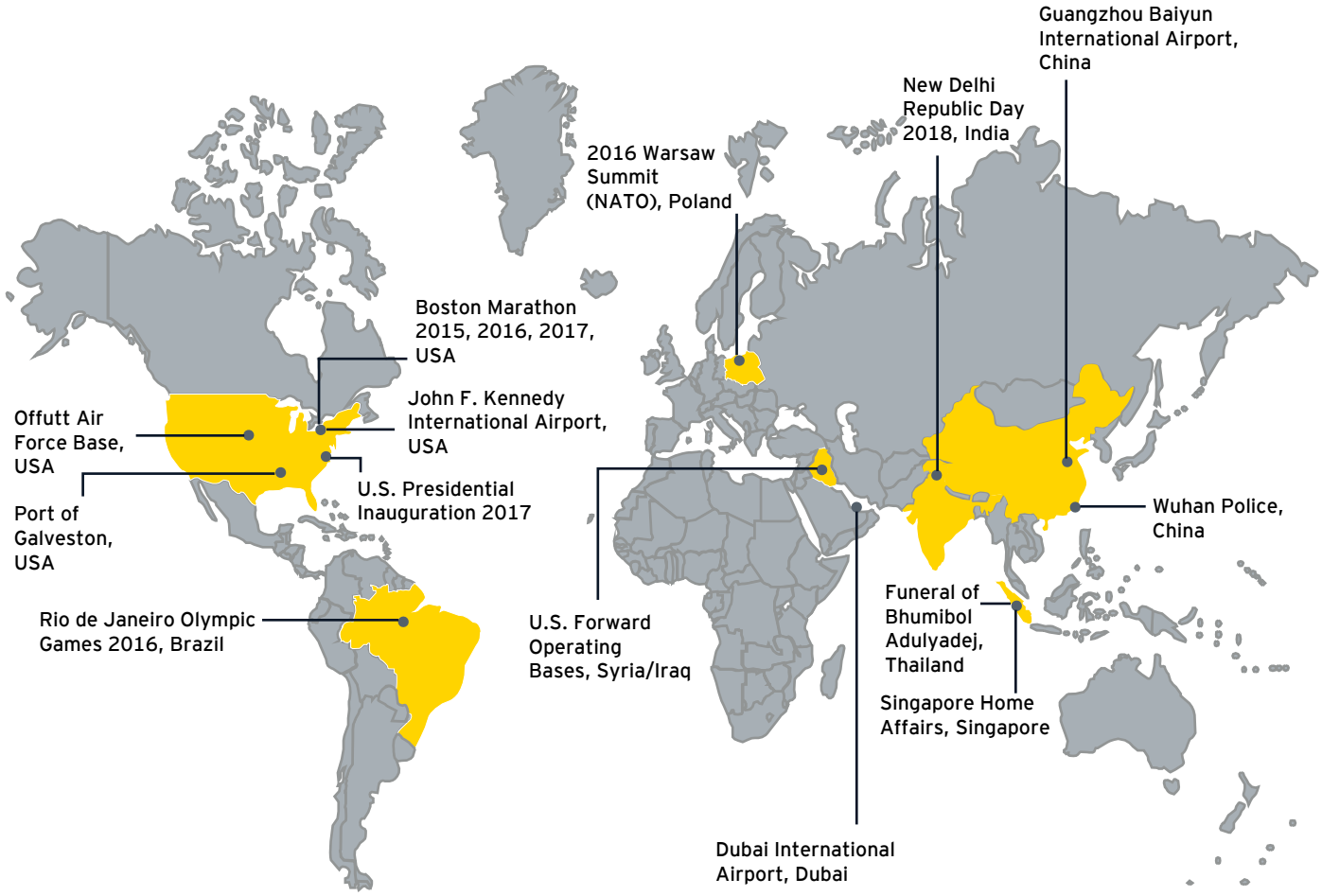
[13] LED-it-GO: Leaking (a lot of) Data from Air-Gapped Computers - https://arxiv.org/abs/1702.06715

[14] Xerox Day Vulnerability - https://ieeexplore.ieee.org/document/8409461

C. Counter-UAS solutions: A US$1.2 billion market by 2025[15]

As indicated above, when used with malicious intent, drones have the potential to be disruptive and destructive. The potential advantages of drone use cases and applications far outweigh the approach to outright ban the import, manufacture or usage of drones. In view of this, multiple governments have taken cognizance of the risk and have started investing in counter-drone technologies. These have been used in high profile events to ensure security and prevent penetration. Some examples of using anti-drone or counter-UAS technologies are as follows:

Figure 1: Examples of using counter-UAS technologies[16]



As indicted in the figure above, cUAS technologies have been used across multiple countries to prevent the risk of disruption or destruction caused by drones. Given the applications of cUAS technologies, experts forecast that this market is expected to initially spurt and then grow as fast as the drone market is expected to grow. A report by Transparency Market Research forecasts the global anti-drone market to expand at an impressive 19.9% CAGR between 2017 and 2025 and attain a valuation of US$1.2 billion by 2025. The market was evaluated to be worth US$215 million in 2016.[17]

[15] PNR Newswire – Transparency market Research - https://www.prnewswire.com/news-releases/anti-drone-market-to-reach-us1-204-9-million-by-2025--thanks-to-growing-border-safety-concerns-noted-tmr-300834533.html

[16] Counter Drone Systems – Centre for Study of Drones - https://dronecenter.bard.edu/publications/counter-drone-systems/

[17] Global Anti-Drone Market Research Report - https://www.marketresearchfuture.com/reports/anti-drone-market-6460

D. What are the risks from UAVs?

As seen above, the cUAS markets help detect, identify and neutralize different types of risks from drone usage. Broadly, drone usage could pose a privacy, security or a penetration risk based on usage. An effective cUAS technology would need to timely identify and address these risks. The different risks are detailed out in the figure below:[18]

1	**Privacy risk** Risk of using drones to capture, process information which compromises the privacy of others	**Spying and tracking:** Using drones to obtain video, images and track movements **Surveillance:** Using drone images and other payload data to enable spatial reconstruction and reconnaissance
2	**Security risk** Risk of using drones to engage in physical attacks, move contraband to compromise the security of a location	**Physical attacks:** Leveraging drones to drop harmful or explosive payload or damage via collision **Smuggling:** Using drone payloads to move contraband or transfer material into sensitive zones
3	**Penetration risk** Use drones to increase the chances of gathering information or controlling a system	**Data leakage:** Leveraging drones' spatial accessibility to enable penetration to cause data leakage **Control and spoof:** Using drone payloads to remotely control and spoof unsecured devices

- **Spying and tracking to create a privacy risk:** Most drones today have first person view (FPV) along with HD resolution capabilities. This helps drone operators to remotely observe and track movements of objects of interest. This is crucial as:
  - It eliminates the need for a malicious operator to be close to the drone or target by allowing the operator to maneuver the drone from far away to a target that is also far away from the operator's location
  - It can be secured using encryption
  - It supports HD resolution that enable the attacker to obtain high quality pictures and close-ups (by using the video camera's zooming capabilities)

This has created threat which invade individual privacy for example, spying on a cheating spouse[19], capturing intimate images[20], tracking celebrities[21]

- **Surveillance to create privacy risk:** Malicious entities can also use drones to survey and conduct reconnaissance of sensitive installations. Apart from video survey and monitoring, images obtained from drones can be used for 3D spatial reconstructions of installations with sufficient details to perform visual reconnaissance. There have been instances of burglars monitoring movements of occupants to target empty houses for theft in residences.[22]
- **Physical attacks to create security risk:** Drones can also be used for conducting physical attacks. Today, using drones for physical attacks is not relegated to the realm of military scenarios. As seen in the examples in the previous section, drones have been used to conduct physical attacks on civilian targets. Apart from threat to world leaders, drones can also be used to orchestrate disruption on civilian infrastructure[23], aircraft[24] and others.

[18] SoK - Security and Privacy in the Age of Drones: Threats, Challenges, Solution Mechanisms, and Scientific Gaps by Ben Nassi, Asaf Shabtai, Ryusuke Masuoka, Yuval Elovici: https://arxiv.org/abs/1903.05155

[19] N. Y. Post, "Husband uses drone to catch cheating wife," https://nypost.com/2016/11/16/husband-uses-drone-to-catch-cheating-wife/

[20] kiro7, "Woman terrified by drone outside her window," - http://www.kiro7.com/news/woman-terrified-drone-outside-her-window/81721261

[21] N. Washington, "Virginia woman shoots down drone near actor Robert Duvalls home," -http://www.nbcwashington.com/news/local/Virginia-Woman-Shoots-Down-Drone-Near-Actor-Robert-Duvalls-Home-391423411.html

[22] The Telegraph, "Burglars use drone helicopters to target homes," - https://www.telegraph.co.uk/news/uknews/crime/11613568/Burglars-use-drone-helicopters-to-identify-targe-homes.html

[23] Reuters, "Greenpeace crashes superman-shaped drone into French nuclear plant," - https://www.reuters.com/article/us-france-nuclear-greenpeace/greenpeace-crashes-superman-shaped-drone-into-french-nuclear-plant-idUSKBN1JT1JM

[24] Forbes, "British army used Israeli tech to end Gatwick airport Christmas drone chaos," - https://www.forbes.com/sites/annatobin/2018/12/26/british-army-used-israeli-tech-to-end-gatwick-airport-xmas-drone-chaos/#75b0793f6e6e

- **Smuggling using drones create security risk:** Drones have started to be used for smuggling contraband across borders[25], dropping prohibited items in sensitive areas like prisons[26] and other restricted places[27]. These events have the capacity to enable security risks as they circumvent the traditional security processes.
- **Data leakage by increasing penetration risks:** We have seen in the previous examples how drones can be used to create covert channels of communication using peripherals like multi-function printers and LEDs in hard drives. These examples show that drones along with the requisite payloads can be used for increasing penetration risks to cause data leakage.
- **Control and spoofing create penetration risks:** Drones also be used for spoofing WiFi routers and mobile devices by leveraging right payloads to enable the ability to control and track different devices in the environment[28].

Given the above nature of risks, counter-UAS technologies become important to mitigate, manage and monitor these perils. Considering the drone platform and the number of different payloads which can be used on the platform, cUAS technologies have seen extensive investment and development. The competition between "hackers" who leverage technology to expose different types of risks, with or without malicious intent, which require preparation. While the above examples are largely global, they are possible in the Indian context and can be risks which require preparation. In fact, in India the cUAS technologies have greater importance as explained in the next section.

[25] L. A. Times, "Two plead guilty in border drug smuggling by drone," - http://www.latimes.com/local/california/la-me-drone-drugs-20150813-story.html

[26] BBC, "Big rise in drone jail smuggling incidents," - http://www.bbc.com/news/uk-35641453

[27] D. Trends, "Smugglers used aerial drones to sneak $80 million in iphones into china," - https://www.digitaltrends.com/mobile/iphone-smugglers-aerial-drones-hong-kong-china/

[28] J. Chesaux, "Wireless access point spoofing and mobile devices geolocation using swarms of flying robots," Master optional semester Project, Spring, 2014 - https://smavnet.epfl.ch/pdfs/CheseauxJonathan_SemesterProject.pdf

III

Counter-UAS in the Indian context:

The law of the land

A. Knowing the landscape: Overview of UAS operating framework in India

The Directorate General of Civil Aviation released the Civil Aviation Regulations (CAR) – Section 3, Series X, Part I – in August 2018[29] to be implemented effective December 2018. This policy document, marked a significant milestone in drone adoption in India, since it sought to regulate and legitimize drone ownership and operations, both of which were not strictly legal at the time.

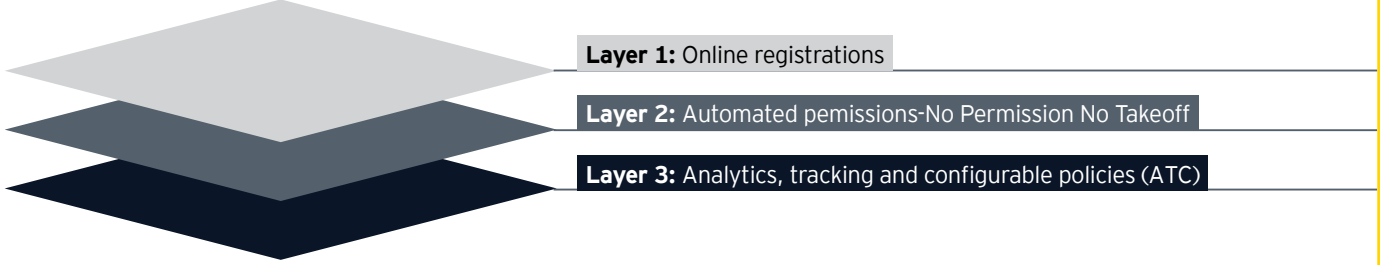
According to the CAR, UAVs are categorized into nano, micro, small, medium and large based on their weight classification. It may be assumed that this classification also reflects the threat or damage potential of these UAVs. Thus, increasingly higher safety related requirements are prescribed in the policy document for each subsequently higher category of UAVs. Even operational accountability goes up progressively as per categorization.

The following table depicts safety and operational accountability comparison of UAV classes as prescribed in the CAR.

	Nano	Micro	Small	Medium	Large
Weight criteria	= or < 250 Gm	> 250 Gm, =<2 Kg	> 2 Kg, =< 25 Kg	> 25 Kg, =< 150 Kg	> 150 Kg
UIN (Unique Identification Number)	No	Yes	Yes	Yes	Yes
UAOP (Unmanned Aerial Operators Permit)	No	No	Yes	Yes	Yes
NPNT	No	Yes	Yes	Yes	Yes
Allowed height (AGL – Above Ground Level)	50 Ft (above 50 ft, not exempt)	200 Ft (above 200 ft, not exempt)	400 Ft	400 Ft	400 Ft
Night operations	No	No	No	No	No
Visual LoS (Line of Sight)	Yes	Yes	Yes	Yes	Yes
Flight plan	No	No	Yes	Yes	Yes
ADC/FIC (Air Defence Clearance/Flight Information Centre)	No	No	Yes	Yes	Yes
Flight path planning	No	Yes	Yes	Yes	Yes
Operation envelope	Indoor and uncontrolled Airspace	Uncontrolled Airspace	Uncontrolled and Controlled Airspace	Uncontrolled and Controlled Airspace	Uncontrolled and Controlled Airspace
Security clearance	No	Yes	Yes	Yes	Yes
Pilot training	No	No	Yes	Yes	Yes

The Civil Aviation Regulation provided for an online registry platform (Digital Sky) for drone ownership and operations, which is key to laying a strong foundation for an effective regulation. The Indian government intends to bring the policy level requirements to execution, with the Digital Sky Platform. This platform will enable all the UAVs, their owners and their operating entities – companies as well as individuals - to register with DGCA.

Complemented by anti Drone technology for highly sensitive areas[30]



[29] DGCA Website - http://dgca.nic.in/cars/D3X-X1.pdf

[30] Graphic courtesy Ispirt - https://www.thequint.com/tech-and-auto/tech-news/digital-sky-india-drone-take-off-platform-all-you-need-to-know

As per the regulation, all UAVs either imported, assembled or manufactured in India will need to get a Unique Identification Number (UIN), provided they meet specific hardware and software requirements based on their weight class. To operate small and above category of UAVs, the operating entities will require to get Unmanned Aerial Operations Permit (UAOP) at an organizational level and would require their operators to be trained by registered flight training organizations (FTOs). The policy also requires that the airspace be segregated into zone classifications at a state level, thus ensuring that the operating risks are mapped to not just aircraft type but also airspace within which such operations are proposed. Further, a minimum set of manufacturing guidelines have been introduced to introduce elements of safety, security and privacy protection. The regulation also highlights that discharging and dropping substances from the drone during flight is not legal.

In effect, the CAR has all the cornerstones for a well-thought and structured framework for mitigating risks through UAS operations in India. Further, India is unique in its regulatory implementation, by means of its No Permission No Take-off (NPNT) policy for UAV operations. Under the process, each proposed UAV flight needs to have a permission token loaded on the UAV autopilot, to enable its take-off. The NPNT framework is proposed to be integrating UAV operating compliance requirements at the auto-pilot hardware and software levels.

B. C-UAS in the Indian context

The CAR framework for UAS in India provides a robust structure to mitigate the different types of risks from rogue drones. While the implementation mechanism is being put in place, it is also important to understand why the cUAS technology is important from an Indian perspective. While CAR provides a framework to define the legality, cUAS provides the array of counter measure options in case the regulation is not being followed. While we will understand the range of counter measure options in the next section, it is important to understand why these options are critical in a diverse and unique country like India, as illustrated below.

1. Land of the people: India's demographic situation

India, as unique as it is in opportunities due to its demographics, is also vulnerable to rogue elements for the same reason. We have more events and opportunities for disruption than any other country in the world where a few thousand people gather at a single place. Even if we were to look beyond hundreds of illegally operated drones filming private social events and weddings, the residual risk to public events is considerably high. Take an example of an event like Kumbh Mela, whose minor or major form occurs every six years. This event takes the crown both on the scale of human gathering and threat perception for the same reason. The latest Ardha Kumbh which was held in January 2019, at Prayagraj also received a terrorist threat[31]. Any disruption (intentioned or otherwise) at such large-scale gatherings by technology enabled rogue elements could do severe damage. For example, in 2015, religious idols strapped to UAVs flew over crowded areas in nine cities[32] for considerable amounts of time. While it was reported that the act was a publicity stunt, the risk to safety of to the gathering, notwithstanding communal overtones, was equally grave as any other ill intended UAV usage. On the military side, a recent aerial transgression and its subsequent neutralization reported[33] along the Gujarat border was carried out using a drone.

From a population perspective, India is by far the country with highest population density (411 persons per square km) as compared to any other country of comparable – (or even a little smaller) size. This makes it vulnerable to maximum collateral damage in wake of an intentional or unintentional UAS related disruption. Drones are controlled over wireless links with a typical span of control over two kilometers. This makes it possible to be controlled from anywhere within a 13 square km. area – an area larger than an Indian city suburb. This makes tracing the drone operator a virtually impossible task. This is true for any operations environment, let alone a densely populated Indian urban area. Moreover, increasing wireless activities by an ever increasing "smart" urban infrastructure to make our cities smart is making electronic wireless tracking a prohibitively operations intensive task for the technologically challenging regulatory and enforcement infrastructure that we have currently..

[31] India TV News Desk (18 January 2019). "Kumbh Mela 2019: ISIS issues threats of chemical attack, NDRF conducts mock drill". India TV.

[32] "Who allowed Hanuman drones to hover over city," The Times of India, September 19, 2016 http://worldpopulationreview.com/countries/countries-by-density/

[33] India Today (26 February 2019). https://www.indiatoday.in/india/video/pakistani-drone-shot-down-in-gujarat-border-this-morning-1465246-2019-02-26

2. Increasing air traffic: Growth in aviation sector

The International Air Transport Association (IATA), in its paper published during the Global Civil aviation summit in January 2019, has predicted that Indian air transport sector will continue to grow at a rapid pace on the back on driving factors like rising living standards, aided by technology advancements, population and demographic factors. To cater to the rising air traffic, the Government of India has been working towards increasing the number of airports. As of March 2019, India has 103 operational airports. India has envisaged increasing the number of operational airports to 190-200 by FY40. Further, the rising demand in the sector has pushed the number of airplanes operating in the sector. As of July 2018, there were nearly 620 aircraft being operated by scheduled airline operators in India. The number of airplanes is expected to grow to 1,100 planes by 2027.[34] Rising number of aircrafts and airports, both point towards increased risk of irresponsible, mistaken or ill intended UAS operations.

3. Latent population of unregistered drones

The most compulsive case for India to implement counter-UAS technologies on an urgent basis is also a result of the CAR framework. According to some estimates,[35] close to 50,000 drones were operating in India prior to policy notification (CAR, 2018) in August 2018. Almost all of these drones are not compliant to the NPNT requirements mandated in CAR. Even though the first official notice banning the use of UAVs in Indian airspace was issued by DGCA, way back in October 2014[36], it was difficult to enforce this ban. Notwithstanding their legalities or otherwise, of manufacture, import or assembly, these drones are currently facing an uncertain future since they would not be compliant to NPNT requirements. Limited ability to monitor flights of this latent population of unregistered drones highlight an immediate risk in operations and the need for cUAS technologies.

4. Civil Aviation Regulations 2.0

During the Civil Aviation Summit in January 2019, the government also released its roadmap[37] for the next wave of regulations for the UAV operations in the country. These set of regulations, aptly named CAR 2.0 are likely to include framework for operating UAVs beyond visual line of sight (BVLOS) autonomously with minimal manual intervention. The UAV operations envelope shall also be expanded to include dedicated "drone corridors" and creation of UAV operations infrastructure like Unmanned Traffic Management (UTM) setup and Droneports. This fillip at the policy level will lead to a significant boost to the UAV traffic and a heightened UAV traffic and will further accentuate the need for not just the presence of C-UAS systems in the country, but also for making the C-UAS sophisticated in its technologies.

[34] https://www.ibef.org/industry/indian-aviation.aspx

[35] https://www.rediff.com/business/report/security-scare-50000-illegal-drones-in-india/20190108.htm

[36] Government of India, Office of the Director General of Civil Aviation, "Public Notice - Use of Unmanned Aerial Vehicle (UAV)/ Unmanned Aircraft Systems (UAS) for Civil Applications," October 7, 2014.

[37] Drone Ecosystem Policy Roadmap, Ministry of Civil Aviation, Government of India. https://www.globalaviationsummit.in/documents/DRONE-ECOSYSTEM-POLICY-ROADMAP.pdf

IV Strategies for Defense

Tools of trade for the marshalls

Traditional methods of protecting the airspace from manned aircrafts have generally proven themselves ineffective against drones. The anti-aircraft radars have been designed to detect large metallic and fast-moving objects. Thus, it is mostly difficult to use radars for detecting drones which are small, slow moving and low-flying.

One of the primary cUAS systems in the first line of defense are the no-fly zones mandated by the regulators. These no-fly zones are typically created by demarcating polygons of GPS coordinates around sensitive locations like landmark sites, critical infrastructure and other high-risk locations from a security standpoint. In the Indian context, the NPNT process and demarcation of green, amber and red zones through the Digital Sky platform is designed to ensure that the UAS are automatically directed back to their home location before entering the fly zones

.

A. Types of C-UAS systems

A complete counter-UAS system must be capable of detecting, tracking as well as intercepting UAVs. Different principles of operations are deployed for detection and tracking (D&T) and interdiction.

1. Detection and tracking C-UAS

Radar: This is a traditional method which detects the electromagnetic waves emitted from a transmitter and reflected from an object / UAV to determine the size and speed of the UAV. However, detecting objects the size of a UAV requires a high frequency radar. Further, these systems often employ algorithms to distinguish between drones and other small, low-flying objects, such as birds. While radar can be used to detect and track a UAV, the detection reliability is low and highly susceptible to weather conditions. Efficacy of algorithms also determine the true positive rates of the radar, i.e., distinguishing UAVs from birds.

Radio-Frequency (RF): RF scanners and spectrum analyzers identify the presence of drones by scanning for frequencies on which most drones are known to operate. Algorithms do pick out and geo-locate RF-emitting devices in the area that are likely to be drones but are not very accurate. RF scanners can be effective at detecting the presence of a drone and probably identifying the type. However RF scanners are limited in their capability to accurately locate a drone in space.

Electro-optical (EO): Visual cameras are also used for detection and tracking of UAVs. A UAV could be detected and its path traced using a single camera by detecting motion cues, visual marks and shape detectors. Multiple fixed ground cameras are also used in some cUAS systems. Recently neural networks have been trained to detect these cues and isolate a UAV, but they do have high volume of false positive detections due to similarities between UAVs and birds. Similarly, newer, non-standard or customized UAVs also result in high false negatives detection. All visual cameras have a natural limitation of being ineffective in darkness. Thermal cameras are a good option to use in darkness. These cameras capture the heat signature of UAVs. While thermal cameras also are limitations around distinguishing drones from birds, however heat signature databases are making this distinction an easier challenge to resolve. Most of the commercial system combine visual and thermal sensors to make them deployable in day, night and twilight conditions.

Acoustic: Acoustic systems overcome and EO sensor's challenge of line-of-sight requirements and small size of UAVs. Typically, these systems capture the noise of UAV rotors and compare them with a library of sounds produced by known drones. Sound signatures of drones have a high susceptibility to surrounding noise, wind direction and ambient temperature.

Combined sensors: Typically, most of the commercially available cUAS integrate a variety of different sensor types to provide a more robust detection capability. For example, a system might include an acoustic sensor that cues an optical camera when it detects a potential drone in the vicinity. The use of multiple detection elements may also be intended to increase the probability of a successful detection, given that no individual detection method is entirely failproof.

Number of considerations need to be done when evaluating a C-UAV detection method. Many factors, including ambient light, weather, ambient noise, cost, line of sight and detection range influence the effectiveness of each method.[38]

	RF		Optical			Acoustic
Factor	Active Radar	RF Scanner	Visual	IR	Laser	
Light	✓	✓	✓		✓	✓
Darkness	✓	✓		✓	✓	✓
Noise	✓	✓	✓	✓	✓	✓
Birds		✓				
Adverse Weather						
Identification		✓	✓	Limited		✓
Multiple UAV detection	✓	Only if on different channels	✓	✓	✓	Only if different type
Cost		✓	✓			
Long Range Detection	✓	✓	With focus lens		✓	
Tracking	✓	Multiple	✓	✓	✓	Multiple

[38] SoK - Security and Privacy in the Age of Drones: Threats, Challenges, Solution Mechanisms, and Scientific Gaps by Ben Nassi, Asaf Shabtai, Ryusuke Masuoka, Yuval Elovici: https://arxiv.org/abs/1903.05155

2. Interdiction

While detection and tracing of rogue UAVs is a crucial element in cUAS space, it is only half of the complete solution. Interdiction of an unauthorized UAVs and neutralizing their threat will after all make the skies safer. Most of the methods available for interdicting a UAV can either be classified as:

a. Protocol based interdiction

b. Sensor based interdiction

c. Interdiction using jammers

d. Physical interdiction

Protocol based interdiction:

These systems exploit protocol vulnerabilities in the communication systems of drones, which we would normally term as hacking. Older generation UASs worked on open access point based WiFi networks and were easier to hack into and gain control. Some UAVs (rudimentary, inexpensive) use MAVLink protocols, which can be easily hacked into using replay techniques[39]

Sensor based interdiction:

Drones contain various sensors like motion sensors, gyroscopes, obstacle avoidance sensors, camera sensors and many others which are used for various flight functions. Sensor based interdiction (also called spoofing), typically disrupts or spoofs the sensor outputs for the UAV to receive error signals and the UAV is likely to either crash or activate an internal safety maneuver to land safely. Spoofing the GPS to force a UAV to change its pre-programmed mission plan to another safe one is also a common interdiction methodology.

Interdiction using jammers:

Jammers disrupt the radio frequency link between the drone and its operator by generating large volumes of radio frequency output. Once the RF link, which can include WiFi links, is severed, a UAV will either descend to the ground or initiate a return to home maneuver. Similarly, satellite signal jamming disrupts the UAV's satellite link, such as GPS or GLONASS, which is used for navigation. UAVs that lose their satellite link will hover in place or land.

Physical interdiction:

Physical interdictions UAVs are almost always aimed towards crashing the UAV to ground. These cUAS systems typically use bullets or other specialized ammunition to be fired at the rogue UAVs. High energy Laser beams are also targeted at UAVs to burn them down. Some C-UAS systems also use nets to be fired at UAVs to tangle their propellers and bring them down. Physical interdiction cUAS systems often are often self-defeating in their purpose, since a falling UAV is a dangerous projectile.

[39] Replay Technique: https://www.kaspersky.com/resource-center/definitions/replay-attack

V Use cases: Current Approaches – Enabling our Marshalls

As highlighted in Section II.C, multiple governments have started cognizance of the risk and have started investing in counter drone technologies. These have been used in high profile events to ensure security and prevent penetration.

In this section, we will look at specific examples of how anti drone systems have been used across the world and the current landscape of anti-drone systems in India.

A. How are military personnel using anti-drone systems?

The foremost adopters of counter-UAS technologies have been militaries and defense organizations around the world. The growing use of military drones around the world has sparked off a race to develop and procure the most cutting edge anti-drone systems in the world. Though militaries have been highly secretive of the anti-drone systems deployed, there is some information in the public domain on the nature of their installations. The anti-drone systems deployed have been found to use the following techniques:

- **GPS spoofing:** A noteworthy example is Iran which has allegedly twice taken down US drones in the past. In 2011, the RQ-170 Sentinel stealth UAV which was spying on Iran's nuclear facilities was brought down by Iran. Iran claimed that its cyber warfare unit had jammed the drone's communication and by GPS spoofing, made the drone land in Iran which seems believable as the drone, which was later displayed to the world as proof of Iran's claims, was unchanged and intact. Again, in 2012, Iran took control of a US Scan Eagle long endurance drone.[40]
- **Laser guns:** Militaries around the world have used strong laser guns to bring down rogue or unidentified drones with US Marine Corps testing the system in Jun'19. The U.S. Marine Corps is testing a prototype laser weapon that could be used by war fighters on the ground to counter enemy drones. The prototype Compact Laser Weapons System— or CLaWS— is the first ground-based laser approved by the US Defense Department for use by ground troops, the US Marine Corps explained. However, the laser is not a standalone weapon, but is meant to serve as part of a larger counter-drone system.[41]
- **Machine guns and a hybrid system:** Belarus has developed "TRIO," a new air defense system that can target and destroy aerial targets including drones as small as 30x30 cm. The system has three attack units comprised of short range missiles, surface to air missiles and machine guns which can automatically detect and deploy the best option to tackle the drone depending on the threat level and the size.[42]
- **Missiles:** In a rare event, it was revealed in 2017 that a US military ally had used a US$3 million patriot missile to bring down a US$200 commercial drone thus highlighting the very needs of this industry of bringing and adopting cost effective ways to tackle with rogue drones.[43]

B. Anti-drone systems in our backyard: Police operations

While military applications of anti-drone systems focus on range and "shoot to kill" operations, approaches adopted by local police personnel are more focused on capturing the drones or thwarting the drone operations to not injure civilians on the ground below. In addition, it might be more important for police personnel to identify and capture the drone operators so that perpetrators can be brought to justice. Across the world we have seen various techniques both hi-tech to low and even no-tech being deployed.

- **Drone nets:** Tokyo police have been known to use drone nets to capture rogue drones by flying a big net attached to a "good" drone which is then flown near the rogue drone to capture its propellers on the net thus catching and neutralizing the drone.[44]
- **RF jammer guns:** Changhua County Police in Taiwan have been testing RF jammer guns to bring down rogue drones.[45] RF jamming guns typically work by the transmission of radio signals that disrupt communications between the UAV operator and the UAV thus breaking the communication link and initiating a default "return to home" maneuver or a "stand-by" maneuver and hence neutralizing the threat by stopping the drone from carrying out its intended operation. This method is the most common method that is being explored by police and military personnel across the world.
- **Eagles:** Police forces have also been dabbling with non-technology solutions to bring down rogue drones. The police in Netherlands started training eagles to bring down rogue drones by latching on to the propellers with their talons, instantly disabling them. However, they stopped using them when they proved ineffective over time.[46]
- **Tracking:** In India, the Goan police has successfully tested a new system which can live track the current location of unauthorized flying drones, with data which can also be stored for later investigation. The system deployed is mobile and works for a 5-km range. It also has a public announcement system and can also be used to provide additional safety to VVIP movements and other big events in Goa.[47]
- **Guns:** Finally, police personnel have also been authorized to shoot down drones as a contingency measure. In India, the Delhi Police was authorized to shoot down unidentified flying objects to ensure public safety.[48] However, this method is dangerous as the wreckage can harm innocent civilians on the ground below and there is always the threat of stray bullets hurting someone.

[40] "Iran's alleged drone hack: tough but possible" - https://www.wired.com/2011/12/iran-drone-hack-gps/

[41] "US Marines to test drone-killing laser weapon" - https://www.defensenews.com/industry/techwatch/2019/06/19/us-marines-to-test-drone-killing-laser-weapon/

[42] "Belarus Develops Anti-Drone Defense System" - https://www.defenseworld.net/news/24642/Belarus_Develops_Anti_drone_Defense_System#.XS654ugzaM8

[43] "A US ally shot down a $200 drone with a $3 million Patriot missile" - https://www.theverge.com/2017/3/16/14944256/patriot-missile-shot-down-consumer-drone-us-military

[44] "Tokyo police are using drones with nets to catch other drones" - https://www.telegraph.co.uk/technology/2016/01/21/tokyo-police-are-using-drones-with-nets-to-catch-other-drones/

[45] "Changhua police test jammer devices used to disable drones" - http://www.taipeitimes.com/News/taiwan/archives/2019/06/28/2003717743

[46] "Dutch police will stop using drone-hunting eagles since they weren't doing what they're told" - https://www.theverge.com/2017/12/12/16767000/police-netherlands-eagles-rogue-drones

[47] "Now, Goa police can live track illegal drones" - https://www.thehindu.com/news/national/other-states/now-goa-police-can-live-track-illegal-drones/article25935442.ece

[48] "Police can shoot down unidentified flying objects" - https://timesofindia.indiatimes.com/city/delhi/Police-can-shoot-down-unidentified-flying-objects/articleshow/50763996.cms

C. Event specific measures

Organizers of large events are increasingly looking to deploy anti-drone systems to monitor the air-space above the event to ensure the absence of rogue drones during the event. Large gatherings are hot spots and a logistical nightmare for police forces to provide security to the event. In case of unidentified drone sightings in these events, the priority of security personnel is to detect and stop the drone operation without causing any harm to the civilians below. In case that doesn't work, security personnel may resort to more destructive means of bringing down drones.

- **Audio receptors:** At the Boston marathon in the past, organizers have deployed audio receptors to identify the location of drones and then deploy appropriate counter-drone measures to neutralize them. Drones make a unique sound, like that of an "angry beehive" and the same is scanned to detect drones. This is not an advanced radar or early-warning detection system- the company's system simply compares sounds it hears to a database of drone sounds. When there's a match, the system sends out an alert via text message or email. Net guns are then used by police personnel to bring down the drones.[49]
- **Drone nets:** For the Winter Olympics held in South Korea in 2018, as part of safety precautions, drone-catching drones were deployed to cast nets over any dangerous-looking unmanned aerial vehicles that approach the Olympics grounds in Pyeongchang. Additionally, security teams were also trained to shoot down such UAVs.[50]
- **RF jammers:** French Army soldiers were seen holding anti-drone guns during the traditional Bastille Day military parade on the Champs-Elysees Avenue in Paris, France.[51] RF jammers can prove to be an effective way of successfully neutralizing drones at such crowded events with minimum to no collateral damage.
- **GPS spoofing:** In India, the Ahmedabad Police Department used an anti-drone system during the 142 Lord Jagannath's Rath Yatra. The system was used to eliminate any unauthorized drones or unmanned aerial vehicles used during the Rath Yatra. The city police installed the anti-drone system to jam the GPS signals of the unauthorized drones in the area to stop the user from operating the drones during the Rath Yatra.[52]

D. Measures taken by private entities

Following the London Gatwick airport's closure for 33 hours where the military was called in to tackle the threat, several private players and airports are buying anti-drone systems themselves instead of relying on government or military provided anti-drone systems. Such a huge investment by a private entity might just be necessary to ensure smooth running of operations at least in the short term.

- **Military grade hybrid systems:** At the end of December 2018, Gatwick Airport, the second largest airport in the UK was shut down after a drone was reportedly sighted flying nearby. Flights resumed at the airport three days later, after the British Army reportedly brought in an Israeli-built drone defense system.[53] To protect themselves from future incidents, both Gatwick and Heathrow airports have invested in their own anti-drone systems . Heathrow and Gatwick confirmed that they've spent millions to acquire and install their own "military-grade anti-drone apparatus". Neither airport indicated what technology they've fielded, but they've indicated that they will provide a "similar level of protection" as what the army brought with it in December. That system was reportedly manufactured by Israeli defense contractor Rafael, which allows operators to jam a drone's radio signals and allow it to land safely.[54]
- **Hybrid detection systems and drone nets:** German companies have tested a solution that could be highly automated, connecting existing air traffic data with advanced radar systems, acoustic and infrared sensors and optical equipment to first detect possible intruders and then neutralize them with other drones. In the tests, after detection, "good" drones were sent with large nets attached to them to neutralize rogue drones.[55]

[49] "The low-tech anti-drone technology at the Boston Marathon today involves net guns and text messages" - https://qz.com/387162/the-low-tech-anti-drone-technology-at-the-boston-marathon-today-involves-net-guns-and-text-messages/

[50] "Security measures at the Winter Olympics include drones that catch drones" - https://qz.com/1193748/winter-olympics-2018-drones-that-catch-drones-are-part-of-security-measures-at-the-pyeongchang-games/

[51] "Drone snipers" - https://news.abs-cbn.com/overseas/multimedia/photo/07/15/19/drone-snipers

[52] "Ahmedabad: Anti-drone system installed to monitor threats" - https://www.dnaindia.com/ahmedabad/report-ahmedabad-anti-drone-system-installed-to-monitor-threats-2767542

[53] https://www.theguardian.com/world/2019/jan/03/heathrow-and-gatwick-millions-anti-drone-technology

[54] "London's Heathrow and Gatwick airports have purchased their own anti-drone systems" - https://www.theverge.com/2019/1/5/18169215/london-heathrow-gatwick-airports-anti-drone-defense-systems

[55] "Germany's DFS, Rheinmetall demonstrate system to prevent drone disruptions" - https://www.reuters.com/article/us-germany-drones/germanys-dfs-rheinmetall-demonstrate-system-to-prevent-drone-disruptions-idUSKCN1PV2E7

E. Challenges

As much as these technologies are successfully tested in controlled environments, their success and applicability in real-world scenarios is yet to be completely established. Anti-drone technologies are still very nascent and companies are trying to build the best systems involving multiple technologies to deal with all possible contingencies. However, their effectiveness is yet to be established and some of the challenges that we have seen in the market when it comes to their deployment are:

- **Economic feasibility:** A US military ally used a missile costing millions of dollars to bring down a US$200 commercial drone. This highlights the needs of this industry of bringing and adopting cost effective ways to tackle rogue drones.[56] Given the cost of commercially available drones today, there is a need to research economically feasible options for countering rogue drones.
- **Effective contingency plans:** Post the London Gatwick Airport closure in December 2018 due to rogue drone incursions, the London Police revealed that its "drone plan" had been based "around a single drone incursion and not a multiple one"[57]. Further, officers needed to be effectively trained on how "jamming technology" can be used in urban environments. One officer was quoted as saying "I still don't know what effect a jamming technology is going to have on a hospital that is four kilometres away, so we have to be really careful" thus highlighting the opportunity for better preparedness of the local police personnel of dealing with such contingencies despite having the right equipment on ground.
- **Thorough on-field testing:** In the same event highlighted above at the London Gatwick Airport, the police also revealed that the jamming technology intended to bring down a drone was "just not tested". The police officers further commented that, "All this stuff is built for theatre of war. We are introducing something that is great in a desert into an urban environment and saying we are not quite sure what it's going to do."[58], thus highlighting the need for constant on-field testing for all officers so that they understand the technology, its usage and its repercussions.
- **Want of effective solutions:** In October 2016, the FAA sent out a letter to airports saying "Unauthorized UAS detection and counter measure deployments can create a host of problems, such as electromagnetic and Radio Frequency (RF) interference affecting safety of flight and air traffic management issues"[59], which highlights the challenges of using RF or electromagnetic jammers in areas like the airports as it might interfere with local operations. In 2018, the FAA issued a follow up letter to the October 2016 letter which discussed the findings of the counter drone study they did at some airports concluding that airport environments had numerous sources of potential interference–more than anticipated and high radio spectrum congestion in these environments made detection more difficult and, in some instances, not possible.
- **Legal challenges:** In most countries jamming radio signals often requires permission and a host of approvals and licenses before such equipment can be deployed. For example, in the UK, one needs to have authority under the Wireless Telegraphy Act to start broadcasting any kind of signal – even one intended to bring down a fleet of unauthorized drones.[60] In the US, one runs into the Communications Act of 1934 and the FCC regulations having similar repercussions.[61]
- **Lawsuits for damages:** If police personnel are using anti-drone measures in crowded areas to bring down a drone without taking adequate measures, it could lead to injuries to some observer down below thus not only inviting a civil lawsuit but also endangering people's lives. In one instance in Hong Kong, GPS jamming caused 46 drones to plummet during a display over Victoria Harbour causing at least HK$1 million (US$127,500) in damage, according to a senior official from the Hong Kong Tourism Board.[62]
- **Rapid technological advancement:** Drones is a nascent industry that is still evolving technically. Researching and finding new solutions to counter rogue drones requires significant investment and can sometimes lead to results that may not be technically relevant by the time they are launched into the market. In its statement in 2018, the FAA said, "Drone detection systems require redundant equipment in order to cover an airport, making the costs prohibitive," and because drone technology is changing so rapidly, any counter measure "rapidly becomes obsolete."[63]

[56] "A US ally shot down a $200 drone with a $3 million Patriot missile" - https://www.theverge.com/2017/3/16/14944256/patriot-missile-shot-down-consumer-drone-us-military

[57] "Gatwick Airport police 'not prepared for two drones'" - https://www.bbc.com/news/uk-england-sussex-48929442

[58] "Gatwick Airport police 'not prepared for two drones'" - https://www.bbc.com/news/uk-england-sussex-48929442

[59] "7 BIG PROBLEMS WITH COUNTER DRONE TECHNOLOGY (DRONE JAMMERS, ANTI DRONE GUNS, ETC.)" - https://jrupprechtlaw.com/drone-jammer-gun-defender-legal-problems

[60] "A few reasons why cops haven't immediately shot down London Gatwick airport drone menace" - https://www.theregister.co.uk/2018/12/20/gatwick_drone_non_shootdown_reasons/

[61] "7 BIG PROBLEMS WITH COUNTER DRONE TECHNOLOGY (DRONE JAMMERS, ANTI DRONE GUNS, ETC.)" - https://jrupprechtlaw.com/drone-jammer-gun-defender-legal-problems

[62] "HK$1 million in damage caused by GPS jamming that caused 46 drones to plummet during Hong Kong show" - https://sg.news.yahoo.com/hk-1-million-damage-caused-080848555.html

[63] "Ineffective Anti-Drone Systems Leave U.S. Airports Facing Risks Like London's" - https://www.insurancejournal.com/news/national/2018/12/27/512863.htm

VI Path ahead in India –
Taming the Wild West

As indicated in Section III A, by virtue of its robust framework, India has already taken first step towards bringing accountability in drone ownership and operations. Digital Sky, when effectively implemented, will enable controlling the problem in its roots. Besides effective C-UAV strategy must initiate efforts from all quarters of law enforcement, law and citizen participation.

A. Empowering the homeland security forces

The state and city police forces will remain at the tactical level of counter-UAV measures proposed and effected by the regulations and framework. These forces, at police station levels will need to be equipped with training, SOPs and the required hardware equipment to identify, track and neutralize this threat. Our critical infrastructure and large industrial and infrastructure assets are protected by the Central Industrial Security Force (CISF), Central Reserve Police Force (CRPF) and similar paramilitary forces. These important security agencies also need to be equipped with the technologies.

B. Risk and asset profiling

Considering the variety in types, sizes and applications of UAVs and an equally wide spread of C-UAV technology referenced in Section IV-A, the C-UAV protocols, frameworks and implementation may vary from an asset to asset and their unique operating environment. Airport zones, having multiple communication technologies and security/ operating protocols already present, may require highly sophisticated C-UAV technology implementation as compared to a "Smart" city or similar urban environment with dense congestion of Wi-fi or other open radio frequency enabled devices. A long pipeline asset cutting far and wide through a terrain ranging from congested encroached spaces through remote jungles and mountains may require a very different approach to C-UAV implementation. A collective study involving security and safety experts from these asset classes along with the policy making bodies is required to define a broad but inclusive C-UAV framework.

C. Boost to allocation for indigenous R&D and Make in India

Apex security R&D organizations like the DRDO[64] labs and Bureau of Police Research and Development (BPR&D)[65] are already taking up C-UAV related R&D and technology aggregation projects. These projects could be given further boost to support wider participation. Though C-UAV technology is enlisted under the Make in India program as well, major industry participants are from outside the country. Early guidelines from the government will help indigenous manufacturers to plan their technology roadmap and hence increase their share of pie when the market opens for procurement of these systems.

D. Liquidating the threat of legacy UAVs

In section III, B (iii) above, we discussed about a looming threat from the latent population of pre-regulations era UAVs in the country. A program or scheme to either integrate these UAVs within the regulatory fold or a way to ensure that these UAVs have been completely eliminated from the system is an urgent need. The large estimated number of these UAVs shall otherwise risk to remain as a potential threat to our security agencies. Neutralizing such a threat is a difficult challenge at the level of local law enforcement.

E. Citizen participation

The Digital Sky stack as referenced in Section III-A, enables an ecosystem of Digisky Service Providers (DSPs) which could model their business offerings on data available from the Digital Sky platform. An initiative from the enforcement authorities could involve an app, which will help common man identify a drone flying in its vicinity to be either legal or illegal and report this to the authorities, along with the drone's geographical coordinates. This could effectively create a virtual drag net for UAV detection involving citizen "nodes".

[64] Expanding Anti-uavs Market to Counter Drone Technology – Dinkar Peri – Claws Journal – Winter 2015

[65] http://bprd.nic.in/content/38_1_ConferenceSeminarWorkshop.aspx

Abbreviations

AGL	Above Ground Level
ATS	Air Traffic Service
AR	Augmented Reality
AI	Artificial Intelligence
BVLOS	Beyond Visual Line Of Sight
CAGR	Compound Annual Growth Rate
CAAC	Civil Aviation Administration of China
DGCA	Directorate General of Civil Aviation, Government of India
DPR	Detailed Project Report
DIPP	Department of Industrial Policy & Promotion
EY	Ernst and Young LLP India
FAA	US Federal Aviation Administration
FCC	US Federal Communications Commission
FDI	Foreign Direct Investment
FICCI	Federation of Indian Chambers of Commerce & Industry
GDP	Gross Domestic Product
GIS	Geographic Information System
IoT	Internet of Things
LIDAR	Light Detection and Ranging
LEAs	Law Enforcement Agencies
LoS	Line of Sight
MTOW	Maximum Takeoff Weight
MHA	Ministry of Home Affairs
NDVI	Normalized difference vegetation index
NPNT	No Permission No Takeoff
PSUs	Public Sector Units
RPA	Remotely Piloted Aircraft
RPAS	Remotely Piloted Aircraft System
SOP	Standard Operating Procedure
UAS	Unmanned Aircraft System
UAV	Unmanned Aircraft Vehicle
UAOP	Unmanned Aircraft Operator Permit
UIN	Unique Identification Number
VLOS	Visual Line-Of-Sight
VR	Virtual Reality

FICCI Committee on Drones

FICCI has many specialised committees where key concerns of the industry are debated and discussed with the specific aim of presenting the recommendations to the Government for favourable decisions.

FICCI has identified drones as one of The priority areas.

FICCI Committee on drones (UAV/UAS/RPAS) has been working on the policy advocacy and the regulatory frame work to facilitate the growth of ecosystem for drones in the country

Some of the focus areas of the Committee are

- Regulatory Evolution
- Industry licensing regime
- Operations regulations
- Import/export-regulation
- Counter drone technologies
- UAV exports from industry
- Demand analysis for drones
- User sensitization / Formal education

Contributors to this Paper

EY

Rajan Sachdeva
Partner – EY
Technology Consulting Lead
EMEIA and Indian Region
Email: rajan.sachdeva@in.ey.com

Akshya Singhal
Partner – EY Advisory Services
Email: akshya.singhal@in.ey.com

Arun Nagarajan
Director – EY Advisory Services – Digital
Email: arun1.nagarajan@in.ey.com

Shrikant Thakker
Senior Manager – Digital – UAS Centre of Excellence
Email: shrikant.thakker@in.ey.com

Kartik Verma
Consultant – EY Advisory Services – Digital
Email: kartik.verma@in.ey.com

FICCI

Mr. Sumeet Gupta
Senior Director
Email: sumeet.gupta@ficci.com

Ms. Neha Mathur
Joint Director - Drones (UAS) and Geospatial Technologies
Email: neha.mathur@ficci.com

Mr. Ankit Gupta
Deputy Director – Homeland Security
Email: ankit.gupta@ficci.com

Notes:

Notes:

Notes:

EY offices

Ahmedabad
2nd floor, Shivalik Ishaan
Near C.N. Vidhyalaya
Ambawadi
Ahmedabad - 380 015
Tel: + 91 79 6608 3800
Fax: + 91 79 6608 3900

Bengaluru
6th, 12th & 13th floor
"UB City", Canberra Block
No.24 Vittal Mallya Road
Bengaluru - 560 001
Tel: + 91 80 4027 5000
+ 91 80 6727 5000
+ 91 80 2224 0696
Fax: + 91 80 2210 6000

Ground Floor, 'A' wing
Divyasree Chambers
11, O'Shaughnessy Road
Langford Gardens
Bengaluru - 560 025
Tel: +91 80 6727 5000
Fax: +91 80 2222 9914

Chandigarh
1st Floor, SCO: 166-167
Sector 9-C, Madhya Marg
Chandigarh - 160 009
Tel: +91 172 331 7800
Fax: +91 172 331 7888

Chennai
Tidel Park, 6th & 7th Floor
A Block, No.4, Rajiv Gandhi Salai
Taramani, Chennai - 600 113
Tel: + 91 44 6654 8100
Fax: + 91 44 2254 0120

Delhi NCR
Golf View Corporate Tower B
Sector 42, Sector Road
Gurgaon - 122 002
Tel: + 91 124 464 4000
Fax: + 91 124 464 4050

3rd & 6th Floor, Worldmark-1
IGI Airport Hospitality District
Aerocity, New Delhi - 110 037
Tel: + 91 11 4731 8000
Fax + 91 11 4731 9999

4th & 5th Floor, Plot No 2B
Tower 2, Sector 126
NOIDA - 201 304
Gautam Budh Nagar, U.P.
Tel: + 91 120 671 7000
Fax: + 91 120 671 7171

Hyderabad
Oval Office, 18, iLabs Centre
Hitech City, Madhapur
Hyderabad - 500 081
Tel: + 91 40 6736 2000
Fax: + 91 40 6736 2200

Jamshedpur
1st Floor, Shantiniketan Building
Holding No. 1, SB Shop Area
Bistupur, Jamshedpur – 831 001
Tel: +91 657 663 1000
BSNL: +91 657 223 0441

Kochi
9th Floor, ABAD Nucleus
NH-49, Maradu PO
Kochi - 682 304
Tel: + 91 484 304 4000
Fax: + 91 484 270 5393

Kolkata
22 Camac Street
3rd Floor, Block 'C'
Kolkata - 700 016
Tel: + 91 33 6615 3400
Fax: + 91 33 6615 3750

Mumbai
14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (W), Mumbai - 400 028
Tel: + 91 22 6192 0000
Fax: + 91 22 6192 1000

5th Floor, Block B-2
Nirlon Knowledge Park
Off. Western Express Highway
Goregaon (E)
Mumbai - 400 063
Tel: + 91 22 6192 0000
Fax: + 91 22 6192 3000

Pune
C-401, 4th floor
Panchshil Tech Park
Yerwada
(Near Don Bosco School)
Pune - 411 006
Tel: + 91 20 4912 6000
Fax: + 91 20 6601 5900

Ernst & Young LLP

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 22 Camac Street, 3rd Floor, Block C, Kolkata - 700016

EYIN1907-016
ED None

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

JS

Federation of Indian Chambers of Commerce and Industry

Industry's Voice for Policy Change

About FICCI

Established 92 years ago, FICCI is the largest and oldest apex business organization in India. Its history is closely interwoven with India's struggle for independence, its industrialization, and its emergence as one of the most rapidly growing global economies.

A non-government, not-for-profit organization, FICCI is the voice of India's business and industry. From influencing policy to encouraging debate, engaging with policy makers and civil society, FICCI articulates the views and concerns of industry, reaching out to over 2,50,000 companies. FICCI serves its members from large (domestic and global companies) and MSME sectors as well as the public sector, drawing its strength from diverse regional chambers of commerce and industry.

The Chamber with its presence in 16 states and 10 countries provides a platform for networking and consensus-building within and across sectors and is the first port of call for Indian industry, policy makers and the international business community.

The information in this publication has been obtained or derived from sources believed to be reliable. Though utmost care has been taken to present accurate information, FICCI makes no representation towards the completeness or correctness of the information contained herein. This document is for information purpose only. This publication is not intended to be a substitute for professional, legal or technical advice. FICCI does not accept any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents

ey.com/in

@EY_India EY|LinkedIn EY India EY India careers ey_indiacareers