The fourth unit is a more explicit and traditional EW unit known as the EW Jamming Regiment, again highlighting the intersection between the cyber and EM domains.[56]

III. Capturing and Monitoring Technological Innovation: The Five Revolutions[57]

Defense communities across the Indo-Pacific are turning to investment in new and emerging dual-use 4IR technologies to better cope with the complex, uncertain, and fast-moving strategic context and expanding threat environment described above.

The identity of the specific technologies of interest is not a secret. A survey of government documents from India, China, the United States, Australia, and Japan, and of open-source reporting and commentary about each country's defense-technology development priorities, reflects widespread and overlapping interest in the technologies in Table 2 below.

These lists are useful, but they are also vague. They tend to capture *categories* of technologies—AI, advanced materials, energy capture, and storage are all useful examples—that include multiple specific technologies or techniques. Many of the technologies of common interest have an array of applications—for instance, blockchain, unmanned systems, or directed energy—that can support a number of missions and achieve various effects. Moreover, different states will have different resources available for developing these technologies for military use.

In fairness, some militaries are more open and granular in their discussion of their interest in emerging technologies and their objectives in developing them. Australia's "Defence Science and Technology Strategy 2030" includes a robust discussion of the technological context and landscape, but also establishes eight high-impact "Star Shot" initiatives that help observers understand where its technological investment priorities rest, including[58]

- resilient multi-mission space;
- information warfare;
- agile command and control;
- quantum-assured position, navigation, and timing;
- disruptive weapon effects;
- operating in chemical, biological, radiological, and nuclear (CBRN) environments;
- battle-ready platforms; and
- remote undersea surveillance.

Still, the task of capturing and assessing the strategic and operational impact of defense innovation efforts based on monitoring technologies can be overwhelming, and can leave analysts and decision-makers with an incomplete understanding of how technology is shaping the future of military capabilities, the threat environment, and strategic competition in the Indo-Pacific.

Table 2: A list of technologies of general interest to militaries in the Indo-Pacific.

Artificial intelligence	5G networks	Quantum computing and encryption
Additive manufacturing	Unmanned systems and robotics	Hypersonic flight
Advanced materials	New energy capture, storage, and distribution	Directed energy
Electromagnetic weapons	Secure communications	Neuro and biotechnologies
Internet of Things	Augmented and virtual reality	Big-data analysis
Cloud computing	Blockchain	Smart sensors
Space technologies		

56 Dr. Thomas Withington, "Know Your Enemy," *Armada International*, August 27, 2020, https://armadainternational.com/2020/08/know-your-enemy/.

57 The author developed this framework while at IHS Jane's (now Janes) in 2016. It originally featured four revolutions, and the content was first published as part of the Eurosatory Show Daily in 2016. The author has briefed versions of the framework in both public and private settings over the last four years. The framework has been refined and expanded to include cyber and information operations in 2019 and 2020.

58 "More, Together: Defence Science and Technology Strategy 2030."

Figure 1: The Five Revolutions in capabilities that militaries seek to achieve through technological innovation and development (source: Tate Nurkin, with images from Microsoft 365).

A more constructive and efficient approach is to focus instead on the *effects* that defense communities are trying to achieve through their research and development (R&D) efforts and through associated organizational changes and industry-engagement efforts.

Here, most modern militaries are remarkably consistent in the outcomes they are trying to achieve, namely driving step-changes—or "revolutions"—in capabilities in five broad areas.

Like all frameworks, this one comes with caveats. The seams between these five revolutions are not always clean. Broad capability areas such as human-machine teaming—and especially brain-machine interfaces—could fall into both the first and second revolutions, and possibly the fourth. Components of EW could also easily be disentangled and captured by perception, processing, and cognition (SIGINT collection and analysis); human and machine performance (electronic defense); and communication, navigation, targeting, and strike (electronic attack).

Even with room to debate how some capabilities might be categorized, in an environment in which technologies and domains are blurring and fusing into an amorphous, sometimes difficult to disaggregate mess of "innovation" and "multi-domain operations," there remains utility in understanding what effects militaries are trying to achieve through their investment in emerging technologies.

1. Toward Perfect Situational Awareness: A Revolution in Perception, Processing, and Cognition

Decision-makers and operators are under considerable pressure to speed up Colonel John Boyd's OODA (observe-orient-decide-act) loop to, in the words of the Australian Defence Science and Technology Strategy 2030, "understand, shape and dominate the future multi-domain battlespace."[59]

This revolution concentrates on efforts to accelerate the first three components of the loop—observe, orient, and decide—by improving the scale of information collected, the pace of its processing, and, as a result, the quality of situational awareness on which decisions are made and subsequent actions taken.

Novel capabilities, such as smart-sensor networks, persistent and frequently uncrewed ISR systems, AI-enabled

59 Ibid.

radio-image identification technology (a priority application of AI for Japan's Self-Defense Force), and even more aspirational capabilities such as synthetic-biology anti-submarine warfare sensors are all among the broad suite of technology-enabled capabilities designed to collect more, more frequent, and more accurate information.

The perception, processing, and cognition revolution is particularly important in the Indo-Pacific context, which is marked by massive distances, different topographies, long borders and boundaries, large and crowded cities, and a strong maritime nature.

Being able to persistently collect data in contested urban environments across huge geographical spaces and in opaque environments, such as the undersea domain, is essential to first detecting, and then rapidly devising responses to, fast-moving, if distant, challenges. As noted above, Australia has prioritized enhancing remote undersea sensing.[60] In addition, DARPA's "Ocean of Things" project aims to "seed the seas with thousands of floating sensors, monitoring everything that passes from aircraft to submarines."[61]

The processing and cognition component of this revolution is also relevant because, while the distances across the region can be vast, the speed at which platforms, systems, and sub-threshold threats move has eroded one of the values of the region's strategic geography: time to react. Mark O'Neill of Australia's Lowy Institute argues in a recent article that "geography, previously a useful strategic advantage for island nations, is less of an asset when facing 21s century technologies that are agnostic about distance and domain."[62] AI and big-data technologies that enable information and intelligence to be processed quickly, detect patterns and anomalies, and better understand the nature of operational and tactical environments will buttress efforts to craft effective responses along compressed timelines.

Focus Areas of the Human and Platform Performance Revolution in the Indo-Pacific

- Training and simulation
- Human performance enhancement and hyper-enabled operators
- Exoskeletons
- Brain-machine interfaces and other types of human-machine teaming
- New energy capture and storage and design approaches to enhance endurance and efficiency
- New lightweight, dynamic, and programmable materials
- Active protection systems
- Electronic defense
- Enabling operations in CBRN environments

2. An Age of Hyper-Enabled Platforms and People: A Revolution in Human and Machine Performance

The human and machine performance revolution calls upon 4IR technologies and novel materials to optimize the performance of people, platforms, and systems. Of particular interest is the ability of technologies to improve a suite of common attributes that are vital for the future effectiveness of people and machines, including

- health and recovery capacity;
- speed, strength, and maneuverability;
- power storage and endurance/persistence;
- protection and survivability, including in harsh environments;
- adaptability and resilience;
- connectivity;
- vision, detection, and cognitive capacity; and
- human-machine teaming.

For platforms and some uncrewed systems, this revolution centers on dynamic materials that suppress electromagnetic emissions or enhance kinetic protection. It also features active protection systems that offer proactive defense for crewed platforms against a range of mainly kinetic threats.

Design approaches such as biomimicry are also relevant to ensuring survivability, endurance, and stealth of unmanned systems, depending on the context. In May 2019, South Korea's Defense Acquisition Program Administration (DAPA) announced it is pursuing the development of biomimetic robot systems designed to mirror the natural movements of animals and insects, with plans to field these systems as early as 2024. According to DAPA spokesman Park Jeong-eun, "Biometric robots will be a game changer in

60 "More, Together: Defence Science and Technology Strategy 2030."

61 David Hambling, "DARPA Progress With 'Ocean of Things' All-Seeing Eye On The High Seas," *Forbes*, August 13, 2020, https://www.forbes.com/sites/davidhambling/2020/08/13/darpas-ocean-of-things-is-an-all-seeing-eye-on-the-high-seas/#35226caaf270.

62 Mark O'Neill, "Australia's New Strategic Geography," Lowy Institute, January 13, 2020, https://www.lowyinstitute.org/the-interpreter/australia-s-new-strategic-geography.

One of the US Army's eight cross-functional teams (CFTs) is dedicated to creating a synthetic training environment (STE) to improve soldier training. Here, US Army soldiers assigned to 10th Special Forces Group (Airborne) use and fire an M3E1 Multi-Role Anti-Armor Anti-Personnel Weapon System (also known as a Carl Gustav recoilless rifle) during a Reconfigurable Virtual Trainer demonstration at the 7th Army Training Command's Grafenwoehr training area, Germany, on February 13, 2020. *Source:* US Army photo by Markus Rauchenberger. https://www.dvidshub.net/image/6102694/carl-gustav-virtual-training-grafenwoehr

future warfare, and related technologies are expected to bring about great ripple effects throughout the defence industry."[63]

Multi-faceted efforts to develop "hyper-enabled human operators" are also an important part of this revolution, both within the US military and in several defense communities in the Indo-Pacific.[64]

Advancement in AI, virtual and augmented reality, cloud computing, haptics, and other associated technologies are facilitating more advanced and useful synthetic training environments. Virtual training environments reduce costs of training while simultaneously creating new opportunities for training "reps and steps" that will allow individuals and units to improve performance and better take advantage of more expensive—and, in the age of COVID-19, riskier—live training exercises.

AI is a particularly potent training technology that can enable dedicated virtual assistants, tailored training curricula, and more efficient mining of past training data, all of which can play a role in boosting human performance. Integrating machine and deep learning into wargames will also enhance the fidelity of simulations, which, in turn, can better prepare personnel for more complicated defense and

63 "South Korea to Develop Bio-Inspired Military Robots for Future Warfare," Yonhap News Agency, May 12, 2019, https://en.yna.co.kr/view/AEN20190510008000325.

64 Patrick Tucker, "Special Operations Command Made a Mind-Reading Kit For Elite Troops," *Defense One*, December 11, 2019, https://www.defenseone.com/technology/2019/12/specops-lab-made-mind-reading-kit-elite-troops/161830/.

security environments to include the subtle, difficult-to-detect, and frequently sensitive gray-zone contingencies prevalent in the Indo-Pacific strategic context.

A recent example of the flexibility and utility of virtual training environments is seen in the Royal Australian Air Force's (RAAF) Exercise Virtual Pitch Black. The exercise—held over two weeks in late June and early July 2020—allowed the RAAF to train virtually during heightened concerns about COVID-19.[65]

One of the key aspects of the exercise was the merging of simulators that existed separately, creating an integrated training system that delivered a complexity, density, and scale that effectively represented contested, degraded, and operationally limited environments. A spokesman for the Department of Defence noted at the conclusion of the exercise that "large-scale virtual exercises such as VPB20 are expected to increase in frequency and the RAAF, through the [Air Warfare Centre], is investing to create the Advanced Training and Test Environment (ATTE)."[66]

Development of technologies that facilitate a deeper connection between humans and machines, such as human-machine hybrids and brain-machine hybrids, are also gaining momentum, especially in the United States and China. In December 2019, the US Army released a report entitled "Cyber Soldier 2050: Human/Machine Fusion and the Implications for the Future of the DoD." The report observes that ocular enhancements, optogenetic bodysuit sensor webs, exoskeletons, and auditory enhancements all have the potential to "incrementally enhance performance beyond the normal human baseline" for military operators while "the development of direct neural enhancements of the human brain for two-way data transfer would create a revolutionary advancement in future military capabilities."[67]

This effort to fuse human and machine intelligence and functionality is also a growing preoccupation of China's military and civilian R&D effort. A September 2020 report from the Center for Security and Emerging Technologies at Georgetown University argues that "China has engaged in a nationwide effort to 'merge' artificial and human intelligence as a major part of its next-generation AI development program" through multiple types of brain-machine interfaces.[68]

3. New Efficiencies and the Impending Design Age: A Revolution in Manufacturing, Supply Chains, and Logistics

Additive manufacturing, advanced automation, Internet of Things, digital design and testing, cloud manufacturing, and emerging manufacturing techniques like four-dimensional (4D) printing and synthetic biology manufacturing are combining to usher in a new industrial design age, in which manufacturing processes and material properties will be seen as powerful enablers of constructive innovations in capabilities, rather than as constraints.[69]

The USAF's September announcement of a digitally designed and developed next-generation aircraft has already provided indications of the revolutionary efficiencies in costs and timelines these technologies can generate. Another representative example is the incorporation of AI-enabled predictive maintenance to calculate the health of assets and identify trends in data, allowing militaries to greatly increase the efficiency of logistics and sustainment by anticipating potential failures and ensuring that vehicles stay in service for as long as possible.

Australia's Defence Science and Technology Organisation (DSTO) has included a holistic view of digital manufacturing and predictive maintenance as one of its eight "Star Shots" under the label of "battle-ready platforms." The concept incorporates data analytics, machine learning, and digital twinning to help "predict material state to guarantee platform availability and capability."[70]

The widespread introduction over the next decade of digital design, advanced manufacturing, and predictive-maintenance technologies will necessarily upend current logistics systems, industry dynamics, and industrial supply chains, creating layered challenges for defense communities and industry across the Indo-Pacific.

Most notably, point-of-use printing, digital design, and other technologies and applications will upset industry

65 Flight Lieutenant Bel Scott, "Seizing the Opportunity for Simulated Success," Australian Government, Department of Defence, July 16, 2020, https://news.defence.gov.au/capability/seizing-opportunity-simulated-success.

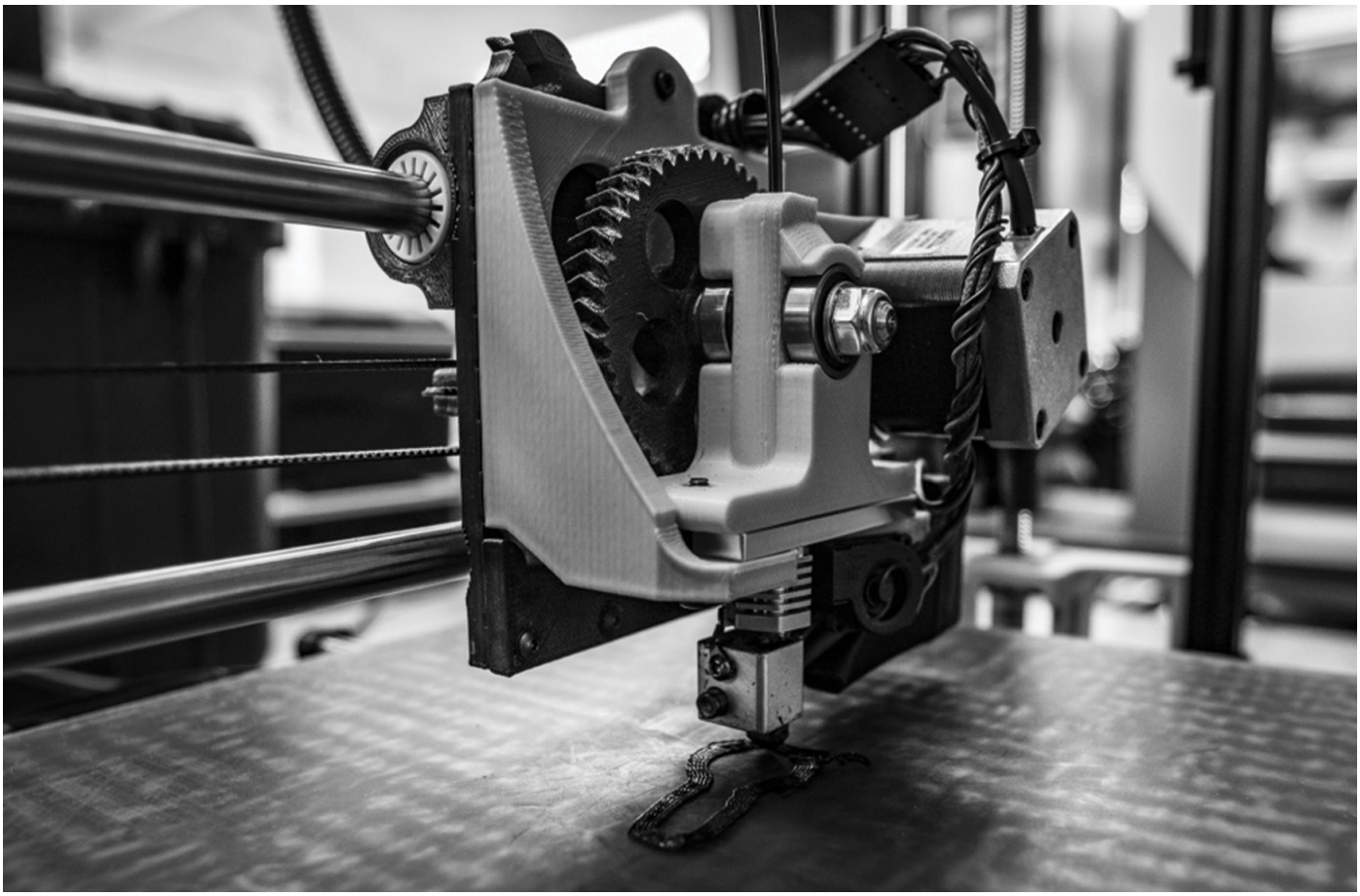
66 Mike Rajkumar, "Exercise Pitch Black 20 Goes Virtual for 2020," Halldale Group, August 18, 2020, https://www.halldale.com/articles/17468-exercise-pitch-black-20-goes-virtual-for-2020.

67 "Cyber Soldier 2050: Human/Machine Fusion and the Implications for the Future of the DoD," U.S. Army, Biotechnologies for Health and Human Performance Council Study Group, November 2019, https://community.apan.org/wg/tradoc-g2/mad-scientist/m/articles-of-interest/300458.

68 William C. Hannas, et al., "China AI-Brain Research: Brain-Inspired AI, Connectomics, Brain-Computer Interfaces," Center for Security and Emerging Technology, Georgetown University, September 2020, https://cset.georgetown.edu/wp-content/uploads/CSET-China-AI-Brain-Research.pdf.

69 Tate Nurkin, "Testimony before the US-China Economic and Security Review Commission Hearing on 'Implications of China's Military Modernization,'" in *Hearing on China's Military Reforms and Modernization: Implications for the United States*, February 15, 2018, https://www.uscc.gov/hearings/chinas-military-reforms-and-modernization-implications-united-states

70 "More, Together: Defence Science and Technology Strategy 2030."



The US Army's first 3D printer, operated by soldiers assigned to 194th Combat Sustainment Support Battalion, 2nd Sustainment Brigade, 520th Support Maintenance Company, manufactures an ignition switch for a Humvee at Camp Humphreys in the Republic of Korea on October 29, 2018. The printer uses the method of additive manufacturing, which is the process of building a 3D structure by introducing material to a space that previously had none. *Source:* US Army photo by Spc. Adeline Witherspoon, 2nd SBDE PAO. https://www.dvidshub.net/image/5010018/2nd-sustainment-brigade-hosts-armys-first-3d-printer

dynamics, especially established supply chains. These supply chains have already been disrupted by attempts to reshore or move supply chains out of China due to the coronavirus pandemic. In response to the combined technological and geopolitical disruptions, many suppliers across supply-chain tiers will need to identify, certify, and integrate new suppliers and manage new approaches to supply-chain management, none of which will be easy or inexpensive.

In addition, countries across the region will need to balance the need for bilateral and multilateral cooperation in defense technology and capability development and procurement to meet immediate challenges with a longer-term desire across many larger states in the region to establish self-reliance in their domestic defense-industrial bases.

The bilateral Defense Technology and Trade Initiative (DTTI) between the United States and India offers a useful example, though many observers believe this initiative has not yet delivered the hoped-for material results in technology development.

Perhaps a better example of these types of bilateral agreements is the recently reported agreement between Australia and Japan that covers "training and exercises, defence science and technology, and defence industry co-operation and co-ordination on regional issues of shared interest."[71]

This instinct to collaborate to meet immediate challenges is being balanced in all three non-US Quad states (as well as others in the region) by the need to build sustainable

71 Gabriel Dominguez, "Australia, Japan Agree to Deepen Defence Co-operation," *Janes Defence Weekly*, October 19, 2020, https://customer.janes.com/Janes/Display/FG_3772218-JDW.

defense and high-tech industry self-reliance. Australia's "2020 Defence Strategic Update" stresses the need for "strengthened sovereign capabilities to enhance the ADF's self-reliance," especially through leveraging 4IR technologies such as three-dimensional (3D) printing, Internet of Things, and fifth-generation (5G) networks.[72]

India, which is currently among the world's largest defense importers, has been even more vocal in its need to build and reform its defense industry. In August 2020, the government issued a ban on the import of one hundred and one weapons systems and defense items that will be implemented in a phased fashion between now and 2024, allowing India to continue defense technology- and capability-development initiatives, including those covered by the DTTI.[73] The announcement was followed closely by a second announcement from the Defense Research and Development Organization (DRDO) of one hundred and eight technological components and systems that will now be developed domestically—including some unmanned systems—as part of the government's Atmanirbhar Bharat ("Self-Reliant India") initiative.[74]

4. Connectivity, Lethality, and Flexibility: A Revolution in Communication, Navigation, Targeting, and Strike

If the perception, processing, and cognition revolution covers the first three components of the OODA loop, the communication, navigation, targeting, and strike revolution is about enabling the final one: act.

This revolution is centered on innovations in operational capabilities and concepts that will disrupt strategic competitions across several critical military domain areas and help militaries gain advantage in the struggle between power projection and A2/AD efforts.

Technology development in this revolution is designed to enable radically new or enhanced capabilities to

- **communicate** more easily between more numerous and more dispersed systems interacting across multiple domains;
- **navigate** platforms and systems, even in environments in which access to global navigation satellite systems (GNSS) is denied;
- **target** platforms and systems with more precision and flexibility, in order to reduce risk in complex, uncertain, and shifting operational environments; and
- **strike, interdict, or deter** adversary capabilities and assets at short notice, at longer ranges, and in contested environments.

Interest in and development of hypersonic missiles—both hypersonic-glide vehicles and scramjet-based missiles—by China, Russia, the United States, Japan, India, and Australia (which has expressed interest in the weapons) is a clear indicator of the significance of this capability revolution to deterring and responding to an expanding range of defense and security threats in the region. Increasing development of these weapons is also stimulating investment in missile-defense systems and capabilities—from high-end interceptors to hypervelocity projectiles and directed energy, among others.

In addition to the strike versus air- and missile-defense competition, actors across the region are also prioritizing development of novel capabilities associated with this revolution in the undersea domain. Taiwan is moving forward with its own indigenous submarine project while Japan welcomed its new *Taigei* class of submarine into service in October 2020. Australia and other states across the region have ongoing submarine procurement and development programs to meet the growing range of threats in the region.

The nature of weapons systems being developed for the undersea domain goes beyond just crewed submarines.

Indicative Focus Areas of the Communication, Navigation, Targeting, and Strike Revolution in the Indo-Pacific

- Advanced/maneuverable/long-range missiles
- Missile-defense interceptors
- Hyper-velocity projectiles
- Hypersonic missiles
- Drone swarms
- Loitering munitions
- Quantum encryption (specifically, quantum-enabled position, navigation, and timing (PNT))
- Directed-energy weapons
- Railguns
- Electronic attack capabilities
- Advanced anti-submarine warfare capabilities

72 "2020 Defence Strategic Update."

73 "India to Ban Imports of 101 Items of Military Equipment," Associated Press, August 10, 2020, https://thediplomat.com/2020/08/india-to-ban-imports-of-101-items-of-military-equipment/.

74 "DRDO Comes Out with list of 108 Military Systems for Production by Domestic Industry," *Times of India*, August 24, 2020, https://timesofindia.indiatimes.com/india/drdo-comes-out-with-list-of-108-military-systems-for-production-by-domestic-industry/articleshow/77725175.cms.

Australia's "2020 Force Structure Plan" mentions development and deployment of undersea mines as a means of protecting the waterways leading into Australia's sovereign territory, while Japan is developing two prototypes of a remotely operated, self-propelled mine system.[75] These systems are designed to be deployed to high-risk sea areas and loiter there until they are remotely detonated in the proximity of enemy vessels."[76] In October 2020, India's DRDO successfully tested a "game changing" anti-submarine warfare weapon known as the Supersonic Missile Assisted Release of Torpedo (SMART) weapon system, which could allow India's navy to engage adversary submarines beyond torpedo range.[77]

5. Monitoring, Manipulation, and Weaponization: A Revolution in Cyber and Information Operations

The final revolution in the framework addresses how emerging digital technologies are changing the competition in cyber and information operations. The importance of cyber, information, and disinformation operations, both as a means to disrupt societies and polities and to undermine the operational efficacy of adversaries, has been discussed at length above.

However, what has not been addressed as thoroughly is the power of modern technologies, especially AI, to amplify the threat to societies and militaries posed by cyber and information operations.

The Internet Observatory Cyber Policy Center at Stanford University noted in a July 2020 report on China's efforts to shape global narratives and influence political situations in Taiwan and Hong Kong that "today's emergent technologies are enhancing those longstanding capabilities, enabling greater velocity and virality, and offering access to new audiences and ways of spreading information."[78]

AI is at the top of the list of "emergent technologies" influencing developments in both traditional cyber warfare and in the future of information operations. Smart bots, fake AI-generated pictures and profiles, and deepfakes are already being used to influence elections, spread misinformation and disinformation, and harden narratives that could serve as part of gray-zone challenges in the region. Technological advances, as well as refinement of operational concepts, are making the AI-enabled disinformation challenge more difficult to detect and counter. A September 2019 study from researchers at the University of Southern California indicates that bots are getting smarter, and that AI-enabled smart bots make it difficult to distinguish social media interactions with humans from those with bots deployed to manipulate, influence, and outrage. According to the report, "bots better aligned with humans' activity trends, suggesting the hypothesis that some bots have grown more sophisticated."[79]

The Confluence of Social Media Monitoring, Manipulation and Weaponization, and Regional Border Tensions

In July 2020, the Indian Army mandated that personnel delete eighty-nine apps from their mobile phones due to operational security concerns. Banned apps included Facebook, Instagram, and fifty-nine with Chinese links. The Indian Army had previously banned use of WhatsApp for official work in November 2019.

Indian concerns over social media activity are layered. There have been cases in the last several years in which Pakistani agents posing as women have convinced military personnel to divulge classified information. Some military personnel have been court martialled for posting sensitive or classified information—for example, the location of a unit—on social networking websites. In addition, the prevalence of Chinese-developed or Chinese-owned apps also reflects a broader information/cybersecurity concern, especially in light of the recent conflict between China and India.[1]

1 "Army asks soldiers, officers to delete Dailyhunt, Facebook and Instagram; uninstall 89 apps", *The Times of India*, 8 July 2020, https://timesofindia.indiatimes.com/india/army-asks-soldiers-officers-to-delete-dailyhunt-facebook-and-instagram-uninstall-89-apps/articleshow/76858779.cms

75 "2020 Force Structure Plan."

76 Kosuke Takahashi, "Japan Aiming to Develop Prototypes of Self-Propelled Mine System," *Janes*, June 23, 2020, https://www.janes.com/defence-news/news-detail/japan-aiming-to-develop-prototypes-of-self-propelled-mine-system.

77 "India Successfully Tests 'Game Changer' SMART Torpedo System," *Times of India*, October 5, 2020, https://timesofindia.indiatimes.com/india/drdo-successfully-flight-tests-weapon-system-smart/articleshow/78489306.cms.

78 Renee Diresta, et al., "Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives," Stanford Internet Observatory Cyber Policy Center, Hoover Institution, July 2020, https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sio-china_story_white_paper-final.pdf.

79 Patrick Tucker, "Twitter Bots Are Becoming More Human-Like: Study," *Defense One*, September 6, 2019, https://www.defenseone.com/technology/2019/09/twitter-bots-are-becoming-more-human-study/159697/.

The deepfake challenge is especially acute and concerning. Deepfake technology is growing more sophisticated as well. Even if it remains relatively easy for deepfakes to be detected visually today, this is unlikely to be the case as the technology behind adversarial examples progresses. Perhaps more concerning, deepfake technology is also proliferating widely and being increasingly incorporated in a range of commercial applications—from marketing and advertising to corporate training—which will almost certainly further their distribution.

The combination of technological advancement and general proliferation has created a growing risk for both localized disruption—including from non-state actors—and, more regionally, affecting strategic instability and insecurity as nations employ the technology to create self-serving or destabilizing alternative realities that either reduce the will of targeted populations to resist coercion or, possibly, affect the realities upon which competitor and adversary military and political leaders make decisions.

A January 2020 report from the Bulletin of Atomic Scientists (BAS) stressed the erosion of truth stemming from AI-enabled disinformation campaigns in particular. According to the report, "The recent emergence of so-called 'deepfakes'—audio and video recordings that are essentially undetectable as false—threatens to further undermine the ability of citizens and decision makers to separate truth from fiction."[80]

The good news, if it can be called that, is that the same technologies that are most useful for designing deepfakes and developing particularly agile and effective malicious code are also being used to help detect these malicious threats, reinforcing the interest of defense and broader security communities in these technologies.

But, meeting the challenge will also require additional non-technological innovations, some of which are already taking place in states across the region as recognition of the threat from cyber operations and disinformation campaigns increases. Australia, India, and Singapore, for example, have all established separate defense-focused organizations dedicated to the cyber threat in the last two years.

In addition, countries like Australia and Singapore—through Total Defence—among others, have dedicated resources to expanding the general public's and commercial industry's understanding of the cyber and disinformation threat. Australia's "Cyber Security Strategy 2020" outlines the country's approach "to keeping families, vulnerable Australians, critical infrastructure providers and business secure online" and notes that the strategy is "for all Australians and Australian business." Like Singapore's Total Defence approach, the document stresses that security in the modern strategic and operational environment is "a whole-of-community effort, in which we all have a role to play."[81]

It also sets aside funds—in total, $1.67 billion—to enhance cybersecurity capabilities to "assist industry to protect themselves and raise the community's understanding of how to be secure online."[82]

IV. Key Takeaways and Implications for Strategy and Policy

The changing strategic and operational environment in the Indo-Pacific is helping to drive accelerating innovation efforts among militaries across the region with a particular focus on:

- capitalizing on the digital transformation enabled by the 4IR to develop novel capabilities that can help defense and security communities anticipate and detect subtle and fast-moving challenges that sit at the junction of military and non-military activities and assets;
- building enhanced situational awareness not just to collect information, but also to process it quickly, and multi-mission capability to develop sufficient agility to quickly respond to disparate threats;
- developing the capacity for a range of military responses—including non-kinetic ones such as electronic attack, cyber weapons, and "soft-kill" directed-energy weapons—that offer militaries the flexibility to respond to both traditional and non-traditional threats and challenges in ways that avoid unnecessary escalation or reduce risk to humans—both military personnel and citizens; and
- enhancing the lethality of military forces, largely as a means of deterring actors—particularly China—and being able to bring decisive force to bear in a high-intensity conflict. While such contingencies are generally believed to be unlikely, the intensifying US-China

80 John Mecklin, ed., "It Is 100 Seconds to Midnight: 2020 Doomsday Clock Statement," *Bulletin of the Atomic Scientists*, January 2020, https://thebulletin.org/doomsday-clock/current-time/.

81 "Australian Cyber Security Strategy 2020."

82 Ibid.