INTELLIGENCE IN A NEW AGE OF WAR

by **CPT Katie Qintan Lin**

ABSTRACT

The new age of war will be an age of robots and automation, of a highly urbanised and interconnected world with blurred boundaries, and of hybrid warfare and terrorism. This essay focuses on three main areas in its exploration of the new landscape of war and the role of intelligence in it: (1) unmanned systems and platforms, (2) hybrid warfare and open-source intelligence, as well as (3) active hunting and persistent sensing. The author highlights that there is a need for the intelligence community to evolve in terms of adopting nascent and unmanned technologies, as well as developing new doctrines or concepts of operation for new domains of intelligence. Only then can timely, accurate and relevant intelligence be provided to the SAF in the future.

Keywords: Artificial Intelligence; Unmanned System; Hybrid Warfare; Information Operations; Revolution in Military Affairs

INTRODUCTION

The face of warfare as we know it is rapidly changing. A new Revolution in Military Affairs (RMA) is taking place, according to many military scholars, and that is the age of robots and Artificial Intelligence (AI).[1] As with the invention of gunpowder, steam ships, tanks and information technology, RMAs are paradigm shifts in the characteristics of warfare that have drastically transformed the way war is waged, driven by game-changing technologies and/or radical war concepts. Aggregated findings indicate that in the future, war will likely be hybrid and cyber in nature, featuring unmanned platforms, satellite systems, advanced sensing systems, and military nanotechnologies.[2] As P.W. Singer puts it, unmanned technologies will not just change how we fight, but who fights in war.[3]

This transformation in warfare is not just driven by unmanned technologies but also by radical concepts in how wars are fought. In 2014, Russia shocked the world by annexing Crimea from Ukraine without a shot fired. Coined hybrid warfare, it is a complex and holistic approach involving cyber attacks, information operations, conventional military posturing, unconventional destabilisation activities, economic pressure and political activities. Hybrid warfare will increasingly become the *de facto* mode of war in the future.[4] This also means that there is now a second battlefront that takes place in virtual reality, where wars of words and codes are fought.

What implications does the future of warfare bring to the domain of intelligence? Traditionally, the role of intelligence is to give timely, accurate and relevant information on the opposing force(s) and conflict environment(s), so that uncertainty is reduced and the best decisions can be made.[5] This essay discusses the implications of a new age of war on intelligence, through exploring three main areas in the new landscape of war: unmanned systems and platforms, hybrid warfare and Open-Source Intelligence (OSINT), as well as active hunting and persistent sensing.

THE NEW AGE OF UNMANNED SYSTEMS AND PLATFORMS

Unmanned systems and platforms are not new; the Predator Unmanned Aerial Vehicle (UAV) had been conducting surveillance and firing missiles back in 2001, shortening the Sense-to-Strike cycle.[6] Other high-altitude long-endurance UAVs bring advantages that manned aircraft cannot achieve, such as the 'Vulture' by the US Defense Advanced Research Project Agency (DARPA) which can stay aloft for five years to provide ultra-persistent surveillance.[7] Fighter drones, such as DARPA's Tactically Exploited Reconnaissance Node (TERN) which can take off and land vertically on small ships, could usher in a new age of 'drone carriers' and consequently even drone warfare.[8] Moving forward, UAVs and Unmanned Combat Aerial Vehicles (UCAVs) would likely move from the man-in-the-loop controller concept (where a human operator controls the drone) and semi-autonomous concept (where machines have AI, but will seek approval before making key decisions) to the autonomous concept, where drones could essentially find, fix, track and engage targets on their own based on pre-programmed parameters.[9] The increasing autonomy of drones paves the way for drones to operate in swarms, networked by advanced tactical datalinks, much like bees. These swarms could take down key anti-air strategic targets deep in enemy territory, sanitise enemy airspace by engaging in air-to-air combat, and provide multi-domain intelligence using a diverse set of sensors spread over a wide area. Future air battles could be decided by huge swarms of weaponised drones.[10]

A photo of UUV REMUS (front) and Seafox (rear) .

The proliferation of unmanned platforms is not just limited to UAVs, but also Unmanned Ground Vehicles (UGVs), Unmanned Surface Vehicles (USVs) and Unmanned Underwater Vehicles (UUVs). UGVs fulfil a diverse range of roles, ranging from Intelligence, Surveillance and Reconnaissance (ISR), urban-terrain mapping and Explosive Ordnance Disposal (EOD) operations, to human detection (possibly even identification) and tracking, and even combat missions.[11] Out in the sea, UUVs are used for mine countermeasure operations, and could even be used for Sense-and-Strike operations, such as Lockheed Martin's submarine-launched unmanned 'subplane' called the Cormorant.[12] The future abounds with possibilities for highly capable and versatile unmanned platforms that can traverse the boundaries between air, land and sea.

What does this mean for intelligence in a future where drones (with far superior ranges and endurance compared to their manned counterparts) can spy covertly and persistently from high altitudes, and operate autonomously in networked swarms to both sense and strike targets? For one, the military that studies, adopts and develops unmanned technologies first would have the first-mover advantage, and would not only drastically increase its edge in ISR capabilities, but also in strike capabilities. Unmanned technologies could greatly augment intelligence collection. UAVs (like the Global Hawk) could greatly increase the range and endurance of airborne ISR collection. Autonomous sensor platforms could be inserted far behind adversarial boundaries to covertly collect intelligence on targets in the depth, while autonomous swarms of nano-drones could be the 'eyes' and 'ears' in hard-to-reach places. However, the simple adoption of unmanned technology will not ensure success; it is the revolution of the whole warfighting and intelligence approach, with the full integration of unmanned systems that will give us the strategic edge. In deciding to shift towards unmanned platforms and systems, the SAF would first have to consider if these would better serve its military strategy, environment and constraints.[13]

Second, organisational structures would have to change to suit the shift to unmanned technologies. When the use of unmanned technologies becomes more prevalent, it becomes inefficient for all unmanned operations to be handled by a single Command. The author proposes that while unmanned strike operations for air, land or sea could be handled by the respective services, unmanned ISR operations could better be handled by the Intelligence community. This also means that respective services or the Intelligence community should have their own drones and pilots for more direct Command and Control (C2) and to develop operation-specific capabilities. Third, the SAF could study and develop technologies that could counter unmanned platforms of adversarial forces, and develop systems that could detect and track UAVs to mitigate the risk of spying by adversarial UAVs or terrorist drones.[14] What we could see in the future might not just be humans as drone operators, but rather as leaders of their individual drone swarms, multiplying both the reach and scale of our forces.

HYBRID WARFARE AND OPEN-SOURCE INTELLIGENCE

Even as armed forces around the world continue to train and plan for conventional warfare, emergent trends indicate that future wars could likely take the form of hybrid and psychological warfare involving cyber attacks and information operations, irregular dispersed warfare involving small clandestine organisations with privatised and miniaturised combat capabilities aided by the diffusion of technology, and even neurological biochemical warfare (involving the use of weapons that act on the nervous system to cause great physical harm).[15] Yet, some continuities will remain—the military will continue to be the state's instrument of policy and limited resources as well as ideological clashes will remain drivers of war. In the face of such changing trends, the best that militaries can do is to understand these trends, adapt, innovate and prepare for the future forms of war.[16]

In hybrid warfare, any combination of Information Operations (IO) and cyber attacks could be used in tandem with other instruments of state such as diplomatic alliances, political manoeuvring and economic pressure. To understand information warfare, information must be viewed as both a weapon and a target. IO activities comprise five core capabilities: Psychological Operations (PSYOPS), Military Deception (MILDEC), Operational Security (OPSEC), Computer Network Operations (CNO), and Electronic Warfare (EW). Offensive IO capabilities may

An Image that shows the core capabilities in Information Operations – Psychological Operations.

take the form of PSYOPS such as misinformation and using traditional mass media (television and radio broadcasts) or social media platforms to influence the opinions and actions of the target audience, or MILDEC activities such as decoys and false 'intelligence' to deliberately mislead adversary military decision makers.[17] We have seen how effective IO or psychological warfare can be—in the 2006 Israeli-Hezbollah War, a guerrilla organisation far inferior in size and technology managed to 'force' a regional power's withdrawal from south Lebanon through PSYOPS, illustrating how 'the pen is mightier than the sword.'[18]

In the cyber domain, cyber attacks are aimed at degrading or disrupting computers, networks and systems whether of the individual, organisation or state. These could take the form of cyber espionage (through illegal exploitation of computers, software or networks), distributed denial-of-service attacks (where the use of networks is denied through data 'flooding'), or data manipulation or sabotage (through malware). Much resources and research would have to be undertaken to develop measures or infrastructure to counter cyber attacks. In fact, the more 'electronically dependent' a state is, the more vulnerable it is to cyber attacks.[19]

In hybrid warfare, any combination of Information Operations and cyber attacks could be used in tandem with other instruments of state such as diplomatic alliances, political manoeuvring and economic pressure.

Yet, while the Information Age brings many new threats, it also presents the intelligence community with new collection opportunities. First, OSINT is a growing domain with huge potential, considering the wealth of information readily available on the Internet and social media platforms; it can cross-cue and enhance conventional intelligence collection from closed sources. However, with the prevalence of misinformation online, the quality of actionable intelligence derived from OSINT depends greatly on the quality of analysis.[20] Many open-source tools are available for both collection and big-data analysis; some

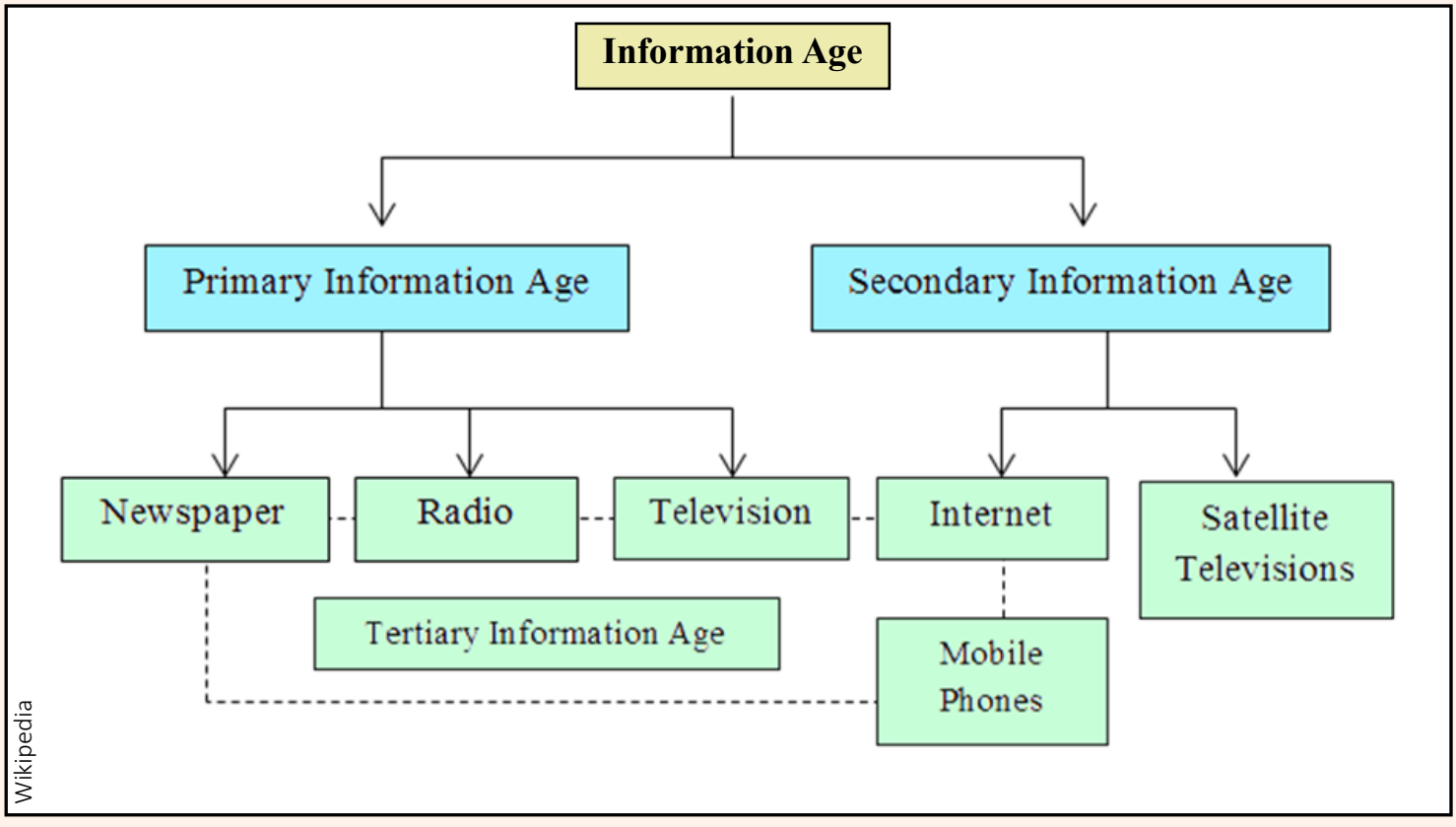
tools map social networks and relationships, while others track and identify people as well as map out places based on geo-tagging of social media posts.[21] Social media is ultimately as much about the meta data as it is about what is said and shown. With the huge amounts of aggregated data to sift through, the author believes that acquiring the right open-source tools becomes even more crucial in ensuring expeditious data collection and analysis to produce useful intelligence.

Second, along with the rise of OSINT comes the nascent field of Digital Forensic Intelligence (DFINT). Everyone leaves a permanent but invisible digital trail, which can be exploited for the tracking of individuals and the collection of private data such as that retrieved from mobile phones. Currently, there are already solutions to extract and analyse data retrieved from mobile phones.[22] One can imagine the use of such digital data extraction solutions in conjunction with unmanned remote-sensing platforms or Human Intelligence (HUMINT) operatives as a possible mode of intelligence collection in the future. As misinformation campaigns become more prevalent, digital forensics also becomes increasingly important in discerning and uncovering truth from lies, by analysing the invisible digital trail of what we see and hear. In sum, the author believes that the in-depth analysis of open-source and social media data as well as its meta data, using the appropriate tools, would be pivotal in giving the intelligence community an edge in the age of hybrid and information warfare.

Yet, while the Information Age brings many new threats, it also presents the intelligence community with new collection opportunities.

ACTIVE HUNTING AND PERSISTENT SENSING

In the new age of war—replete with stealthy unmanned platforms, how can the intelligence community keep up to provide timely, accurate and relevant information to military decision-makers? No longer can intelligence practitioners rely on opportunistic collection of adversarial forces and platforms. With the advent of stealth technology and a military's inherent tendency to conceal its forces for the element of strategic surprise, windows of opportunity for detection are getting smaller. The author proposes for intelligence collection to take on a more active role—akin to hunting—rather than the more passive method of planning routine collection over a probable Area of Operations (AO). To hunt for the target, we have to develop sensing capabilities that can detect stealth platforms as well as concealed targets. This involves as much creative thinking-out-of-the-box as it does futuristic technology. Active hunting is about seeking the hidden. In other words, future Imagery Intelligence (IMINT)



A graph showing the three stages of the Information Age.

should be more than imaging what is already in the light; it should also be about bringing the hidden to light.

First, one way to detect stealth platforms is to invest in counter-stealth technologies such as certain advanced passive radar systems (which use bearing-range triangulation from multiple receivers), Ultra High Frequency (UHF) L-band radars, passive listening systems, and millimetre wave imaging (using naturally-emitted radiometric signatures).[23] Another way to detect stealth platforms is to establish a comprehensive wireless network of unmanned sensors which could be persistently stationed around land, maritime and airspace boundary lines.[24] In other words, we cast semi-permanent 'sensor-nets' that can provide persistent surveillance, border-intrusion detection and even automated target classification.[25] Such systems could be useful in the detection of submerged submarines, particularly for countries with smaller maritime territorial boundaries (such as Singapore) or places with chokepoints (such as the entrances to the Singapore Straits and Straits of Malacca). As stealth technology becomes cheaper and militaries replace ageing platforms in the foreseeable future, stealth platforms could become more commonplace, necessitating the use of counter-stealth detection methods by the intelligence community.

Second, it is increasingly imperative that the intelligence community be able to detect and track targets that are concealed by walls, buildings, foliage or water (such as underwater targets). One way is to continue pushing technology to the limits, to see through walls and underwater. Emerging wall-penetrating technologies include the Low-Frequency Synthetic Aperture Radar (SAR) by Airbus, which can be mounted on airborne platforms to image through walls from stand-off ranges, as well as laser radar-based vibrometry, which remotely measures the vibrations on structures or the ground to detect concealed targets.[26]

To image targets obscured by foliage, foliage-penetrating SAR instruments have typically used lower frequency bands (such as P band), but the associated imaging range and resolution do not enable target recognition. More recently, radars like Lockheed Martin's foliage-penetrating reconnaissance radar can even detect slow-moving troops or vehicles through trees.[27]

In the area of detecting and imaging underwater targets such as submerged submarines, technologies, while still in nascent stages, are promising. Terahertz imaging—used in food analysis and medical imaging due to its sensitivity to water content—could be adapted for submarine detection once solutions to circumvent its short range are developed.[28] More extensive research into blue-green Lasers (explored for submarine communications), Light Detection and Ranging (LIDAR) and Infra-Red (IR) Wake Detection could yield results that offer game-changing solutions to the cat-and-mouse game of submarine detection.[29]

Another way to image what has been previously thought impossible is to look at the problem in a different way. For instance, to image targets in the depth obscured by foliage, swarms of nanobots—nearly imperceptible when they travel alone—could intrude deep into adversarial territory, converge again when one of them detects a target (in the absence of observers) to image it, and separate again en route to its next mission. These swarms could also image underground facilities and bunkers, or inside buildings.[30]

Third, persistent sensing should be an area of focus for the intelligence community. We can have persistent 'eyes' on high-value targets through various means. One way is through biomimicry—the use of robots camouflaged as elements of nature such as insects of birds. While biomimicry can present great advantages such as self-healing armour and dynamic camouflage to the military by modelling animal biology, the greatest advantage of biomimicry to the intelligence community would perhaps be the ability to collect covert and persistent multi-domain intelligence at stand-in ranges in adversarial territory.[31] The sensing platform could take the form of a 'bird' perched high up in a tree, or even a cluster of 'cockroaches'—much can be left to the imagination.

Another way to have persistent sensing capabilities is to exploit the Internet-of-Things (IoT) of Closed-Circuit Television (CCTV). Given the prevalence of CCTVs installed all over the world, the ability to exploit the IoT of CCTV to obtain footages would be a huge step up for the domain of IMINT. At the same time, we must extensively study the vulnerabilities in our CCTV systems to mitigate risks of hacking.[32] But, aside from the challenge of exploiting the IoT of CCTV in unauthorised areas without being detected, the greater challenge lies in being able to detect targets of interest in the ocean of data obtained, without knowing what we are specifically looking for. This is the reason why CCTV is mostly used in the identification of suspects after a crime, not in the prevention of the crime itself. Nonetheless, CCTV offers us millions of 'eyes on target' and plenty of surveillance opportunities, be it for counter-terrorism, military defence, or monitoring of adversarial targets.

CONCLUSION

With the RMA of unmanned technology set in motion, the future shape of war will be drastically different. The intelligence community will have to evolve in anticipation of the changing battlefield and the way wars

will be fought. It is only by staying ahead of changes and developments that our intelligence community can provide the SAF with the strategic edge, through the provision of timely, accurate and relevant intelligence.

As explored in this essay, unmanned platforms and systems offer unprecedented opportunities for intelligence collection. UAVs could provide ultra-persistent surveillance and shorten the Sense-to-Strike cycle, while versatile unmanned sensors could be submarine-launched or drone-inserted deep into adversarial territory for covert ISR collection. Autonomous swarms of small drones could provide real-time multi-domain intelligence covering wide expanses of hard-to-reach areas such as underground spaces and military installations, or under foliage in the depths.

The Information Age offers us new domains of intelligence to be exploited, even as it is seen to be the harbinger of hybrid, cyber and information warfare. Yet, to truly capitalise on OSINT and DFINT, not only must we not spare resources to obtain or develop the right tools, we must also update our doctrines, concepts of operations, and processes, as well as properly train intelligence practitioners in these new methods of collection.

The Information Age offers us new domains of intelligence to be exploited, even as it is seen to be the harbinger of hybrid, cyber and information warfare.

Finally, the way we approach intelligence collection must change as well, from a more passive process of opportunistic and routine collection based on the probable AO of targets, to an active hunting process. It does not suffice to just hunt for targets; it is also about what we hunt—the 'invisible'—and how we hunt, in ways least expected by our adversaries.

Ultimately, the intelligence community that will have the strategic edge in the new age of war is one that dares to dream and to change—one that embraces new technologies and generates radical solutions. And it is the hope of the author that the SAF's intelligence community will be precisely that—an intelligence community leading the way into the future.

ENDNOTES

1. Singer, P.W. *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. New York City, NY: Penguin Books (2009).
2. Burmaoglu, Serhat, and Saritas, Ozcan. "Changing characteristics of warfare and the future of Military R&D," *Technological Forecasting & Social Change*, no. 116 (2017): 151-161.
3. Singer, P.W. *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. New York City, NY: Penguin Books (2009).
4. Barber, Nicholas. "A warning from the Crimea: hybrid warfare and the challenge for the ADF," *Australian Defence Force Journal*, no. 201 (2017): 46-58.
5. Clapper, James R. Jr. "Challenging Joint Military Intelligence," *Joint Force Quarterly,* Spring (1994): 92-99.
6. Whittle, Richard. "The Man Who Invented the Predator," *Air & Space Magazine* online. Last modified April, 2013. https://www.airspacemag.com/flight-today/the-man-who-invented-the-predator-3970502/?all
7. "DARPA's Vulture: What Goes Up, Needn't Come Down." *Defense Industry Daily* online. Last modified September 16, 2010. https://www.defenseindustrydaily.com/DARPAs-Vulture-What-Goes-Up-Neednt-Come-Down-04852/
8. Atherton, Kelsey D. "DARPA Wants To Turn Small Ships Into Drone Aircraft Carriers." *Popular Science* online. Last modified December 30, 2015. https://www.popsci.com/darpa-wants-more-navy-ships-to-carry-drones

   Shugart, Thomas. "Build All-UAV Carriers." *U.S. Naval Institute Proceedings Magazine* online. Last modified September, 2017. https://www.usni.org/magazines/proceedings/2017-09/build-all-uav-carriers
9. Rogoway, Tyler. "The Alarming Case of the USAF's Mysteriously Missing Unmanned Combat Air Vehicles." *The War Zone* online. Last modified June 9, 2016. http://www.thedrive.com/the-war-zone/3889/the-alarming-case-of-the-usafs-mysteriously-missing-unmanned-combat-air-vehicles

10. Hambling, David. *Swarm Troopers: How Small Drones Will Conquer the World*. Venice, FL: Archangel Ink (2015).

11. Nguyen, Hoa G. et al. "Land, sea, and air unmanned systems research and development at SPAWAR Systems Centre Pacific." *SPIE Proceedings: Unmanned Systems Technology XI*, vol. 7332 (May 1, 2009). doi: 10.1117/12.818994

12. Sweetman, Bill. "The Navy's Swimming Spy Plane." *Popular Science* online. Last modified February 21, 2006. https://www.popsci.com/military-aviation-space/article/2006-02/navys-swimming-spy-plane

13. Fowler, Mike. "The Strategy of Drone Warfare." *Journal of Strategic Security* 7, no. 4 (2014): 108-119.

14. Ganti, Sai R and Kim, Yoohwan. "Implementation of detection and tracking mechanism for small UAS." In *2016 International Conference on Unmanned Aircraft Systems (ICUAS),* Arlington, VA, USA (June 7-10, 2016). doi: 10.1109/ICUAS.2016.7502513

15. Johnson, Robert A. "Predicting Future War." *Parameters* 44, no. 1 (Spring 2014): 65-76.

16. Giordano, James. "The Future of Warfare and the Responsibilities of Today's Brain Science." *Human Brain Project* online. Last modified May 11, 2017. https://www.humanbrainproject.eu/en/follow-hbp/news/the-future-of-warfare-and-the-responsibilities-of-todays-brain-science/

17. Wilson, Clay. "Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues." *CRS Report for Congress* (March 20, 2007).

18. Schleifer, Ron. "Psychological Operations: A New Variation on an Age Old Art: Hezbollah versus Israel." *Studies in Conflict & Terrorism* 29, no. 1, (2006): 1-19.

19. Nguyen, Nam. "Evolution of the Battlefield: strategic and legal challenges to developing an effective cyber warfare policy." *Australian Defence Force Journal,* no. 196 (2015): 60-69.

20. Gibson, Stevyn. "Open source intelligence: An intelligence lifeline." *The RUSI Journal* 149, no. 1 (2004): 16-22.

21. Batrinca, Bogdan, and Treleaven, Philip C. "Social media analytics: a survey of techniques, tools and platforms." *AI & Society* 30*,* no. 1 (2015): 89-116.

22. Quick, Darren, and Choo, Raymond Kim-Kwang. "Pervasive social networking forensics: Intelligence and evidence from mobile device extracts." *Journal of Network and Computer Applications,* no. 86 (2017): 24-33.

23. Westra, Arenda G. "Radar versus stealth: Passive radar and the future of US military power." *Joint Force Quarterly,* no. 55 (2009): 136-143.

24. Felemban, Emad. "Advanced Border Intrusion Detection and Surveillance Using Wireless Sensor Network Technology." *International Journal of Communications, Network and System Sciences,* no. 6 (2013): 251-259.

25. Baker, C.J., and Hume, A.L. "Netted radar sensing." *IEEE Aerospace and Electronic Systems Magazine* 18, no. 2 (2003): 3-6.

26. Doody, S.G. et al. "Low Frequency Synthetic Aperture Radar Data-Dome Collection with the Bright Sapphire II Instrument." *NATO Science and Technology Organization Meeting Proceedings* (May 2, 2017). doi: 10.14339/STO-MP-SET-247-03-PDF

    Lutzmann, P. et al. "Potential of Remote Laser Vibration Sensing for Military Applications." *NATO Science and Technology Organization Meeting Proceedings* (Dec 23, 2004). doi: 10.14339/RTO-MP-SCI-145-24-pdf

27. "Lockheed Martin Foliage-Penetrating Reconnaissance Radar Integrated with System to Detect Slow Moving Objects." *Lockheed Martin*, October 23, 2012. https://www.lockheedmartin.com/us/news/press-releases/2012/october/isgs-sar-gmti-1023.html

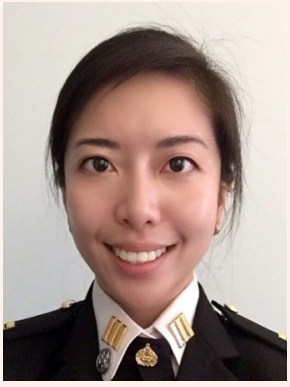
28. Ergün, Salih, and Sönmez, Selçuk. "Terahertz technology for military applications." *Journal of Military and Information Science* 3, no. 1 (2015): 13-16.

29. "Technologies and Anti-Submarine Warfare." *British Pugwash* online, last modified July, 2016. http://britishpugwash.org/wp/wp-content/uploads/2016/07/Read-a-selection.pdf

30. Kladitis, Paul E. "How Small Is Too Small? Technology into 2035." In *The Wright Flyer Papers,* no. 46. Maxwell AFB, AL, USA: Air Command and Staff College (2010).

31. Phua, Charles Chao Rong, and Seah, Calvin Ser Thong. "Learning from Mother Nature: 'Biomimicry' for the next-generation armed forces." *Pointer* 41*,* no. 1 (2014): 1-11.

32. Costin, Andrei. "Security of CCTV and video surveillance systems: threats, vulnerabilities, attacks, and mitigations." In *Proceedings of the 6th International Workshop on Trustworthy Embedded Devices* (2016): 45-54.



CPT Katie Qintan Lin is currently an Officer Commanding (OC) in Imagery Support Group, C4I. A Naval officer by vocation, CPT Katie has served in the SAF Information Group in Joint Operations Department, as well as the Navy Information Centre in Naval Operation Department. She graduated from the University of Pennsylvania with a Masters of Science (Education) in Counselling, as well as a Bachelors of Arts in Psychology *(manga cum laude) with honours*.