Technologies in Hybrid Warfare: Challenges and Opportunities

by **ME6 Gabriel Tham, CPT Edward Wong & ME4 Kelvin Kuo Kai Ming**

Abstract:

In recent years, hybrid warfare has become increasingly widespread, comprising various conventional and non-conventional means of warfare, as well as non-military options. While technological progress will generate more opportunities, it can also bring about threats to a country. For instance, drone-related technologies pose a sizeable threat due to their accessibility and low cost, enabling mass production and swarm tactics. For Singapore, the Republic of Singapore Air Force (RSAF) will also have to consider methods of minimising collateral damage in air strikes, to alert civilians to impending air strikes, although such technologies are not without limitations. Electromagnetic Pulse (EMP) weapons also pose a significant threat to Singapore, and to combat these, the RSAF can choose to employ active or passive systems. Ultimately, continual technological development is essential for the RSAF to maintain its edge over potential aggressors.

Keywords: Hybrid Warfare, Technology, Drones, Collateral Damage, Weapons of Mass Destruction

INTRODUCTION

Hybrid warfare has attracted the attention of many militaries across the world, especially with the rise of global terrorism and the increasing reluctance of countries to participate in full-scale conflicts. Past conflicts between Israel and Hezbollah to more recent ones such as the annexation of Crimea all saw the use of hybrid warfare. Hybrid warfare comprises a mixture of traditional military maneuvers and confrontations, non-conventional methods such as guerrilla and cyber warfare, and even non-military options such as economic strangulation aimed to weaken an opponent's political and social will. Similar to many other military developments throughout history, technology continues to shape and evolve military strategies and tactics. The face of hybrid warfare will therefore continue to change as technology advances. This essay aims to explore some key trends in hybrid warfare, and look at how technology can provide opportunities as well as pose threats to the RSAF. It will also discuss some of the possible technologies that the RSAF can explore to overcome challenges associated with hybrid warfare.

CHALLENGE #1: RAPID DEVELOPMENT OF COMMERCIAL DRONES – A NEW THREAT FOR AIR FORCES

While countries pursued military technological advancements to gain a capability edge over potential adversaries in the past, rapid development of commercial technologies and the accompanying low-cost options now pose new challenges to the military. Advancements in the fields of robotics, artificial intelligence, additive manufacturing and nano-materials have not only shortened the product development cycle but have also given rise to a whole range of low-cost, yet effective military options.[1] The availability of low-cost commercial technologies provides an affordable means for militaries to rapidly assimilate these new technologies and evolve their fighting concepts and tactics. On top of that, the use of these low-cost technologies can enable the underdog to overturn capability asymmetry, sometimes forcing their enemies to follow in terms of adapting low-cost technologies in their fighting systems.[2] It is however challenging to do this while having to keep the capability edge in conventional war. Hence, to adapt some of their conventional capabilities, countries would end up investing heavily in adapting or developing their weapons systems to overcome the new threats.

While countries pursued military technological advancements to gain a capability edge over potential adversaries in the past, rapid development of commercial technologies and the accompanying low-cost options now pose new challenges to the military.

There has been an enormous growth in the field of commercial unmanned systems over the past decade. Fully autonomous, cheap and long-range drones have emerged in the mass market for recreational applications. Some recent technological developments in commercial drones have raised several concerns amongst militaries across the globe. First, since they are designed for the mass market, these unmanned systems are relatively low in cost, easily available and easy to use. With their composite construction and very low energy usage, they will be very difficult to detect. Of even greater concern, these small, inexpensive drones are designed to be operated by people with little or no specialised skills and in-house maintenance capabilities. Once equipped with a small explosive payload, it could prove difficult to detect and defend against such weapons of terror. Second, they are becoming increasingly smart. The autonomy of commercial drones is improving as they are equipped with smart technologies such as sensors, advanced navigation systems with GPS, powerful microprocessors, digitally encrypted controls and communications.[3] Non-state actors can now easily produce cheap, smart and deadly drones that could operate co-operatively in swarm tactics to saturate and overwhelm a military air defence.

Last but not least, these drones are becoming cheaper. With additive manufacturing, the cost of manufacturing customised high-end drones will go down. Recently, researchers in England have prototyped a printed drone that will cost roughly $9 a copy. This drastically opens the access of inexpensive high end drones to both state and non-state actors. For example, the Chinese have fielded the Harpy Unmanned Combat Air Vehicle (UCAV). Initially developed in the 1990s by Israel as an anti-radar system, the Chinese version has a range of 500 km and a 32kg warhead with multiple types of seeker heads. One Chinese configuration has 18 Harpies in box launchers mounted on a single truck bed (other configurations use 6 launchers per truck).[4] Essentially, these are expendable drones capable of saturating defensive systems. This system represents a first step towards inexpensive swarms.

There are many ways that these commercial drones could be used and become a threat to the Air Force. The most obvious is to use these drones as a weapon. Without the need for sophisticated navigation systems or target recognition, these autonomous drones can easily fly a pre-programmed route to a target area and inflict damage on any of the designated targets.

Example of a Commercial Unmanned Aerial Vehicle that could be used as an airborne obstacle

Navigation could be done through GPS or Google Maps, and cheap and commercially available optical recognition hardware and software would provide rough targeting. Commercially available quadcopters, which are able to carry loads such as a GoPro camera weighing 100g and with endurance of over 30 minutes, could easily be modified for military use. In the past, skilled machinists with high-quality machine tools were required to equip commercial drones with explosively formed penetrators (EFPs). However, in the last few years, additive manufacturing has advanced to the point where such EFPs could be 'printed'.

For Air Forces, this approach poses a major threat to the air power generation. Instead of engaging in an air campaign, the adversary could send hundreds or even thousands of small drones after each aircraft at its home base. Larger-sized support aircraft, such as tankers, airborne early warning and control aircraft (AWACs), and transports, are even more vulnerable to this form of attack. If drones were equipped with larger explosives, aircraft protected by shelters, radars, fuel systems and ammunition dumps could be vulnerable too. The massive deployment of these drones could even hinder the launch capabilities of the Air Force. Acting as airborne obstacles, these drones could effectively create a blockage over any airfield.

Anti-Drone Technologies

To overcome the threats posed by commercial drones, Air Forces will need to invest in anti-drone technologies. Many technologies have emerged to overcome the challenges posed by commercial drones. In order to effectively deal with this new threat, technologies to detect and then terminate these drones are required. Detecting these commercial drones is quite difficult, especially in a busy urban environment. These small and slow-moving drones render traditional radar and imaging technologies ineffective.[5] To overcome this, some anti-drone systems use composite radar and imaging techniques to detect incoming drones. The Sky Archer Counter Micro-UAV System, primarily uses a visual detection system but can be upgraded with radar to enhance detection. A system is being developed by Singapore Technologies Electronics which would allow users to watch over specific areas where UAVs are not permitted.[6] Newer technologies that leverage on acoustics are also being explored. The DroneShield system is one such solution that centres on detecting, identifying and locating an incoming drone based on the sound it makes. The system will run every sound it hears through a library which contains the noises made by different types of drones. If a match is found, it can alert a human operator to confirm and track the incoming drone.

After detection, the termination or disabling of these drones could be done in a few ways. The most popular approach currently is to disable the drone through radio frequency jamming. The most rudimentary method is to flood the radio frequency band that the drone is operating in. This will disrupt the connection between the controller and the drone, making the drone uncontrollable and ultimately causing it to crash. However, modern commercial drones employ spread spectrum communications, making it difficult to jam the control frequencies. Other more elegant methods such as GPS spoofing or hacking into the drone's control systems are being developed. Another approach to disable a drone requires a physical net to be deployed onto the drone. Systems such as Skywall by OpenWorks Engineering and MP200 by MALOU Technologies use propelled or drone-carried nets to take down any hostile drones. However, this approach requires training and specialised skills and may not be effective when dealing with a saturation attack by a swarm of autonomous drones.

Directed-Energy Weapon (DEW) – A Means to Overcome Drone Saturation

To overcome a swarm of autonomous drones, the traditional means of jamming each drone or shooting them down with a physical net is no longer effective. The rise of low cost drones has enabled the mass deployment of autonomous drones, particularly by state actors aiming to use unconventional means to wage hybrid warfare. Directed-Energy Weapons (DEW) provide a low cost means to overcome such attacks. One such system is Lockheed Martin's newly developed Athena (Advanced Test High Energy Asset) weapon, which uses a 30-kilowatt fibre laser.[7] It was tested against a small Phantom quadcopter drone's engine and camera with precision at over a kilometre away. The system is capable of creating a hole through five-centimetre thick steel, such as that of the engine of a truck, in seconds. Most importantly, each shot cost less than a dollar. The cost-efficiency of such counter-measures is critical when dealing with application of drone swarm. DEWs have applications that extend beyond commercial drones; they also provide a cost-effective defence against rockets and can replace expensive missiles. Compared to the Iron Dome used by the Israel Defense Forces (IDF) which costs around $20k per interception, DEW provides a much cheaper alternative to combat short-range rockets fired by Hamas and Hezbollah. Past lasers were inefficient because of their large size, large power demand and inability to cool. However, with advancements in laser technology, these shortcomings were mitigated and lasers became viable weapons in the directed energy arsenal. For example, Boeing has developed the (BA) YAL-1 Airborne Laser, a megawatt chemical laser system built in 2002 that can be mounted inside a modified Boeing 747. With the advancement in DEW technologies, we can expect to see more of such systems deployed in airborne platforms.

CHALLENGE #2: INCREASED DIFFICULTY FOR AIR STRIKE OPERATIONS IN DENSELY POPULATED ENVIRONMENT

When the adversary is inferior, either in terms of military capability, size or technology, it may choose to employ non-conventional means to overcome this asymmetry. The adversary will leverage on any advantage it can attain to mitigate the advantage its enemy has in conventional warfare. In some instances, it could hide among civilian infrastructure that should not be targeted by conventional military actions, such as schools, hospitals or religious buildings, and adopt such civilian infrastructure as its headquarters or staging areas for military operations. This makes it difficult for conventional militaries to execute their mission while trying to comply with international agreements such as the Geneva Conventions. The Geneva Convention states that:

> *"The presence or movements of the civilian population or individual civilians shall not be used to render certain points or areas immune from military operations, in particular in attempts to shield military objectives from attacks or to shield, favour or impede military operations. The parties to the conflict shall not direct the movement of the civilian population or individual civilians in order to attempt to shield military objectives from attacks or to shield military operations."*[8]

These scenarios present a 'Catch-22' for militaries between neutralising the threat with possible civilian casualties and inaction that could lead to more friendly casualties. The Gaza–Israel conflict is one such example. Hamas fighters understand the restrictions most conventional militaries have. Knowing that places of worship, residences and hospitals can easily be reckoned as illegitimate military targets in the eyes of the world, they purposely used these places as weapon caches, shelters for military personnel, concealed tunnels and command posts. The IDF was then forced to make difficult decisions of whether to conduct air strikes on these civilian buildings, many of which were even schools, hospitals and mosques within Gaza.[9] In fact, there were instances of IDF intelligence clearing a target for an air strike, only to find that the battle damage assessment showed no signs of Hamas militants.[10] It is very likely that the militants escaped through their network of tunnels. Not only did Hamas take advantage of the protection that these places provided, they also exploited the resultant collateral damages from the IDF air strikes and raised dissent in the war-torn people against the IDF.[11]

When the adversary is inferior, either in terms of military capability, size or technology, it may choose to employ non-conventional means to overcome this asymmetry.

In densely-populated Gaza, where there are almost two million people within an area of 380 square kilometres, the fear of inflicting collateral damage remains despite advancements in precision munitions. Regardless of the enhanced precision, any effective munitions required to destroy the enemy's weapons cache or command posts would still have a certain blast radius, thus still affecting population around the target. With the enemy hiding in the midst of civilians, launching rockets into Israel and quickly finding cover back among the masses of densely populated residential area, the IDF found it challenging to be effective in the execution of their air strikes.

Wreckage resulting from an air strike in densely-populated Gaza

'Knock On Roof' – Integration of Commercial-Military Technologies

In order to minimise civilian casualties in the conduct of precision air strikes, the IDF adopted a 'Knock on Roof' concept. Phone calls or Short Message Service (SMS) was first sent to potential targets.[12] Subsequently, a dummy missile with little to no explosive load would be dropped at the targeted building, the actual 'Roof Knock', informing building inhabitants of the imminent air strike.[13] Finally, an actual bomb would strike the target, taking out the enemy's weapons cache or command posts. The IDF hoped that this approach would provide Gaza civilians with an adequate warning to react to the incoming air strike. The IDF also claimed that it conducted persistent Intelligence, Surveillance and Reconnaissance on these targeted buildings to understand how many people were in the buildings at any one time, allowing them to conduct accurate assessments of the number of residents present.

It is not clear how the IDF delivered the warning calls and SMS to unknown phone numbers, but the attributes are similar to commercial Cellular Broadcast technologies. For example, Alcatel-Lucent developed the Broadcast Message Centre (BMC) to send text alerts to mobile users based on their geographic location. The BMC was initially developed to broadcast warnings to locations, which could be experiencing a gas leak, chemical spillage or natural disaster, thereby providing early notice for evacuation. BMC works through cellular network and infrastructure where the requestor first sends a required message to an alert gateway. This is relayed to the BMC, which delivers the messages to the respective carriers to broadcast the message to phones within the allocated area.[14]

Long Range Acoustic Device – An Alternative to 'Roof Knock'

However, the 'Knock on Roof' concept has its limitations. The warnings before an actual air strike may not be effective. The 'Roof Knock' is essentially still a munition—albeit without the explosives—and is still capable of causing damage on unstable roof structures. In some cases, the 'Roof Knock' caused damage to the building or people inside before the actual strike occurred.[15] In addition, it is still subject to the same errors of a live strike. A typical bomb guidance unit has a Circular Error Probability (CEP) of 5 to 30m. This CEP in the context of a dense, urban environment could translate to potential misses of the intended target. Also, 'Roof Knock' could easily be mistaken for another nearby explosion, causing residents to disregard these warning shots. Even phone calls or SMS could be easily missed, rendering it difficult to ensure effective warning.

While phone calls or 'Roof Knock' may not provide enough coaxing for residents to evacuate a building that has become an imminent target, Long Range Acoustic Device (LRAD) could potentially be a viable alternative in the future. LRAD is able to create a directed blast of high volume sound waves, which are irritating, loud and potentially painful, over long distances. The military-grade LRAD 2000X can transmit voice commands up to 162 decibels (dB) with a range up to nine kms away.[16] LRAD would be able to provide a more effective Roof Knock as there would be no ambiguity of where the noise is coming from and this could reduce errors inherent to dropping aerial munitions. If directed voice commands are not 'persuasive' enough, LRAD could apply increased power to 'encourage' residents to vacate a building. Human discomfort begins when sounds increase past 120dB. LRADs have recently been used in the Ferguson riots in Missouri, USA as a method of crowd control.[17]

Long Range Acoustic Device capable of producing directed blasts of high volume sound waves.

CHALLENGE #3: EMERGENCE OF CHEAP AND ACCESSIBLE WEAPONS OF MASS DESTRUCTION

Traditional Weapons of Mass Destructions (WMD), including biological, nuclear or chemical weapons have become less acceptable to be used in view of the inhumane effects they bring on both their human targets and the environment. These weapons not only have the ability to wipe out whole cities or states but also have the prolonged ill-effect of rendering the area unusable by enemy forces. Therefore, in the past, WMDs were employed mainly by terrorist organisations that aimed to strike fear in a population or by state actors who utilised them as a last resort. However, modern technologies have brought about a new range of WMDs. Besides cyber warfare that could wreak disasters on national infrastructure such as power, water or transportation, another such means is Electromagnetic Pulse (EMP) weapons.

EMP weapons will provide potential adversaries with an avenue of initial attack, without the remaining ill-effects of a nuclear strike

Electromagnetic Pulse Weapons

Nuclear weapons have been around since World War II (WWII), and the most well-known employment was by the United States (US) on Nagasaki and Hiroshima leading up to the eventual Japanese surrender. 'Fat Man' and 'Little Boy' were aerially dropped. Employment of these weapons has become more diverse since then. Though the majority of a nuclear weapon's destruction is caused by very high temperatures and pressures coupled with an expanding shockwave, there is also damage caused by an accompanying EMP. For example, during nuclear weapons testing in 1962, codenamed Starfish Prime, a 1.4 megaton warhead which detonated 386 km above the earth was launched from Johnson Island in Ohio, USA. The EMP from this weapon was strong enough to affect the electrical grid in Hawaii 1148km away, resulting in blown streetlights, telephone outages and radio blackouts.[18]

EMP weapons will provide potential adversaries with an avenue of initial attack, without the remaining ill-effects of a nuclear strike. Compared to the requisite knowledge to develop a full atomic weapon, developing an EMP weapon requires relatively less know-how. With the ability to cripple city networks without the adverse effects of nuclear fall-out and destruction, EMP weapons would be attractive to state and non-state actors in hybrid warfare. Many countries have started developments of a kamikaze drone. These will be employed during time critical missions where the operator will acquire the target before the drone strikes and explodes itself. Kamikaze drones such as the Harop by Israel Aerospace Industries and AeroVironment's Switchblade can be armed with an EMP payload to deliver the first blow to an adversary.[19] As demonstrated by nuclear tests, even small yield nuclear weapons may have big EMP ramifications. Radars, aircraft and air defence systems could easily be disabled within the first blow and would no longer be useful for the rest of the air campaign.

EMP weapons also provide militaries with more surgical strike options. Since EMP weapons are only effective against electronics, they provide a means to knock out an opponent's command posts and weapons systems without the fear of causing civilian casualties. The United States Air Force has recently modified cruise missiles to carry a high-powered energy weapon. This missile can be set with a pre-determined flight path and is able to send up to 100 microwave pulses, which could short electronics on the ground.[20] The use of EMP weapons does face some challenges. Operating in environments where friendly ground troops are in forward-deployed positions would enforce limitations. Frying friendly communications, and weaponry in some cases, could prove fatal to troops on the ground.

Closer to home, EMP weapons can threaten our very way of life. Should an EMP be detonated nearby, it would leave Singapore without electricity, communications, transportation, fuel, food or even running water. The fact that Singapore is a small island state makes it geographically even more susceptible to EMP weapons as they could affect the country's entire electrical grid, taking months or even years to rectify.[21] The RSAF can also be vulnerable to an EMP attack as aircraft, Ground-based Air Defence systems, radars and UAVs all make up the RSAF's order of battle, none of which are absolved of the EMP threat in view of their reliance on electronic systems. The RSAF must be conscious of the threat and employ the necessary defensive measures to ensure the safety of Singapore's skies.

PASSIVE AND ACTIVE DEFENCE AGAINST EMP WEAPONS

Passive defences could be employed to guard electronic systems from the EMP pulses produced by low-yield Hydrogen bombs. The concept of a Faraday cage is by no means new technology (as it was invented by Michael Faraday in 1836) and can be applied to defend against EMP attacks.[22] Ground-based critical systems such as radars, servers and operations nodes as well as aircraft hangars are typically hardened against kinetic munitions and the hardened facilities can be easily improved with a simple Faraday cage to provide a passive, last-layer defence against EMP weapons.

Second successful launch of the Arrow-3 interceptor in January 2014.

However, it is not enough to rely solely on passive systems. The deadliness of high-altitude nuclear attacks is largely proportional to the altitude at which they are detonated. As such, an early-warning, missile-interception system that could prevent such a missile from reaching critical altitude could be adapted to target EMP missiles. Long range systems such as the Israeli Arrow would be able to undertake high altitude interceptions at long ranges, effectively covering a wide swath of airspace. The Arrow-3 has a range of 90km and maximum altitude of 50km. This is significant upgrade to Israel's Patriot PAC-2 local missile defence system which has a range of 40km.[23]

CONCLUSION

Whether by addressing threats such as commercially-available drones or operating in densely-populated environments, hybrid warfare poses several new challenges to the RSAF. The rise of commercial drones, being cheaper and smarter, provides opportunities for the RSAF to employ swarm techniques. However, the fact that such technology is equally-accessible to non-state actors or adversaries of lower technological capability poses new challenges to the RSAF. These drones can now be used as cheap weapons or even co-operatively operated to hinder launch and recovery operations. As the defence and security industries develop new technologies in the detection and termination of these drones, the RSAF will need to explore low cost options such as DEW to overcome potential saturation attacks by a swarm of low-cost drones.

Even with increased precision, air strikes will increasingly become more difficult as we fight in a more densely-populated environment. The enemy is expected to take cover in populous areas, making it difficult to conduct air strikes without collateral damage and civilian casualties. While the IDF developed a 'Knock on Roof' concept, it had limited success. New technologies that leverage commercial communications as well as specialised systems such as LRAD can be used to overcome some of the challenges.

Finally, the RSAF will need to closely monitor the development of EMP weapons, which can be very effective against the electronics and networked systems in any Air Force. While EMP weapons can provide new surgical strike options for the RSAF, there are also challenges to their viable application. Friendly forces in the field and civilian infrastructure at home are also susceptible to its adverse effects, which posing limitations to their application in both offensive and defensive settings.

Improvements in technology have heralded trends in hybrid warfare that amplify threats to the RSAF. They would require the RSAF to seek out possible solutions to combat these threats. While the threats listed above are urgent and critical, they are definitely not exhaustive. Combating nuclear, space and cyber threats continue to be at the forefront of Air Forces' priorities in the foreseeable future. Weapons which are cost-effective in dealing with the identified threats become all the more important in a prolonged period of conflict. The RSAF will have to continually update its weapons systems and concept of operations by sieving out the trends ushered in by new technology, so as to maintain its technological edge over any possible adversaries.

ENDNOTES

1. Rusling, Matthew. "For the Military, a Future of Hybrid Wars." National Defense Magazine. September 1, 2008. Accessed July 7, 2016. http://www.nationaldefensemagazine.org/archive/2008/September/Pages/Hybrid_Wars.apsx

2. Hoffman, Frank G. "Hybrid Warfare and Challenges." Joint Force Quarterly. February 2, 2009. Accessed July 15, 2016. http://smallwarsjournal.com/documents/jfqhoffman.pdf

3. Johnson, David. "Military Capabilities for Hybrid War." RAND Corporation occasional paper series. June 26, 2010. Accessed July 15, 2016. http://www.rand.org/content/am/rand/pubs/occasional_papers/2010/RAND_OP285.pdf

4. Hambling, David. "Drone swarms will change the face of modern warfare." Wired. Accessed July 6, 2016. http://www.wired.co.uk/article/drone-warms-change-warfare

5. Teo, Benita. “Transforming the SAF to meet new challenges.” Cyberpioneer. June 30, 2015. Accessed July 13, 2016. https://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/news/2015/jun/30jun15_news3.print.img.html

6. “ST Electronics Showcases Smart Solutions at Singapore Airshow 2016.” Electronics Review. Accessed July 15, 2016. http://www.stee.stengg.com/pdf/publication/Vol29No1/Event 3.pdf

7. “High-energy laser weapons target UAVs.” C4ISRNET. Accessed July 13, 2016. http://www.c4isrnet.com/story/military-tech/uas/2016/02/19/high-energy-laser-weapons-target0uavs/80553744

8. https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule97

9. Sherwood, Harriet. "In Gaza, Hamas Fighters Are among Civilians. There Is Nowhere Else for Them to Go." The Guardian. July 24, 2014. Accessed July 14, 2016. https://www.theguardian.com/world/2014/jul/24/gaza-hamas-fighters-military-bases-guerrilla-war-civilians-israel-idf

   "UN Report Confirms Hamas Stored and Fired Weapons from UN Schools." The Tower. April 28, 2015. Accessed July 14, 2016. http://www.thetower.org/1955-un-report-confirms-hamas-stored-and-fired-weapons-from-un-schools/

10. Soffer, Ari. "French TV Shows More Evidence of Hamas Hiding Behind Civilians." - Defense/Security. August 5, 2014. Accessed July 14, 2016. http://www.israelnationalnews.com/News/News.aspx/183759#.V3yyUuZ97Vo.

11. Hirschauge, Orr. "Israel and Hamas Take Fight to Social Media." WSJ. July 23, 2014. Accessed July 14, 2016. http://www.wsj.com/articles/israel-and-hamas-take-fight-to-social-media-1406130179

12. Erlanger, Steven, and Fares Akram. "Israel Warns Gaza Targets by Phone and Leaflet." The New York Times. July 08, 2014. Accessed July 14, 2016. http://www.nytimes.com/2014/07/09/world/middleeast/by-phone-and-leaflet-israeli-attackers-warn-gazans.html?_r=1

13. Gayle, Damien. "How Israel Tells Gaza's Residents to Get out of Buildings before They Are Blown Apart: Footage Emerges of Controversial 'knock on the Roof' Air Strike Warning." Mail Online. July 14, 2014. Accessed July 14, 2016. http://www.dailymail.co.uk/news/article-2691302/Watch-Israels-controversial-knock-roof-air-strike-warning-condemned-human-rights-groups.html

14. Team, Gizmag. "Mobile Broadcast Message Center Can Text All Cell Users in a given Geo-location." Mobile Broadcast Message Center Can Text All Cell Users in a given Geo-location. November 17, 2010. Accessed July 14, 2016. http://www.gizmag.com/mobile-broadcast-message-center-text-all-cell-users-given-geo-location/16965/

15. Lister, Tim, and Salma Abdelaziz. "Israeli Military's 'knock on Roof' Warnings Criticized by Rights Groups." CNN. July 15, 2014. Accessed July 14, 2016. http://edition.cnn.com/2014/07/15/world/meast/mideast-israel-strike-warnings/

16. Wilson, Tracy V. "How LRAD Works." HowStuffWorks. March 3, 2006. Accessed July 14, 2016. http://science.howstuffworks.com/lrad.htm

17. "What Are 'sound Cannons' and Why Are Police Using Them in Ferguson?" The Week UK. November 14, 2014. Accessed July 14, 2016. http://www.theweek.co.uk/us/61501/what-are-sound-cannons-and-why-are-police-using-them-in-ferguson

18. Kelly-Detwiler, Peter. "Failure to Protect U.S. Against Electromagnetic Pulse Threat Could Make 9/11 Look Trivial Someday." Forbes. July 31, 2014. Accessed July 14, 2016. http://www.forbes.com/sites/peterdetwiler/2014/07/31/protecting-the-u-s-against-the-electromagnetic-pulse-threat-a-continued-failure-of-leadership-could-make-911-look-trivial-someday/#2bfc4a367fcdd

    "Nuclear Weapon EMP Effects." Nuclear Weapon EMP Effects. Accessed July 20, 2016. http://fas.org/nuke/intro/nuke/emp.htm

19. Fishler, Eliana. "NEWS SUCCESSFUL FLIGHT DEMONSTRATIONS FOR HAROP LOITERING MUNITIONS." June 7, 2015. Accessed July 14, 2016. http://www.iai.co.il/2013/32981-46464-en/MediaRoom_News.aspx

    "Switchblade Tactical Missile System." Army Technology. Accessed July 14, 2016. http://www.army-technology.com/projects/switchblade-tactical-missile-system/

20. Chang, Lulu. "U.S. Air Force Confirms Boeing's Electromagnetic Pulse Weapon." Digital Trends. May 26, 2015. Accessed July 14, 2016. http://www.digitaltrends.com/cool-tech/us-air-force-confirms-boeings-electromagnetic-pulse-weapon/

21. B, G. "Six Common Misconceptions About EMP - ProtecTgrid." ProtecTgrid. Accessed July 20, 2016. http://www.protectgrid.com/civil-defense-2-0/six-common-misconceptions-about-emp/

Huessy, Peter. "Electronic Doomsday for the US?" Gatestone Institute. January 13, 2016. Accessed July 20, 2016. http://www.gatestoneinstitute.org/7214/electro-magnetic-pulse-emp

22. Emanuelson, Jerry. "Electromagnetic Pulse Protection - EMP - Futurescience.com." Electromagnetic Pulse Protection - EMP - Futurescience.com. Accessed July 20, 2016. http://www.futurescience.com/emp/emp-protection.html

Chandler, Nathan. "How Faraday Cages Work." HowStuffWorks. Accessed July 20, 2016. http://science.howstuffworks.com/faraday-cage1.htm

23. Defense Industry Daily Staff. "Israels Arrow Theater Missile Defense." Defense Industry Daily RSS News. June 16, 2015. Accessed July 20, 2016. http://www.defenseindustrydaily.com/israel-successfully-tests-arrow-theater-missile-defense-01571/

ME6 Gabriel Tham is currently the Commanding Officer of 808 SQN. Prior to this, he was the Head Joint Logistics Plans and Resource Branch in Joint Logistics Department (JLD) and Senior Force Transformation Officer (Logistics) in Joint Plans & Transformation Department (JPTD). He also held command appointments in UAV Command and Air Defence & Operations Command (ADOC), and staff appointment in Air Engineering & Logistics Department (AELD) and Defence Science & Technology Agency (DSTA). He attended the Peoples' Liberation Army Air Force Command and Staff Course in 2015. He currently holds a Master in Science in Electrical Engineering (Distinction) from Naval Postgraduate School, a Masters of Science in Defence Technology and Systems from NUS and a Masters in Military Studies from China. He graduated from NUS with a Bachelors of Engineering (Electrical Engineering) and a Minor in Management in Information Systems in 2003.

CPT Edward Wong is a UAV Pilot by vocation and is currently a Staff Officer in Air Operations Department. CPT Wong was previously a pilot in 119 SQN.

ME4 Kelvin Kuo Kai Ming is an Air Force Engineer by vocation and is currently a Staff Officer at Joint Communications & Information Systems Department (JCISD). ME4 Kelvin graduated from Imperial College London with a Masters in Engineering (Aeronautical Engineering).