The Implications for Force Protection Practitioners of Having to Counter Unmanned Systems

A Think-Piece

European Air Group
Groupe Aérien Européen

Joint Air Power
Competence Centre

Cover picture Ⓜ © Alexandre Rotenberg/shutterstock

© This work is copyrighted. No part may be reproduced by any process without prior written permission. Inquiries should be made to:
The Editor, Joint Air Power Competence Centre (JAPCC), contact@japcc.org

Disclaimer
This document is a co-production of the JAPCC with the EAG. It has been initially produced at the request of SHAPE J3 Support to Operations following direction from the NATO Force Protection Working Group. Work has been developed in consultation with Subject Matter Experts at the European Air Group, SHAPE, NATO AIRCOM, the Air Force Interoperability Council (AFIC), nations, academia and industry. It does not represent the opinions or policies of either NATO or AFIC. It seeks to provide insight and analysis that will assist in shaping thinking within the wider Force Protection Community with regards to how to meet the apparent challenge of Countering-Unmanned Systems.

Comments and queries on this document should be directed to either the Air Operations Support (AOS) Branch JAPCC or the EAG Force Protection Team or, e-mail us at contact@japcc.org or prelations@euroairgroup.org.

Release
This document is approved for public release. Portions of the document may be quoted or reproduced without permission, provided a standard source credit is included.

Published and distributed by
The Joint Air Power Competence Centre
von-Seydlitz-Kaserne
Römerstraße 140
47546 Kalkar
Germany

Telephone: +49 (0) 2824 90 2201
Facsimile: +49 (0) 2824 90 2208
E-Mail: contact@japcc.org
Website: www.japcc.org

Follow us on Social Media

Ⓜ Denotes images digitally manipulated

FROM:

The Deputy Director of the European Air Group (EAG)
The Assistant Director of the Joint Air Power Competence Centre (JAPCC)

SUBJECT:

Think-Piece on the Implications for Force Protection Practitioners of Having to Counter Unmanned Systems

DISTRIBUTION:

All NATO and EAG Nations' Specialist Force Protection Staffs

The times when drones were only found in Science Fiction books are long gone and the world is now experiencing a rapid growth in the use and availability of Unmanned Systems. Driving this trend are advances in technology, which are enabling Unmanned Systems to be employed in new ways across an expanding spectrum of environments and disciplines. We are now in an era that permits wide and often unrestricted access to increasingly sophisticated and capable systems for professional and personal use.

On a global level, incidents involving small-scale Unmanned Systems have revealed security gaps for critical installations such as airports, seaports, nuclear power plants, military installations and other key facilities. These incidents highlight a new and rising threat that has become a major concern within NATO countries and partner agencies. In many nations, the unclear or even non-existent regulation regarding Unmanned Systems, coupled with their availability, ease of use and small footprint, all contribute to the increasing risk that they will be used maliciously. The ways in which Unmanned Systems may be used in this context is seemingly endless and examples include malicious imaging and observation, smuggling, hacking, tapping, impeding vehicles movements, delivering improvised explosive devices and more. Rogue States, hostile armed forces, terrorists, protest groups, disaffected individuals and other potential threat sources all now have access to Unmanned Systems that they could potentially use in a broad range of situations. The threat from Unmanned Systems is therefore a global issue, posing risks to national security, law enforcement, public safety and military operations.

In order to mitigate the threat, the armed forces have to adapt their security systems and put in place a comprehensive defensive capability, comprising hardware, organization, doctrine and training. As a central element of the Armed Forces' defensive scheme, the Force Protection (FP) practitioner has to understand the specifics about this emerging challenge

and integrate it into a broader spectrum of existing threats. This Think-Piece, which is the result of a collaboration between the JAPCC and the EAG, provides personnel at all levels with a detailed insight into the threat posed by Unmanned Systems. It also provides the FP practitioner with essential considerations to contribute to the planning process for exercises and operations. Together with the JAPCC, subject matter experts from all EAG Nations have participated in the production of this Think-Piece and have agreed to use it as a common framework. This work is intended to form the basis for developing common Tactics, Techniques and Procedures, in order to improve the interoperability between the Nations and their ability to counter the threats posed by Unmanned Systems.

We trust that you will find this document useful, informative and relevant. Your comments are not only welcomed but encouraged.

Stefan Scheibl
Brigadier General, DEU AF
Deputy Director, EAG

Giuseppe Sgamba
Brigadier General, ITA AF
Assistant Director, JAPCC

TABLE OF CONTENTS

THE IMPLICATIONS FOR FORCE PROTECTION PRACTITIONERS OF HAVING TO COUNTER UNMANNED SYSTEMS – A THINK-PIECE

THE IMPLICATIONS FOR FORCE PROTECTION PRACTITIONERS OF HAVING TO COUNTER UNMANNED SYSTEMS – A THINK-PIECE

1. Introduction

1.1 Overview. The subject of Counter-Unmanned Air Systems (C-UAS) has become what can best be described as a 'hot-topic', not just for the North Atlantic Treaty Organization (NATO) but, globally. The primary question that this think-piece seeks to explore is whether this challenge is new and unique or, whether it is actually just one of many threats that NATO faces that can be addressed with a little intellectual effort and with existing technology or, novel use of existing technology?

1.2 Task Background. Supreme Headquarters Allied Powers Europe (SHAPE) as the Chair of the NATO Force Protection Working Group (FPWG), raised the issue of potential adversary use of UAS as an issue at the October 2017, FPWG in Brussels. The Nations subsequently endorsed a proposal that SHAPE should produce a Request for Support (RfS) to the Joint Air Power Competence Centre (JAPCC) to examine the issue with specific focus on the implications for the Force Protection (FP) practitioner. The need for this work was strengthened with the receipt at SHAPE, from Kabul, of a Crisis Response Urgent Operational

Requirement (CUR). This CUR sought to address the question of how the migration of adversary tactics used in Iraq and Syria could be countered in Afghanistan and specifically, what can be done to mitigate adversary use of UAS, especially when weaponized?

1.3 Task Development. Subsequent to SHAPE issuing the RfS, NATO HQ Air Command (HQ AIRCOM), Ramstein convened its own FP Seminar to address the same issue. Given the SHAPE RfS, the JAPCC was asked to brief on its initial thoughts on the subject. In discussion following the brief, it was apparent that the JAPCC had effectively captured the essence of the challenge as perceived by both the NATO Air and broader Joint FP Communities and, what had *not* been captured, could be easily incorporated. It was also identified at the Seminar that both the European Air Group (EAG) and 1 German/Netherlands Corps (1GNC) were running their own similar projects. The pragmatic conclusion was that, with the agreement of the attendees at the Air FP Seminar and the EAG, the JAPCC would incorporate further discussion into the JAPCC work and subsequently make the resulting product available to a wider audience. Finally, the Air Force Interoperability Council (AFIC)[1] were briefed on the work, and they too have now provided input. Therefore, this think-piece now represents the thoughts of a wide range of interested parties captured during the period 14 March–21 December 2018[2]. Of note, this paper was reviewed immediately after the 19–21 December 2018 disruption at London's Gatwick Airport caused by apparent multiple 'drone' sightings. The thoughts reflected in this paper, it is offered, remain valid in light of this much discussed and publicized event.

1. Consisting of the '5-Eyes Community'.
2. Note that SHAPE sent 2 x FP-related RfS to JAPCC on 5 Dec. 2017. The first RfS was considered a priority and was the focus of JAPCC FP activity until its delivery on 14 Mar. 2018. Work on this RfS then commenced.

© Crown Copyright

2. Parameters

2.1 Approach. Importantly, this issue is not only a challenge for the Air Component. Despite the apparent focus on UAS, it is offered that Unmanned Systems exist in all domains and that all Components are at risk from these systems operating in domains other than the Components parent domain (e.g. an airbase can be targeted by a land-based Unmanned System; a port can be targeted by water-based systems, surface or sub-surface). Furthermore, these Unmanned Systems can either be remotely operated or autonomous (i.e. once launched, the vehicle functions without further input from an operator). This said, even autonomous systems will have a human within the system at some point (e.g. launch and possible recovery). Also, the level of autonomy of any Unmanned System will be a function of the level of technology available and the ingenuity of the operator to use even simple technology to best effect. Therefore, trading on the JAPCC's 'independence', this think-piece will attempt to address the general challenge of Countering-Unmanned Systems (C-US), not just the specific challenge of C-UAS.

2.2 Focus. The focus of this think-piece is the conceptual challenge of C-US at the Operational Level. It will not provide doctrinal guidance, specific recommendations on Tactics, Techniques and Procedures (TTPs) or, recommend specific equipment that can be employed at the Tactical Level. It is acknowledged that Unmanned System capability (payload, speed, concealment, range, level of autonomy, responsiveness, etc.) will all vary with domain and these factors will no doubt be considered by our adversaries when deciding on any attack vector (kinetic or non-kinetic). To date the use of UAS has dominated; it is suggested that this is primarily because of the availability of technology. However, technology will develop and what is true today will not be so tomorrow. The intelligent adversary will always be able to exploit technology to their advantage[3]. Therefore, it is offered that whilst the reader may perceive that this think-piece is air-centric, the principles offered are applicable multi-domain.

2.3 Objective. The objective of this think-piece is to create an accepted baseline of thinking across a broad customer base[4]. If this can be achieved, it will provide the foundation for the actual delivery of capability and as a result, this paper attempts to capture and subsequently shape thinking across as many of the NATO Capability Development, Lines of Development (LoD)[5] as possible.

2.4 Limitations. Countering contemporary threats, to include but not limited to Unmanned Systems, will require both a Comprehensive and Multi-Domain approach. This think-piece does not seek to describe the nature of NATO's Comprehensive Approach to operations nor the complex issue that is the emerging concept of Multi-Domain Operations. However, what is offered, is that countering any Unmanned System will require a multi-agency approach (so not just the military) and, irrespective of where a threat system is operating (on the surface, in the air or sub-surface), agencies will be required to cooperate and will likely need to operate in more than one domain concurrently (Maritime, Land, Air, Space and Cyber), in order to counter the threat. The age-old problem of information sharing will no doubt persist but, to create effective C-US strategies, inter-agency and inter-state cooperation will be necessary. This factor should lead directly to a significant conclusion i.e. that the Command, Control, Synchronization (and/or deconfliction) of FP activity, as well as the ability to communicate effectively, often rapidly[6] across many involved parties, remains an essential enabling capability for effective and resource efficient provision of FP effect (to include the defeat of adversary Unmanned Systems).

3. A simple land-based system may currently be defeated by passive measures such as physical obstacles. However, systems can be built or adapted to cross or breach obstacles.
4. See 'Task Background' and 'Task Development'. Those requesting this product are now SHAPE, the FPWG, AIRCOM, the EAG and AFIC. It is estimated that between the NATO FPWG, EAG and AFIC there are a minimum of 22 nations currently interested in this specific JAPCC think-piece.
5. Doctrine, Organisation, Training, Materiel, Leadership, Personnel, Facilities and Interoperability (DOTMLPFI).
6. Ideally in real-time.

The UK's Maritime Autonomy Surface Testbed, an unmanned surface vessel.

2.5 Threat System Consideration. A vast range of commercially produced Unmanned Systems exist across all domains; equally, a capable adversary could also manufacture their own improvised but none the less capable system. NATO has created a taxonomy for UAS which has been used as the basis for **Figure 1** (on the next page). The author has added to the NATO model in an attempt to provide a set of parameters to aid the FP practitioner in planning C-US activity. Nevertheless, further work by the Maritime and Land Components to develop their own domain-specific taxonomies which in turn could be combined with Air to create a Joint or Multi-Domain Unmanned Systems Taxonomy could prove useful. Whilst Figure 1 focuses solely on UAS, it is suggested that the same or similar principles could be applied to systems in other domains. It is offered that the primary challenge comes from systems at the lower end of the spectrum as these are both harder to detect and (if authorized) engage[7].

2.6 Threat Parameters. This think-piece will not address particular threat systems but, when considering threat it is perhaps worth noting that the Indirect Fire (IDF) threat from the almost ubiquitous 107 mm rocket, familiar to many FP practitioners, was from a projectile that weighed 18.84 kg (41.5 lbs); similar to the weight of an Unmanned System at the lower end of the 'Small'

7. The reader is invited to acknowledge that different nations have their own taxonomies and/or interpretation of the NATO Taxonomy.

Class	Category	Normal Operating Altitude	Normal Mission Radius	Endurance
Class I (less than 150 kg)	Nano (Class I (a)) < 200 g	Below 200 ft	1,000 m LOS*	25 mins (approx.)
	Micro (Class I (b)) 200 g–2 kg	Up to 200 ft AGL**	5 km LOS	30 mins
	Mini (Class I (c)) 2–20 kg	Up to 3,000 ft AGL	25 km LOS	30–60 mins
	Small (Class I (d)) 20–150 kg	Up to 5,000 ft AGL	50 km LOS	15 hours
Class II (150 kg to 600 kg)	Tactical	Up to 10,000 ft AGL	200 km LOS	20 hours
Class III (more than 600 kg)	Medium Altitude Long Endurance (MALE)	Up to 45,000 ft MSL***	Unlimited BLOS****	36 hours
	High Altitude Long Endurance (HALE)	Up to 65,000 ft	Unlimited BLOS	36 hours +

* LOS – Line of Sight ** AGL – Above Ground Level *** MSL – Mean Sea Level **** BLOS – Beyond Line of Sight

Figure 1: UAS Classification Guide.

category (20 kg). Likewise, the 122 mm rocket weighs-in at 66.6 kg (147 lbs). In other words, even in the 'Small' Category, Unmanned Systems have characteristics that existing technology can detect, track and if necessary/authorized engage. Therefore, the challenge exists primarily across the 'Nano' to 'Mini' Categories[8] where further useful deductions can be made:

a. Location. The Unmanned System threat of specific concern to the FP practitioner is likely to originate within the NATO base Tactical Area of Responsibility (TAOR) (e.g. the operator and the system will be present in the TAOR).

b. Operating Height. As can be seen in **Figure 1,** operating altitudes will fall within the surface[9] – 3,000 ft range for UAS. At the lower end of this spectrum terrain or infrastructure will present an operating challenge whilst the higher a UAS flies, the more readily it will 'unmask' to detection systems (i.e. they will not be able to hide amongst ground clutter).

c. Non-Air Systems. Without the advantage of height, operators of surface-based systems will have limited awareness of the environment beyond the immediate proximity of the system they are operating. This in turn might imply:

8. Notwithstanding that a small charge can have a large effect particularly if it can be delivered 'surgically' and/or with some additional kinetic force.
9. Note that Unmanned Systems may lie dormant on the surface in proximity to their intended target or in the case of maritime or riverine systems, on the sea or river bed.

(i). Further reduced range?
(ii). The possible requirement for the operator to be nearer the target[10]?
(iii). The utility of Unmanned System to the adversary will be different[11]?
(iv). Likely primary use of non-air systems will be as a means of weapon delivery especially in the hands of a terrorist. However, in the longer-term, the future use of Unmanned Systems, particularly by states, is only limited by imagination and the reality of available technology.

d. Endurance/Range. Unmanned Systems will have limited endurance; increased endurance can be achieved but, often at the expense of reduced payload (and vice-versa).

e. Payload. Smaller Unmanned Systems have limited payloads. Remaining with the IDF analogy, an 18.84 kg (41.5 lbs) 107 mm rocket only carried a warhead of 1.7 kg (2.9 lbs) (see 'Weapon Effects' below). Similarly, the ability of an Unmanned System to carry a sizeable payload will decrease, as the size of the system decreases. The deduction from this is that an intelligent adversary will most likely use Unmanned Systems, certainly in the air, primarily as Intelligence Gathering Assets although in reality, the potential use of any Unmanned System is only limited by an adversary's intellect/imagination. This, in turn, leads to the deduction that there will be a 'human-in-the-loop' and presents an actionable target to the FP practitioner. However, the issue of 'payload' should remain an entirely separate consideration from 'effect'. Specifically, a small system with limited payload could still have a significant effect if deployed against the likes of an unprotected 5th Generation platform. Equally, the perception that an Unmanned System could be deployed by an adversary as a means of delivering a Chemical, Biological or Radiological (CBR) payload will have a huge non-kinetic (psychological) impact. This effect will be irrespective of the technical feasibility and/or actual effects of any such weapon.

f. Effects – Kinetic. Linked to 'Payload' above, there needs to be a basic understanding of weapon effects.

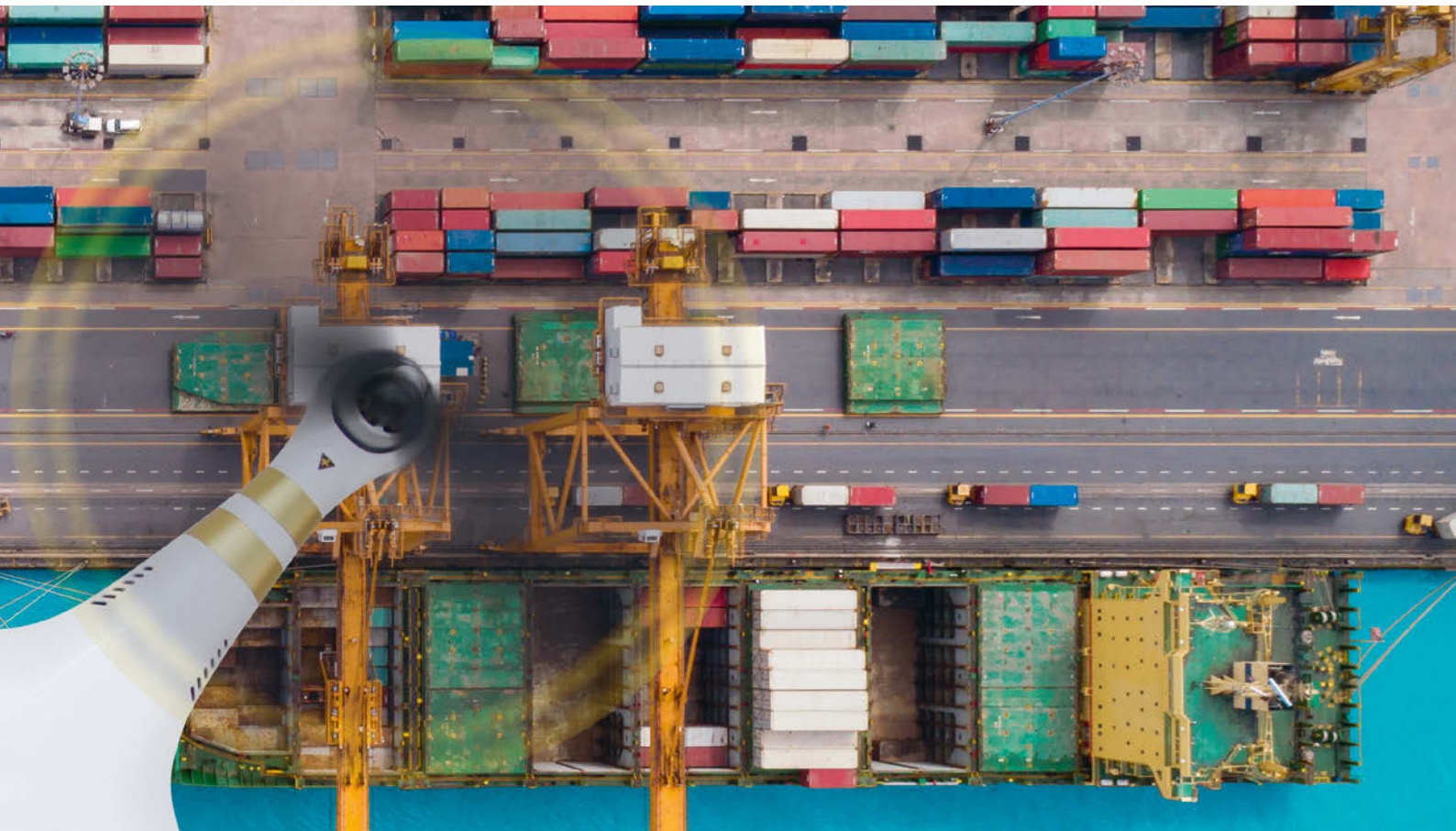
10. It is acknowledged that data from an Unmanned System could be transmitted via some form of link to a remote operator, however, this adds complexity which could in turn be exploited in order to detect and ultimately counter the threat.
11. E.g. The use of a land-based system to convey an explosive charge to a Control of Entry Point may be considered more effective by an adversary than the use of a mini-UAS to gather intelligence.

© Harbour: Studio concept/shutterstock, © Drone: krepnox/pixabay

As stated previously, one of the drivers for this think-piece was the concern over the migration of weaponized UAS from Iraq and Syria to Afghanistan. However, most of the use of weaponized UAS by the Islamic State of Iraq and the Levant (ISIS) consisted of dropping low-payload projectiles similar in size to a hand grenade. Adversaries have become adept at increasing the effectiveness of their Improvised Explosive Devices (IEDs) through the addition of shrapnel (e.g. ball bearings), the ability to add shrapnel (because of weight) on an air-vehicle of limited size is significantly reduced. Whilst this later factor might not apply to surface-based systems, other factors as discussed above, then come into play. What this means for the FP practitioner is that when the threat from Unmanned Systems is broken-down into its component parts, it becomes readily apparent that the threat (whilst clearly a challenge) is not what it may first seem. Proven FP techniques to include (but not limited to) hardening, dispersal, camouflage and concealment, deception and redundancy will all aide threat mitigation.

g. Effects – Non-Kinetic. The presence or potential presence in the battlespace of Unmanned Systems will have an effect irrespective of whether any system is actually weaponized. It should also not be discounted that kinetic effects can have an associated non-kinetic effect, e.g. on the morale of personnel. See also discussion above on the threat of the use of Unmanned Systems with a CBR payload.

Vignette: A video clip aired on many major news outlets reports to show an Iraqi Army tank being destroyed by an ISIS weaponized UAS. It is offered that this was a lucky strike where the weapon fell inside the vehicle but, importantly, the vehicle in question was operating in an urban environment and the crew should have been operating closed-down in order to prevent a hand grenade, IED or even a cruder 'Molotov Cocktail' (fire bomb) being used on the vehicle from above. Therefore, whilst the weapon that destroyed the vehicle was dropped from a UAS, it could have come from multiple other sources. The actual cause of the event was poor crew discipline resulting in a failure to implement basic TTPs for operating armoured vehicles in close terrain. Sensationalist reporting followed by multiple rebroadcasts with increasingly ill-informed comment together with a subsequent failure to properly analyse cause and effect have led to false conclusions being drawn. Had the weapon (improvised or otherwise) not fallen through an open vehicle hatch, the effects would have been negligible as the distance from any blast and shielding be it in the form of armour or infrastructure, reduces blast effect.



2.7 Larger System – Basic Considerations. As a system increases in size, it can be considered as increasing in capability. It will have greater range, longer endurance, be more robust and able to carry a greater payload. From the adversary perspective, this might be considered a positive. Although, obtaining a larger, more capable system comes with its own logistical challenges which could, in turn, lead to a greater 'footprint' or 'signature' that could be of intelligence value to friendly forces. However, for the FP practitioner, a larger system in use will also be more likely to be detected and the simple function of size makes it an easier target to engage.

2.8 Autonomy. Unmanned Systems can be remotely-operated, fully pre-programmed or have the ability to self-navigate having first been given navigational way-points. Whilst full autonomy can be argued to be possible, for the FP practitioner the fact remains that if an Unmanned System(s) threat exists, it has at least two tangible and therefore targetable elements; first is the vehicle itself and second, the user[12]. Therefore, any Unmanned System should be considered as a component of a larger system (similar to current Counter-Improvised Explosive Device (C-IED) doctrine), where the vehicle and/or operator can be exploited in order to gain information that will enable the wider system/network to be targeted. Much has been made of the potential future use of Artificial Intelligence (AI) and whilst the marrying of AI with Unmanned Systems adds yet further complexity, the fact remains that there are still identifiable and subsequently targetable elements within any adversary Unmanned System, system construct.

2.9 Threat Actors. This think-piece seeks to address the threat from Unmanned Systems in the generic sense and provide further 'food-for-thought' on the

12. In the case of an apparently autonomous system, the link between operator and system as a targetable element might be absent, but what would be the ends of that link i.e. the system 'owner' and the vehicle itself remain as targetable entities.

Certain Counter-Rocket, Artillery and Mortar systems may have the ability to engage?

subject. Like the range of possible systems available to an adversary, the range of adversaries is also considerable. Any individual using an Unmanned System can cause a major incident, intentionally or otherwise. The naivety of the general public in relation to matters of security and safety should never be underestimated. The spectrum of 'Threat Actors' covers the range from lone actor misuse, right through to deliberate state use. However, irrespective of who might be employing a system deemed to be a threat, many if not all of the available countermeasures can be employed. As discussed later, the primary limiting factor will usually be the legal framework within which any FP forces are required to operate. It is worthy of note that it is likely that in the case of any deliberate, nefarious use of Unmanned Systems, the system user will likely be aware of the legal framework in place and will seek to exploit it for their own ends.

3. Overarching Considerations

3.1 Capability Requirement Drivers. This paper will not seek to explore in detail what drives NATO's capability requirements. What is worthy of consideration though is 'who' can drive capability requirement? This subtlety is raised because it should be understood that there can be perceived benefit to the individual(s) who bring an apparent issue to the attention of a community of interest. This perceived benefit can take the form of kudos, advancement in rank or shaping a future employment opportunity. These individuals are what commercial conference organizers describe as 'Thought Leaders'. The second 'who' is perhaps more obvious – industry. Industry benefits from being able to develop and manufacture solutions that meet apparent capability requirements. Having described C-UAS above as a 'hot-topic', careful consideration needs to be given to who is driving this apparent challenge and for what purpose? There is no doubt a real-world challenge for the FP practitioner but, is it really a challenge of the magnitude that some would have us believe?

3.2 New Threats – New Countermeasures. As an extension of the drivers of capability above, the identification *(or perception of)* a new threat should not immediately mean that entirely new countermeasures will be needed (as much as industry would like this to be the case). It will often be the case that existing equipment, processes and practices can be adapted to counter the 'new' threat. Equally, even if the new capability requirement is identified, it will take time to deliver, therefore, adapting what we currently have available will always be necessary in the short to even medium term. A key component to countering any apparent new threat has to be the intellectual rigour that is applied to properly understanding that threat in the first place, to include how it will manifest itself (including adaptation and development) over time and space.

3.3 Measures of Effectiveness (MoE). A challenge that plagues the FP practitioner is that of MoE. In its simplest form, has a particular FP Measure or indeed an entire FP Posture been effective; has the adversary been deterred or, simply chosen not to attack? Over the last 20+ years, NATO and Partner Nations have developed an inclination that any attack must owe its occurrence at least in part to a failure in FP[13].

3.4 Reality Check. Following from the above, the reality of the contemporary operating environment is that it is inevitable that adversaries will, from time to time, be successful. These apparent successes when considered after the fact, could well be deemed to have been preventable. However, with the understanding available prior to the event, FP measures could still be considered appropriate. The current threat paradigm, to include C-US, requires the application of tried and tested FP measures, the subtle adaptation of these measures and where necessary, the development of new approaches. The increasing capability of platforms, their enormous cost and their reducing numbers means that the loss of such capability (this includes their operators, maintainers and supporting structures) would inflict real harm on a

13. Noting that Security is an element of FP within NATO FP Doctrine.

nation or indeed the Alliance. This, in turn, means that they present an emerging vulnerability that an adversary will undoubtedly seek to exploit. For the FP practitioner, arguing for a return to 'old' concepts such as dispersal, concealment and hardening will be necessary. Equally, the availability of resource debate cannot be ignored. This should take two distinct forms. Firstly, the requirement for robust FP forces. Second, the need to have sufficient resources, particularly in terms of support activity to allow capability to be operated in a warfighting manner rather than in a manner directed by just-in-time logistics or engineering expediency. Clearly, a balance is required but, the current lack of attention to the FP of high-value, low-density but incredibly fragile assets is concerning.

4. General Analysis – User Groups

4.1 Understanding the Threat. Bold statements that a threat exists are often made. For a threat to exist any adversary has to have both a capability and the intent to use that capability. However, above this sits the fundamental question of what is it that an adversary is actually seeking to achieve (what, why, when, where, how, etc.)? By gaining an understanding of the answers to these questions, the FP practitioner can start to identify how any threat or, threat system, could be defeated[14].

4.2 Threat Actors. No specific threat actors will be discussed but, some general factors require consideration. Firstly, it is offered that two, possibly three broad category of actors exist:

a. State;
b. Non-State;
c. State Sponsored.

An alternative approach could be to categorize use as either military or terrorist. However, the purpose of this paragraph is to offer that what is actually important, is a user's ability to access technology. Five basic options exist for any adversary which are:

a. Buy technology from commercial outlets.
b. Be provided with technology by a third-party.
c. Self-build or improvise the required technology.
d. Steal what is required.
e. A hybrid approach that involves acquiring technology but subsequently adapting it.

Understanding the origins of any threat system provides both insight into the possible scale of threat and how it might be defeated (i.e. if you know where something comes from, then its supply can potentially be interdicted). Also, the more technologically advanced and hence potentially capable a system is, the greater the likelihood that it will pose a real risk. The more complex a system, the higher the likely cost. Equally, the more complex a system, the higher the intellect of the adversary will need to be in order to use it in a way that it was not designed/intended to be used so that it becomes an effective weapon. These aspects of understanding the adversary and/or their system could facilitate the targeting of likely individuals and possible operating locations. Understanding and where possible exploiting the technology that is being used against us will help guide thinking on both what priority countering the threat needs to be allocated (in comparison to other threats) and provide an insight into who is operating it. Ultimately, if Unmanned Systems are viewed as just another threat, like all other threats, understanding where it comes from, who is using it, for what purpose, how it is being operated (adversary TTPs), etc. will all be significant pieces of information that will assist friendly forces in targeting that threat/threat actor. Unsurprisingly, the conclusion that can be drawn is that Intelligence will play a vital part in any ability to C-US (see also 'Categorization of Usage' at **Paragraph 8.4**).

4.3 Uneducated Use of Unmanned Systems. Particularly in the case of the Homebase, not all Unmanned

14. This is a generic statement. Consideration of actual historical examples and/or contemporary challenges, particularly if accessing threat-specific, classified information will enable a more focussed and hence useful analysis to be developed.

Drone threats/scenarios (such as Gatwick Airport, London, December 2018) can reveal potential security weaknesses.

Systems encountered will be used with nefarious intent. An aspect that has received little attention is the general ignorance of the populace at large to the risks to flight safety posed by unthinking use of UAS in the proximity of air operations, both military and civilian. This is compounded by the growing belief amongst many that it is their 'right' to know everything that in turn, leads a few to believe that they have a right to use not just UAS but any Unmanned System to gain insight into what 'the state' and in this case the military, might be doing 'inside the wire'[15].

4.4 Media. The reason that media use of Unmanned Systems has been considered as a stand-alone issue is because this particular area could be problematic for the military. Whilst legal matters are discussed elsewhere, media use of an Unmanned System, even if deemed illegal, is still likely to be branded as being in the public interest. Furthermore, the information or footage gained during such use is likely to be widely broadcast and could, dependent on media outlet, come with a degree of inherent apparent legitimacy to the story. The FP response to any detected use of an Unmanned System in the vicinity of any asset will need to be carefully considered in order to prevent any potential Strategic Communications 'own goal'. Also worthy of consideration is that in discussion with FP practitioners, there is a perception that some nations are reluctant to legislation to control UAS[16]. Given the argument offered elsewhere in this think-piece that such legislation would be of general benefit, the question of who or what is generating this

15. Note that some effective measures are already in place to mitigate the risk of uneducated use of unmanned systems (e.g. Geofencing).
16. Air Systems specifically but, by inference, this argument could be applied to Unmanned Systems in any domain.

apparent resistance should be explored. Given that the media now routinely uses Unmanned Systems and limiting their freedom of operation could greatly reduce their utility to the media, is the media partly responsible for shaping perceptions in the use of Unmanned Systems debate and/or is the 'media lobby' influencing political decision making?

4.5 Other Legitimate Users. Beyond the media, there are multiple commercial users of a variety of Unmanned Systems. These users will on the whole be responsible but, a better understanding of where Unmanned Systems are being employed now and where they are likely to be used in the future is required.

4.6 Detection. As stated above, there is general consensus that unthinking and/or nefarious use of UAS is a problem that requires attention. However, a more worrying question that cascades from this is that if we believe we have a problem based on what we are seeing, what proportion of the problem is going unseen or indeed unreported? For example, what materiel of intelligence value has been gathered using Unmanned Systems, without the presence of that system being detected and hence, a lack of awareness of where compromise may already have occurred? Is the current perceived use of UAS, only the 'tip of the iceberg'; how much Unmanned System activity remains so far undetected and/or unreported[17]?

5. General Analysis – Friendly Forces Perspective

5.1 Understanding is Key. Whilst this think-piece addresses a single issue, that issue is no different from any

17. Particularly as the focus seems to be on UAS. Surface and sub-surface systems (on both land and water) also require consideration.

Stryker armoured vehicle with the Mobile Expeditionary High Energy Laser (MEHEL). The Army has successfully used the system to target and shoot down drones during tests.

© US Army, Monica K. Guthrie

other FP-related challenge. The FP practitioner must understand, in as much detail as possible, both what it is they are protecting and how it functions as well as what the adversary is seeking to do (what, why, when, where, how, or, adversary ends, ways and means).

5.2 Modification of Existing Practices. FP forces already conduct a considerable range of activity both in accordance with ratified doctrine and beyond. How can this activity be modified or re-shaped to take into account the requirement to C-US? Examples here include but, are not limited to, conducting sweeps of the likely areas where Unmanned Systems can be launched and/or operated from, similar to the way that Mortar Baseplate Checks are currently undertaken; if an adversary is building their own, modifying or weaponizing a commercial system, activity designed to identify possible workshops could be considered[18]. Put simply, FP practitioners already conduct counter-threat activity, the concept of the Unmanned System as an additional threat only needs to be added to the list and a 'database' of possible 'combat indicators' developed. Presence Patrols or Outreach Activity in an urban area can be considered to contribute, as a second order effect, to both any C-IED and/or Counter-Surface to Air Fire (C-SAFIRE) effort – one activity, multiple effects. Knowing what to look for and/or what questions to ask will enhance the ability to interdict any threat before it manifests itself. Other simple examples of applicable practices include considering an UAS in flight as an IDF threat or, an immobilized system on the surface or sub-surface as either a mine or IED. Note that it remains vital when planning any activity to consider any negative, unintended consequences.

5.3 Covered Lines of Approach. Associated to the above, in the Cold War era, it was perceived that our installations were vulnerable to and would be targeted by Special Forces. As a result, routine security activity would ensure that pits, ducts, drains and watercourses were secure. Today do we even know where these facilities run that likely criss-cross many if not all our installations or, is this solely the domain of the civilian maintenance contractor? Even if we recognize the vulnerability, is routine security activity still taking place to ensure these 'covered lines of approach' are not being exploited?

5.4 Novel Application of Existing Technology. Again, there is an element of understanding required here. What existing technology if available or, which could be made available with little delay, could be used to either detect or defeat any Unmanned System? If the FP practitioner understands how a piece of technology functions or, can consult with the appropriate Subject Matter Expert (SME), deploying technology in a role for which it was never intended should be considered.

5.5 No Single Solution. A phrase that was often used when NATO was seeking to respond to the growing use of IEDs by the Taliban was that there was no 'Silver Bullet'; no single approach or piece of equipment that would solve the problem in all aspects. Any solution to the Unmanned System question is likely to have multiple facets and require the co-ordinated response of many actors/effectors. Equally, it is unlikely that a solution that works at one location or in one environment can be deployed ubiquitously. If multiple threats exist, each with their own distinct operating parameters, it is likely that multiple counter-systems will be required. Similar approaches or process may be applied but, a radar optimized to detect high and fast targets will struggle to detect low and slow targets and sensor performance should not be compromised by trying to cover too larger threat spectrum. If the threat, criticality of the asset and the appetite for risk drivers require it, a considerable range of sensors to include electro-optical, thermal, acoustic and seismic could be required to counter a range of threats. Similarly, if a variety of threat systems are to be effectively engaged, a range of weapons could be required.

18. For this to be a realistic option, it will be necessary to have an understanding of what Unmanned System components look like and personnel will in turn, need to be trained in identifying such components. A simple example would be the presence in any workshop of rotor-blade assemblies, remote-control devices.

5.6 Constraints. As with the majority of activity, there are likely to be constraints on what can be done; C-US activity will be no different. Considerations will include but, will not be limited to jurisdiction, privacy, Rules of Engagement (ROE), geographic boundaries, areas of responsibility, etc. Of interest, a view expressed by many during the development of this think-piece is that legal aspects are by far the biggest constraint, particularly when considering FP of the Homebase in 'peacetime'. It is not that the FP practitioner is unable to protect against the Unmanned System threat, it is that they are not permitted to.

6. A Proven Approach

6.1 General Considerations. Whilst this think-piece addresses a single threat-type, other as yet unidentified threats will undoubtedly emerge in the future. Probably more importantly at this stage, existing threats will endure, re-emerge, evolve or be revitalized/reinvigorated. Consider, if NATO were to deploy a large number of personnel, particularly at short notice, into a high, IED threat environment, would that force have institutionalized the lessons learned during combat operations in Afghanistan? The answer is probably not. In other words, we would have to re-learn previously hard-won lessons. Relating this thought to the issue of C-US, the question is, is it realistic to develop new approaches and possibly technology, for every new threat? Not forgetting that with every new approach comes a training requirement and with every piece of equipment a maintenance bill. Put simply, it is unrealistic to think that a 'golf club' exists for every eventuality. Key will be the ability to adapt existing methodologies to developing threats through the application of intellectual rigour. Therefore, the FP practitioner should focus on maintaining proven effective and sustainable counter-threat methodologies as captured in NATO FP doctrine, these include, but are not limited to:

a. C-SAFIRE patrolling;
b. Mortar Baseplate Checks;
c. Vehicle Check Points (VCPs) within the TAOR;
d. Influence Patrols;
e. Overt and Covert Observation Posts (OPs);
f. Use of residual air capacity for FP purposes[19].

6.2 Adversary Developments. In developing approaches to mitigate a threat, thought should always be given to how that threat may subsequently develop. If this approach is ignored, it is likely that an intelligent and adaptable adversary will quickly render any counter-measure redundant. As elsewhere, consideration also needs to be given to the concept of second-order effects and/or unintended consequences. What other effects could a counter-measure have (e.g. interference with other electronic systems)? The C-IED fight provides a valuable lesson in this respect where the deployment of supposedly improved protected mobility only drove the adversary to produce larger and more devastating IEDs. A key process for the FP planer is to consider what will be the impact of effectively neutralizing or even defeating a particular threat? What will the adversary conceive next and could it be either more difficult to counter or indeed more effective? An often overlooked approach is to tolerate or accept one threat in order to delay or prevent an alternative, more dangerous one materializing.

6.3 Swarming. A potential adversary tactic/development that requires specific consideration in respect of adversary use of Unmanned Systems is that of the use of so-called 'swarms'. The attacks on Russian Military facilities in Syria widely reported in December 2017 and January 2018 highlighted this tactic. Whilst this alleged use of multiple systems could be used as an argument to advance the perspective that 'new' threats evolve quickly both in quantity and possible quality, an alternative narrative could be advanced. Firstly, and specific to the example above, the ability to confirm the validity of reports in the media is limited in the unclassified domain. Second, and of more importance to the FP practitioner, what element of a

19. Most NATO installations will have at least a helipad. Any aircraft with surplus fuel can be asked to conduct an overflight of an area(s) of interest in support of the overall FP effort.

so-called swarm attack should cause consternation? The reality is that any threat can present itself at a scale that will be difficult to defeat (e.g. an attack by a significant number of adversary personnel supported by sustained mortar fire). The solution to this apparent conundrum lies in the ability of the FP practitioner to accurately identify the type and scale of the threat and subsequently articulate it; the vehicle for achieving this is the FP Estimate. If the analysis within the FP Estimate is robust, it will either lead to the provision of the necessary assets to meet and ideally overmatch the threat or, provide a solid basis for the understanding of any Risk(s) present.

6.4 Deconfliction. Whilst the subject of discussion is adversary use of Unmanned Systems, the fact remains that friendly forces and a growing spectrum of other legitimate Unmanned System users exist. From a FP practitioners perspective moving forward will require broad engagement in order to ensure that other interested parties are working to develop existing traffic management systems to incorporate new users. This may require the commitment of additional resources but, if this facet of the challenge is ignored, it risks issues of fratricide as well as an inability to separate friendly forces and/or legitimate use from ill-advised or foolish and adversary use of Unmanned Systems. Once again, an ability to understand what is in the battlespace will be fundamental to managing the threat and associated risk.

7. Operational Context

7.1 Geographic Location. This think-piece focuses on attempting to provide an approach to C-US at the operational level, however, much of the activity designed to C-US at the tactical level, will necessarily be driven by the location of the asset to be protected. Therefore, if during planning, the FP practitioner can influence the selection of location, this will go some way to simplifying the C-US task. Furthermore, and amplifying the concept that the Unmanned System should be treated as just another threat system, many

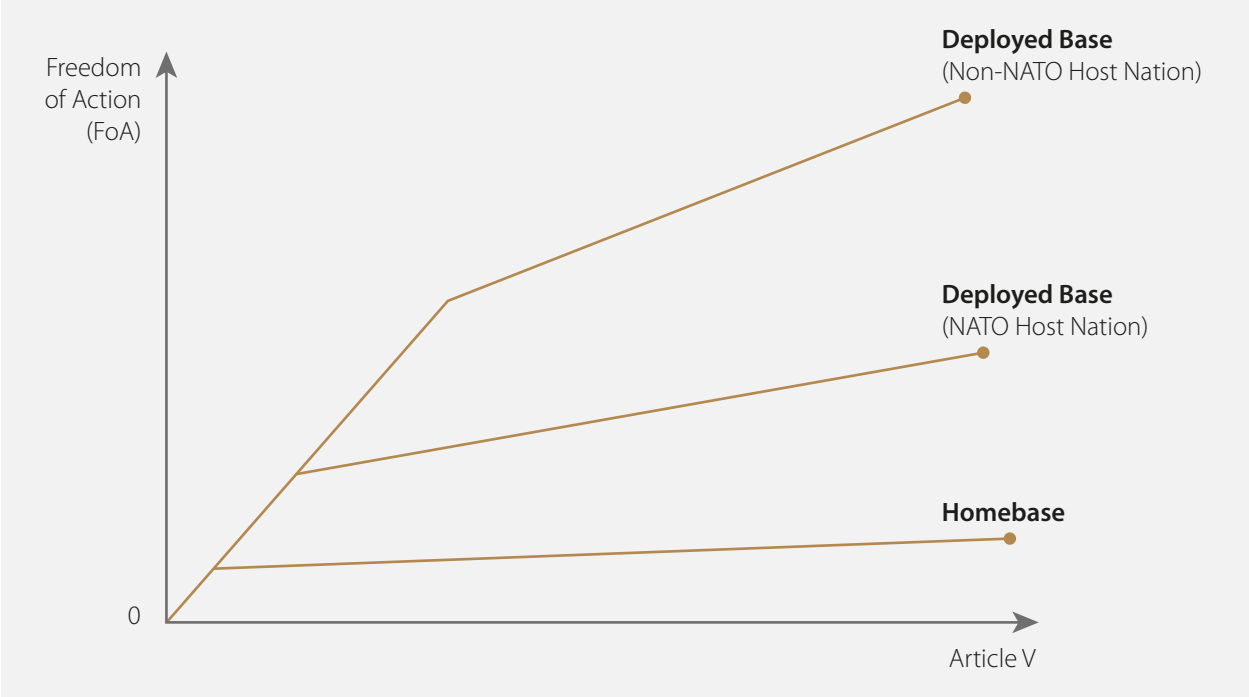


Figure 2: An Example of the Ability of FP Assets to Counter-Threats.

of the factors that simplify the C-US task, also simplify broader counter-threat activity. As an example, complex, densely populated urban terrain in close proximity to the operating location provides a far greater FP challenge than does a sparsely populated, open agricultural landscape. Put simply, the more places that an adversary can hide, the more difficult they will be to detect, deter and if necessary capture or destroy.

7.2 Homebase versus Deployed Operations. The Freedom of Action (FoA) allowed to the military FP community in relation to the protection of the Homebase in peacetime is likely to be limited[20]. It is often the case that they are not permitted to operate outside of the perimeter and activity will be confined to responding only once a threat has been detected. In addition, any response is likely to be extremely limited due to legal considerations. In the case of deployed operations, the possibility to influence the selection of the operating location exists. Furthermore, challenges of legal inflexibility at the Homebase *may* be overcome, at least to some extent, through early and robust engagement in the process that develops Status of Forces Agreements, Technical Agreements, Memoranda of Understanding, Rules of Engagement, etc. Perhaps a way to visualize this area is as a sliding-scale where the FoA to counter either ill-considered or nefarious use of Unmanned Systems (as well as other threats) increases as adversary action increases. Therefore, the constraints on FoA reduce because the operating environment is becoming *less* permissive (i.e. a crisis is developing and/or the Host Nation is less structured and cohesive as in the case of a failed or failing state). See **Figure 2** above.

7.3 Countering-Unmanned Systems in Free Space. This think-piece introduces many potential constraints on the ability of the FP practitioner to counter the threat from Unmanned Systems. If a hypothetical scenario was created where none of the real-world

20. Note also that many Homebase locations are sites that have existed for many years and so the FP practitioner has to work with the environment with which they are presented.

limitations or constraints were present, it is offered that it could be quickly identified that the challenge is not the ability of FP to defeat the Unmanned System threat, rather, the externally imposed constraints on FP that create the real difficulty. This is not to say that constraints imposed are not in place for entirely valid reasons (e.g. prevention of Civilian Casualties, Collateral Damage and Fratricide). The point though is that by thinking of how best to C-US without any externally imposed constraints, a spectrum of capability emerges that would undoubtedly mitigate against the majority of the threat. At this point it should be recognized that this think-piece is attempting to cover a broad spectrum of threat actors and scenarios. As a result, a perhaps unpalatable aspect of the discussion is to acknowledge at the outset that there are situations where an adversary will be successful. Equally, there can be no reference manual that will provide a written guide to C-US in all circumstances; documentation (Doctrine) can only provide a guide or hand-rail. This said, by considering how each of either the 'Force Protection Functional Competencies'[21] or 'Elements of Air Force Protection'[22] can be employed in C-US, a significant number of options emerge, many of which do not require either legal authority to employ nor substantial additional resources. This includes but is not limited to, use of cover, dispersal and concealment. Other more active and/or kinetic options also exist. The key take-away here is that effective (and resource efficient) C-US activity has two primary drivers. First, the ability of the FP practitioner to employ existing capability in an emerging role. Second, understanding the operating environment, particularly its constraints and identifying what measures *could* be employed if permitted. It is then a case for the Chain of Command to work to either remove the constraint(s), accepting the risk from Unmanned System or, terminating the at-risk activity.

21. AJP-3.14, Allied Joint Doctrine for Force Protection, Chapter 1, Paragraph 0106.b, Force Protection Functional Competencies.
22. ATP-3.3.6, NATO Force Protection Doctrine for Air Operations, Chapter 1, Section 4, Paragraph 0122, Elements of Air Force Protection.

8. Legal Considerations

8.1 Overview. This is a highly specialist area where there is no substitute for expert advice. However, a challenge from the outset is that every location (nation) and every mission/operation will have its own distinct legal parameters. In an operational environment where there is a recognized threat, and/or designated adversary, the constraints imposed on the conduct C-US activity are likely to be less. The real challenge exists in peacetime at the so-called Homebase. In this later scenario, the inescapable issue is that the FP practitioner is highly unlikely to be able to counter the Unmanned System threat in the majority of its manifestations, due to legal constraints (e.g. the inability to apprehend the operator, the unwillingness of civilian law enforcement to respond, an inability to seize or impound systems, etc.). Compounding this is the apparent current reluctance to address these legal issues. It is offered that the ability to protect assets could be significantly simplified if there was a concerted effort to either address legal deficiencies or, apply existing legislation more widely and/or more robustly.

8.2 Existing Legislation. Clearly, legislation across Alliance Nations varies. However, many states do have rules governing UAS usage which, with little or no adaptation, could be expanded to cover all Unmanned Systems, irrespective of domain. The European Aviation Safety Authority (EASA) website provides a useful resource. A basic example of such rules could be as follows[23]:

a. UAS (weighing under 20 kg) must be flown no higher than 120 m (400 ft).
b. Must not be used within 50 m (164 ft) of people or private property.
c. Must not be used within 150 m (492 ft) of congested areas or organized open-air assemblies of more than 1,000 people.
d. An operator must keep the UAS within his/her line of sight at all times.
e. The operator must be aware of and adhere to 'no-fly zones' (which notably include prisons and airports).
f. Any user using UAS for commercial purposes must register with the appropriate authority.
g. An 'Operating License' is required for certain types of UAS and can only be obtained having attended and successfully completed a training course.

The key point is that many states do have rules, it is just that the majority of the population do not know what they are. Equally, there is an apparent inability amongst the civilian law enforcement community to effectively enforce any rules. The FP practitioner as the 'conscience' of any operation or activity should be discussing this challenge with the Commander and seeking authority for direct liaison with those civil agencies who may be able to contribute to C-US activity, particularly in 'peacetime'. Whilst basic analysis of media reporting indicates that the situation is improving, it is offered that is an unfortunate reality that it will likely require a major incident to occur before sufficient focus is achieved.

8.3 Legitimate Use. There are clearly many positive and legitimate uses for Unmanned Systems that, so long as there is appropriate deconfliction, present no risk. Equally, it can be argued that there is no foolish, ill-considered, illegitimate or dangerous use that can be argued to have a positive or justifiable component. Activity that risks public safety, invades privacy or threatens security requires the application of legislation to control it.

8.4 Categorization of Usage. It is suggested that the usage of Unmanned Systems can be grouped into five primary areas[24]. Defining categories of usage creates a framework that can be used to better understand but also, potentially manage and then where necessary, control usage. Suggested categories are as follows:

a. Military.
b. Other Government Agencies/Emergency Services/First Responders/Law Enforcement.

23. Extracted from UK Civil Aviation Authority (CAA) rules and provided as an **example only.**
24. No known reference exist and these categories are offered for consideration by the author.

Envisioned commercial use of a UAS.

c. Legitimate civilian use to include:
   (i). Commercial Use.
   (ii). Hobbyist or other legitimate user who understands and adheres to legislation.
   (iii). Legitimate but, foolish, ill-advised and/or dangerous use by the public[25].
d. Media (see also **Paragraph 4.4**).
e. Use for illegal or nefarious purposes.

8.5 Managing User Categories. For 'a.' through 'c.(ii)', it is suggested that all that is required is the deconfliction and perhaps prioritization of any users operating in the same space. In the case of 'c.(iii)', if the necessary legislative framework exists, the operator and/or the Unmanned System can be detained/impounded and a pragmatic approach taken based on a proper investigation of the facts related to any incident. If it is subsequently identified that a user has done something that compromises public safety, compromised privacy or, has risked national security, laws should be in place which allow prosecution and the imposition of an appropriate and proportional sanction. This approach applies equally to dealing with the Media if they are found to be exceeding the boundaries of what can be described as public interest but, noting that as discussed at **Paragraph 4.4,** the Media will require special attention because they are likely to be the ones who will seek to push any boundaries established in pursuit of a story. By establishing 'User Categories' it enables the FP practitioner to streamline the decision-making process. If an Unmanned System is detected and the likely type of user identified, pre-determined TTPs for each eventuality can be developed. More simply, an approach could be taken where an Unmanned System was designated either 'Friend or Foe' and action taken appropriate to whichever designator was applied.

8.6 Effective Communication. An important component in either developing a bespoke legislative approach or applying existing legislation more widely or robustly is to have an accompanying communications

25. Within the UK there has been a year-on-year increase in incidents involving UAS and aircraft, with 71 recorded incidents in 2016 and 89 in 2017.

strategy. At a basic level, it is clear that many casual users of Unmanned Systems are simply unaware of the laws that they are at risk of compromising (see **Paragraph 8.2**). Perhaps more importantly, they are ignorant of the potential consequences of their action; the most obvious example here is an Unmanned System coming into contact with public transport. Again, it is all too easy to think of a UAS being ingested into an aircraft engine, however, there are examples of both model aircraft and model cars impacting passenger carrying, road-going vehicles. Model boats can be ingested into passenger ferry propulsion systems. In simple terms, the general public need to be more aware of both the potential impact of the use of Unmanned Systems and the consequences they could subsequently face.

8.7 Existing Legislation and New Laws. Given that this is a think-piece with a multinational audience, it would be impossible to describe a single legislative approach. A simple, single start-point for the FP practitioner does however exist. What is required is engagement with the Legal Advisor in order to understand what legislation exists in any region and how it may be applied as one of the tools to ensure proper control of Unmanned System usage. If the necessary laws do not exist, it is offered that a robust argument can be advanced as to why such controls are necessary (i.e. public safety, protection of privacy and protection of national security).

8.8 Wider Control Measures. Legislation is but one aspect of a wider framework of control measures.

© Squarehead Technology AS

A variety of organizations exist both at the national and international level that provide rules or conventions that govern the use of space within different environments (e.g. Federal Aviation Authority and International Maritime Organisation). Basic research suggests that most of these rules or conventions with little or no modification[26] can be applied to Unmanned Systems.

8.9 Use for Illegal or Nefarious Purposes. By attempting to categorize users or usage, it should be possible to 'isolate' those that are using Unmanned Systems inappropriately. This approach will take time to implement and remains reliant on both a control structure to include legislation being created, together with effective communication of the fact that such measures are being brought into effect and, will be enforced. For the FP practitioner, this would create a situation where in the event of the detection of the use of an Unmanned System, the implication is that it is being used for illegal or other nefarious reasons. This approach allows for more rapid decision making in that once detected, an Unmanned System can immediately be classified as a threat and the appropriate action taken. It should be noted that any action, in the context in which it is envisaged here[27], will remain the responsibility of the civilian authorities. Military response will remain, as now, confined to 'inside the wire' during peacetime and during some operations.

9. Existing Capability

9.1 Current Doctrine. A suite of current NATO FP documents exists and each contains a list of further reading. Whilst it is acknowledged that as these publications are reviewed, particular mention of Unmanned Systems as a specific threat will be included, current documents *do* already provide a comprehensive spectrum of counter-threat methodologies than can be applied *now* to the challenge of C-US. The pillars of C-IED doctrine (Defeat the Device, Attack the Network and Train the Force) and much of how this is achieved is applicable to C-US activity. A static or immobilized Unmanned System can be approached as an IED. Equally, why can a UAS in flight not be dealt with as an IDF threat? It is offered that current, broader counter-threat methodologies and supporting activity remain the key to countering the Unmanned Systems threat.

9.2 The Human Dimension. Perhaps the NATO FP practitioner's most effective weapon is the ability to analyse and subsequently understand a problem. Equally, it would be an error to consider any adversary as less intelligent than ourselves. Any threat will have a human in the system at some point, even if an Unmanned System is categorized as autonomous, a human will still have to set that system in motion and will be expecting that system to produce some output or effect. The FP practitioner needs to ensure that the correct weight of effort is afforded to the human dimension of the threat as this is ultimately where it is most likely to be comprehensively defeated. Conversely, over-focus on the Unmanned System itself (in C-IED terms the device), will likely lead to a more protracted campaign. At a very basic level, the reinvigoration of 'old' TTPs such as the deployment of Sentries will add to the ability to mitigate the threat.

9.3 Sensors. It was stated at the outset that this think-piece would not discuss specific equipment. Perhaps a task for either or both the Conference of National Armament Directors (CNAD) and the NATO Science and Technology Organization (STO) could be to investigate what within the considerable range of sensor systems currently available, either individually or, when combined with others, is best at detecting Unmanned Systems? Noting that Unmanned Systems exist in all domains, it is likely that the sensor requirement will be bespoke to specific threats to individual locations. In an operating environment with a range of threats, it is likely that a suite of sensors will be required with each sensor system looking at either a

26. In many cases adding 'Unmanned Systems operators' to the list of users to which the rule or convention applies would be all that is required.
27. At the Homebase during peacetime.

specific threat (e.g. Direct Fire), a specific environment (e.g. acoustic or seismic sensors against the sub-surface threat) or, just part of a wider threat spectrum (e.g. an Air Defence Radar specifically 'tuned' for the detection of small, low and slow air threats).

9.4 Effectors. Many current sensors can be deployed with associated effectors as part of a system designed to counter existing, acknowledged threat-types, e.g. Counter-Rocket, Artillery and Mortar (C-RAM), Surface Based Air Defence (SBAD). These systems have a range of effectors optimized for the threat that they are designed to counter. Like sensors, these effectors may be capable of defeating the Unmanned System threat or, a tailored system may have to be deployed.

9.5 System of Systems Approach. As now, the range of threats and hazards faced, drives the range of capability required. If multiple threats can be countered by a single system, this is an advantage. However, an important consideration should be that system performance is not compromised by expecting that one system can be equally as effective against all threats. It is offered that it would be better to deploy several systems, each optimized against a specific threat, rather than deploy a single system that is compromised in its ability to deal with any of the threats. A useful way of considering C-US equipment is to separate sensors from effectors. Sensors can be further divided by role be that Detect, Track or Identify (DTI). Whether a system of systems approach is taken, is a question for future consideration.

10. Emerging Considerations

10.1 Overview. Having stated that the basis for the response to adversary use of Unmanned Systems is the application and/or adaptation of existing Counter-Threat methodologies and associated technology, it is worth brief consideration of emerging technologies which could provide an advantage.

10.2 Geofencing. For the purpose of this think-piece, 'Geofencing' is defined as:

'The use of Global Positioning System (GPS)/Global Navigation Satellite System (GNSS) or Radio Frequency Identification (RFID) technology to create a virtual geographic boundary, enabling software to trigger a response when a mobile device enters or leaves a particular area.'

A number of governments are exploring how geofencing can be used to control or regulate the Unmanned System and specifically UAS use. The concept is that the necessary technology is built-in to the Unmanned System and uses GPS coordinates to prevent the system from entering pre-defined zones, such as prisons or the airspace around airports. Clearly, geofencing can be overcome by an adversary but requires the necessary capability and access to resources to achieve. This said geofencing remains another 'weapon' that can be used against the Unmanned System threat.

10.3 Sensors. It is offered that there is no requirement to develop new sensors specifically designed to detect Unmanned Systems? Existing sensor technology continues to advance, but the old concept of an 'Arms Race' remains as valid today as when the phrase was first coined. It will remain likely that for every development in 'detect' capability, an adversary will eventually develop a method of avoiding such detection. For the Alliance, in a 360-degree threat environment, it is offered that it is inescapable that a range of sensors will be required to detect a range of threats. The ability to fuse sensor data so that a reduced number of sensor operators is required is conceivable. However, the cost, maintainability and supportability of any such solution is questionable at this time.

10.4 Jamming. GPS Jamming may be considered as a tool against the Unmanned System threat. However, with so much Alliance technology relying on GPS or the GPS timing pulse, using GPS Jamming will require careful coordination and deconfliction with multiple agencies. This also assumes that the appropriate (scarce) technology can be obtained for deployment in the FP role? It is more likely that such technology if deployed, will be deployed against larger Unmanned Systems beyond the immediate concern of the FP practitioner.

10.5 Effectors. A myriad of technologies exist that are being marketed as 'counter drone' technologies. However, before considering effectors, the inescapable reality is that the ability to defeat an Unmanned System has to be underpinned by the necessary Rules of Engagement. As discussed in **Section 8,** this is a large and complex area but, there are three major considerations. First, simply, is the engagement of any Unmanned System permitted? Second, in engaging an Unmanned System that could be described as a 'small and fleeting target', if the weapon system in use misses the intended target, where will any effect be realized? Finally, if the Unmanned System is successfully engaged, what will the effect be on both the location being apparently targeted by the system and also any area where the debris (to include a potentially still viable weapon), may fall[28]? Now assuming that engagement is permitted, industry is marketing a variety of C-UAS technologies which utilize various novel technologies to include lasers, bean-bags, nets and various directed energy weapons. It is offered that whilst these 'weapons' have some ability proven in testing, their long-term viability in the operational environment, it is suggested, remains questionable at this stage. Also, as discussed elsewhere, new technologies have an associated resource burden even if it is limited only to training and maintenance. At a very basic but, nevertheless important level, the FP practitioner may have to consider providing FP for any system and its operator(s) as they may not be able to self-protect whilst engaged in C-US activity? Introducing new, potentially unproven technologies into the battlespace requires careful consideration with particular attention being paid to second-order effects and potential unintended consequences.

10.6 Human Factors. The employment of any new technology has resource implications. Beyond the resource implications of introducing new capability is the inescapable fact is that the world of the soldier,

28. Recognizing that this area could well be a civilian area outside the perimeter of an Alliance facility.

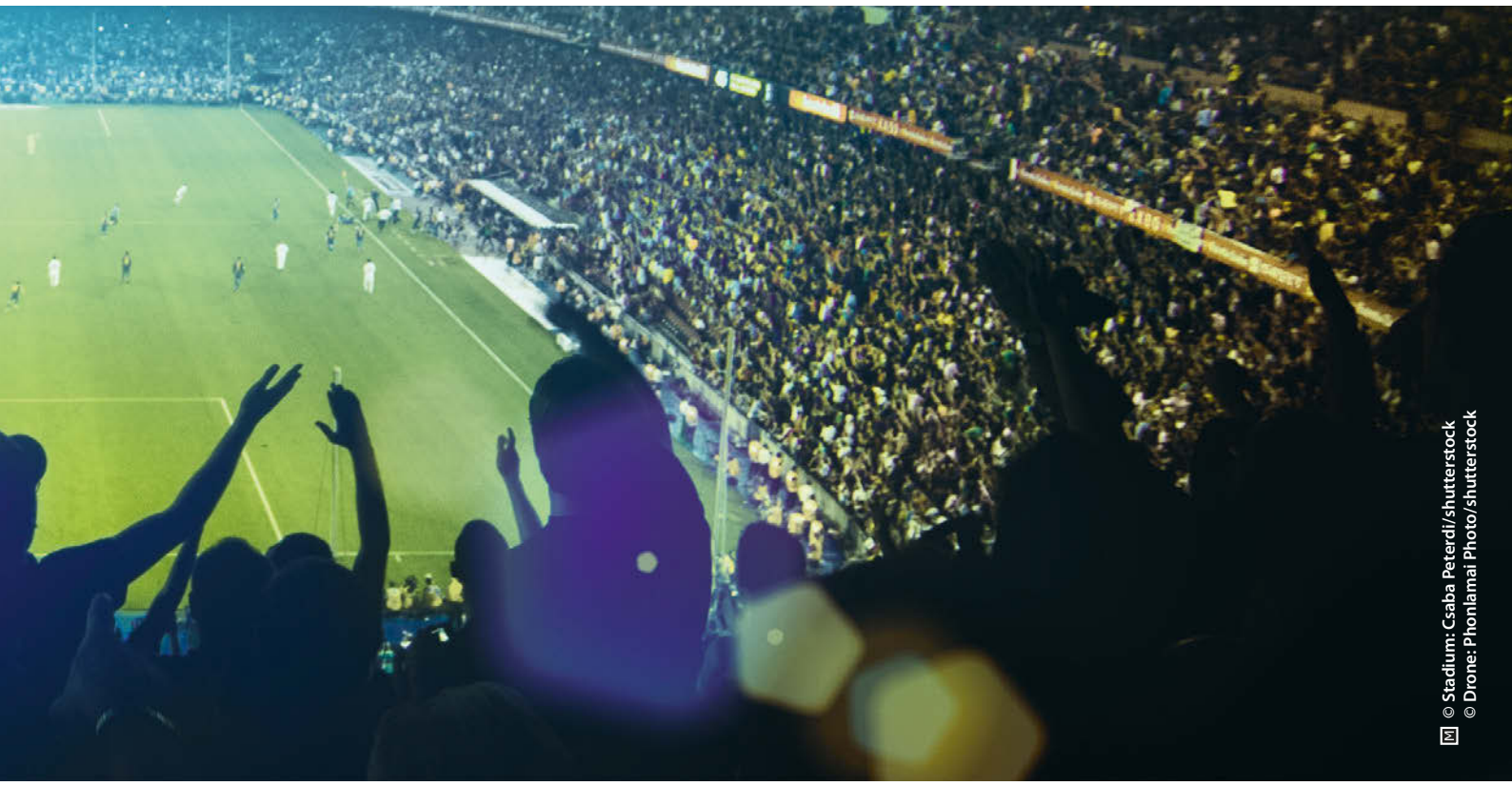
Simple counter threat activity could present sub-surface ingress?

© HolgersFotografie/pixabay

sailor, airman or marine is becoming ever more complex and the point is rapidly approaching where the individual is reaching maximum capacity. This is in terms of both the physical sense of being able to simply carry all the equipment supposedly required and in the cognitive domain where they are again rapidly approaching 'saturation point' and where absorbing how to effectively operate multiple, separately developed, often incompatible systems is becoming beyond many.

10.7 Planning Tools. Following on from the above, an area where technology could have real positive effect for the FP practitioner is in the area of FP planning. The author in the course of researching this think-piece was made aware of a software application originally called 'Surface to Air Missile-Precision Rating and Analysis Software (SAM-PRAS)'[29]. This software is in use with a number of nations and over a significant number of years has been developed well beyond a simple Counter-Surface to Air Missile planning tool. In simple terms, the system can now assist in predicting where an adversary is most likely to use a particular weapon system from. Different layers can be developed each corresponding to either a different threat or different manifestations of the same threat. Of equal value is the ability to use the tool to site different sensor systems for maximum effect. The key point is that it is highly unlikely in the current or foreseeable future, resource-constrained environment, many if any additional resources are going to be made available for FP. Therefore, more effective planning that enables the better use of existing, scarce resources, has to be pursued and relatively cheap but nonetheless effective planning tools require greater investigation.

29. Whilst other software applications may exist, none became apparent whilst conducting basic, open-source market research.



© Stadium: Csaba Peterdi/shutterstock
© Drone: Phonlamai Photo/shutterstock

10.8 NATO Defence Planning Process (NDPP). The argument advanced within this think-piece is that the solution to countering the Unmanned System threat lies predominantly in adapting existing counter-threat thinking and TTPs. However, to do this effectively and particularly if it is identified that additional, specific resources are required, it is perhaps worth considering developing a discreet C-US Capability Code and supporting Capability Statement for introduction into the NDPP.

11. Summary

11.1 General. This think-piece offers that it is not just UAS that present a challenge to the FP practitioner but, Unmanned Systems in all domains. The current perception that these Unmanned Systems are a 'new' threat that requires a bespoke approach should be challenged; who is driving current thinking and why? Are Unmanned Systems actually something different or, are they just the logical employment by our adversaries of increasingly accessible technology? Current FP Policy, Doctrine and Directives remain fit-for-purpose as do the FP Estimate and FP Planning Processes; all that is required is the introduction/incorporation of Unmanned Systems as a further consideration. With the application of intellectual effort to better understand the threat in all its constituent parts, it is offered that it will be realized that existing practices, procedures and technology can be employed to counter most, if not all aspects of the Unmanned System threat. Furthermore, there are 'multiple defeat vectors' and not unlike C-IED thinking, the Unmanned System, the operator or the broader adversary network can all be targeted either individually or simultaneously. There is undoubtedly a role for the use of new and emerging technologies but, this requires careful consideration not least because each new technology comes with an inherent training and maintenance burden. It is suggested that the principle challenge today is not the lack of capability but, the inability to

actually employ that capability. In a crisis situation with the necessary legal framework in place (as a result of robust planning), the ability to target the system, its operator and the broader adversary network should exist. With respect to protection of the Homebase, it is suggested that a compelling argument can be advanced for why the use of Unmanned Systems needs to be better controlled. Clearly the level of control will vary dependent on the actual threat that each system could realistically present. However, the question of why there is apparent resistance to this approach needs to be further examined; particularly the role of the media. The FP practitioner when considering perceived new threats, must not lose sight of existing, accepted threats and finally, to successfully neutralize any Unmanned System threat will require inter-agency co-operation; what might be described in NATO vocabulary as 'the Comprehensive Approach'.

11.2 Specific Observations. During the development of this think-piece, a number of observations came to the fore that it is suggested require highlighting:

a. Unmanned Systems are just another threat for the FP practitioner to contend with. It is offered that they are not 'game changing' and if the challenge is disassembled, it will be quickly seen that there are many existing ways of at least mitigating against, if not immediately neutralizing, the threat. Existing FP documentation will be updated over time. However, it remains fit-for-purpose and can be applied to the C-US challenge.
b. Unmanned Systems exist in all domains. All components could be threatened in all domains (Air, Surface (water and land) and Sub-Surface (again both land and water)).
c. Even a small Unmanned System with limited range, limited endurance and a limited payload could be considered as a major threat in certain circumstances (e.g. if it could be used to damage or destroy a high-value, low-density asset).
d. Other threats remain. The threat from Unmanned Systems should be considered together with all other potential threats. It is not, at this stage, either sufficiently different or more dangerous than the plethora of other FP challenges in the contemporary operating environment. Effective Battlespace Management remains vital.
e. The intellectual component is key. The ability to break any supposed 'new' threat into its component parts is essential if that threat is to be correctly understood.
f. C-US is not only an FP practitioner's responsibility. Any solution needs a comprehensive, inter-agency approach.
g. There is no single solution. Allied to the comment above, a successful response is likely to be based on a system-of-systems approach.
h. Any large organization needs to be wary of having its thinking shaped by a vocal, perhaps influential, minority.
i. The ability of the FP practitioner to C-US is likely to be limited by law in many areas.
j. New technology is not necessarily the answer. Some existing technology will be effective or could easily be adapted (e.g. C-RAM).
k. Any proposed novel approach needs to be considered and evaluated across all NATO Capability Development, Lines of Development.
l. 'Back to the Future' is a useful adage. 'Old' measures such as camouflage, concealment, screening and hardening together with TTPs such as the deployment of Air Sentries will all be effective against this 'new' threat.

Notes

NATO UNCLASSIFIED – PUBLICALLY DISCLOSED

Notes

European Air Group
Royal Air Force High Wycombe
Buckinghamshire | HP14 4UE | United Kingdom

Joint Air Power Competence Centre
von-Seydlitz-Kaserne
Römerstraße 140 | 47546 Kalkar (Germany) | www.japcc.org