Óglaigh na hÉireann
IRISH DEFENCE FORCES

Defence Forces Review 2019

www.military.ie

STRENGTHEN THE NATION

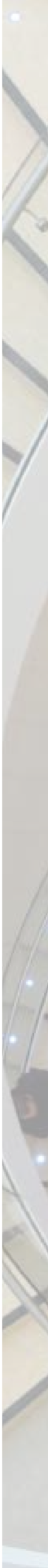
Óglaigh
na hÉireann
IRISH DEFENCE FORCES

Defence Forces Review 2019

ISSN 1649-7066

Published for the Military Authorities by
the Public Relations Section at the Chief of Staff's Branch,
and printed at the Defence Forces Printing Press, Infirmary Road, Dublin 7.

STRENGTHEN
THE NATION



Launch of the Defence Forces Review

In conjunction with an Academic Seminar

University College Dublin, Dublin

05th December 2019

Preface

> *"The secret of change is to focus all your energy, not in fighting the old, but on building the new."*
>
> *Socrates*

It is a privilege for me as Officer in Charge Defence Forces Public Relations Branch to launch the Defence Forces Review for 2019. The purpose of the Defence Forces Review is to provide a forum in which contributors can present their research and facilitate discussion on a wide range of defence-related matters for the benefit of the wider Defence Community. I believe that this issue of the Review will achieve all of these goals, and will, in turn stimulate widespread discussion amongst readers.

Building on recent publications, this year's review primarily focusses on a specific theme, in the case of this year's review the theme is: 'The 22nd Century Military Force: Technology, Innovation and Future Force Concepts.' The articles reflect, among other things, the changing character of warfare, the exponential changes in technology and the likely effects these will have on militaries and the manner in which military operations might be conducted in the future operating environment.

The Editor of the Defence Forces Review for 2019 is Lieutenant Commander Paul Hegarty. Despite a very heavy schedule as an Instructor in the Command and Staff School he assumed this editorial burden with energy and commitment, displaying a commendable level of academic ambition for this project.

For this year's edition, he has assembled a diverse group of contributors, working in academic collaboration with the University College Dublin (UCD) School of Politics and International Relations (SPIRe), and the UCD Clinton Institute. A special word of gratitude to his fellow editors, Professor Ben Tonra (SPIRe, UCD) and Dr. Eugenio Lilli (Clinton Institute, UCD), for their expert insights and invaluable contributions in making this collaborative effort a success.

Again, many thanks to all our contributors without whose commitment and generosity the production and publication of this year's review would not be possible.

Further copies of the Review are available from the Defence Forces Public Relations Branch at info@military.ie or online at http://www.military.ie/info-centre/publications/defence-forces-review.

J. Whittaker
Lieutenant Colonel
Officer in Charge
Public Relations Branch

Editor's Notes

> *The illiterate of the 21st century will not be those who cannot read and write, but those who cannot learn, unlearn, and relearn.*
>
> *Alvin Toffler*

The multiplicity of, and the threats deriving from technological based systems continues to rise as the dawn of the fourth industrial revolution breaks on the horizon. Modern society is undergoing a technological revolution that is fundamentally altering the way we live, work and relate to one another. While it remains uncertain how this will exactly unfold, it is evident, that the response required to manage it must be integrated and comprehensive, and will involve all elements of society, including the military. The future will be characterised by a fusion of technologies that are blurring the lines between the physical, digital and biological spheres.

Technology continues to advance at a rate not foreseen by those who have used it historically in a military context, and while the fundamental nature of warfare may not be changing; its character certainly is, as changes in thinking and technology evolve. How do we comprehend, contextualise, and conceptualise the changes wrought by emerging technologies, which are converging and being applied in completely unforeseen ways? History is littered with inflection points, such as the infamous 'horse and tank' moment, and the future military organisation will have to understand and learn to manage the power of information, in data processing, Artificial Intelligence, robotics, bio-science, materials and autonomy, to name but a few.

While it is acknowledged that the starting point for future strategy must account for the world as it is because of the way it is, the Defence Forces must be prepared to evolve and adapt as threats develop. Military organisations, similar to the society they represent, must learn how to manage and prepare for this (un)certainty and ensure that their structures, equipment and doctrine evolve to meet both current and future potential threats. Fundamental to achieving this objective is the need for military organisations to innovate and to work collaboratively with external partners, such as business and academia, in learning and discussing potential solutions.

This year's edition of the Defence Forces Review is published in academic collaboration with the University College Dublin (UCD) School of Politics and International Relations (SPIRe), and the UCD Clinton Institute. It reflects on the current structure and associated capabilities of the Irish Defence Forces, while simultaneously inviting comprehensive critical analysis with a view to contributing to the current discourse so that we can learn about how to best prepare for the future operating domain, and its associated challenges.

This edition presents contemporary assessments on selected topics in an attempt to add to the current debate, and proposes solutions and a discourse that the Defence Forces can draw and learn from. The papers cover topics that demonstrate a wealth of knowledge both internal to the Defence Forces and in wider academia, both national and international, that in turn will promote further debate on these pertinent and current issues.

In 2019, the Defence Forces delivered its first Joint Command and Staff Course (JCSC), which marks a paradigm shift in how the Defence Forces trains and prepares its future senior leaders on its flagship course. The abstracts from this course, as part of the MA in Leadership, Management and Defence Studies (LMDS) program are included in the Review. To view any of these listed, please contact the Defence Forces Library at; info@military.ie.

The review concludes with short biographical details of the authors who kindly contributed to this year's edition. The Editorial team would like to thank the contributors for their enthusiasm and willingness to prepare papers for submission, thereby participating to the discourse on what a 22nd Century Defence Forces could resemble and what challenges it may face. We are also indebted to the Defence Forces Printing Press (DFPP), in particular, Lt (NS) Colm Fox, and Pte Shane Curran, for their time, patience and professionalism in delivering a high quality finished product.

Editorial Team

Lt Cdr Paul Hegarty	**Prof Ben Tonra**	**Dr. Eugenio Lilli**
Command &Staff School	**SPIRe, UCD**	**Clinton Institute, UCD**

Editor's Biographical Statement

Lt Cdr Paul Hegarty joined the Defence Forces in 2000 as a member of the 40th Naval Cadet Class and currently works as an instructor in the Command and Staff School. He has held several sea-going appointments, and has served in a variety of command, staff and training appointments. He has completed the Royal Navy International Long Navigation Course at HMS Collingwood, holds a BSc in Nautical Science (CIT), a Masters in Project Management (UL) and an H-Dip in Geographical Information Systems (UCC). He is a graduate of the UK Joint Services Command and Staff College and attended the Advanced Command and Staff Course in 2018 and completed an MA in Defence Studies from King's College London. He has submitted research to the Royal Irish Academy for publishing in the upcoming edition of Irish Studies in International Affairs and has lectured on Maritime Security at the Whitaker Institute in NUIG. His PhD research focuses on Change Management in military organisations and he will complete his doctoral studies in early 2020.

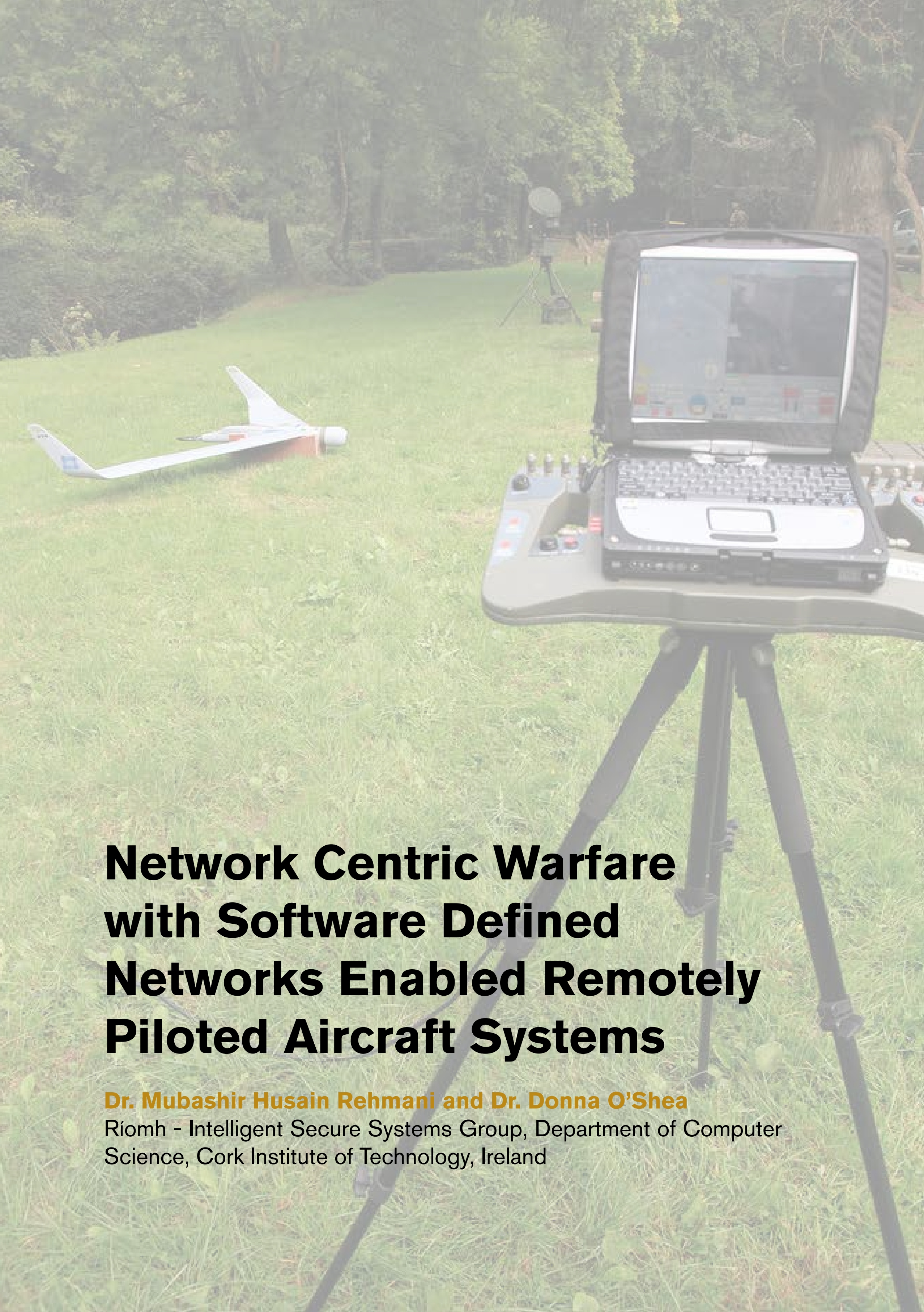
Dr Eugenio Lilli is Lecturer and Coordinator of the Master Program in American Politics and Foreign Policy, at University College Dublin, Ireland. Eugenio's primary area of research is the foreign policy of the United States of America. His current work focuses on US cyber security policy. He is especially interested in how advancements in Information and Communications Technology (ICT) have affected US national security in the areas of defense, homeland security, and foreign policy. Eugenio's publications also cover issues of US foreign policy toward the Middle East, democracy promotion, and international terrorism. Previously, Eugenio lectured at King's College London (2015-16), at the Joint Services Command and Staff College, part of the UK Defence Academy (2011-13), and at John Cabot University in Rome (2016). He was also Honorary Visiting Research Fellow at City University London (2015-16). Eugenio holds a PhD from King's College London, War Studies Department.

Ben Tonra is Full Professor of International Relations at the UCD School of Politics and International Relations. At UCD he teaches, researches and publishes in European foreign, security and defence policy, Irish foreign, security and defence policy and International Relations theory. Outside the university Ben has served as chair of the Royal Irish Academy's Standing Committee on International Affairs and is a co-leader of a research programme in EU security and defence at the Institute of International and European Affairs (IIEA), Dublin. Professor Tonra is a graduate of the University of Limerick (BA and MA) and completed his doctoral studies at the University of Dublin (Trinity College) in 1996.

Table of Contents

Table of Contents

Table of Contents



Network Centric Warfare with Software Defined Networks Enabled Remotely Piloted Aircraft Systems

Dr. Mubashir Husain Rehmani and Dr. Donna O’Shea
Ríomh - Intelligent Secure Systems Group, Department of Computer Science, Cork Institute of Technology, Ireland

Abstract

It is envisioned that the 22nd century military will be heavily reliant on information and communication technologies (ICT). The use of ICT in future military operations will dictate how tactical strategies will be designed. In this context, network centric warfare will provide the basis to consultation, command, and control (C3) for the military operations. In the areas behind the enemy lines, where military personnel access is dangerous, remotely piloted aircraft systems (RPAS) will be used for military operations. RPAS are generally unmanned, therefore, they need to be operated remotely and communication between the RPAS and the operator is normally established through IEEE L-Band, IEEE S-Band, and ISM Bands. The operator will issue the command and RPAS will react accordingly to complete the tasks. However, these wireless spectrum bands are susceptible to jamming by the attackers. Moreover, when these RPAS operate behind the enemy lines, there is high probability that offensive cyber operations may break their communication channels/links. Thus, there is a need to look for switching to reliable communication links frequently for RPAS. To achieve this, software defined networks (SDN) enabled RPAS are highly suitable. In this paper, we propose a counter strategy that can be adopted by the Irish Defence Forces in order to operate in an environment where offensive cyber operations have been used increasingly. We will model this problem as Multi-Armed Bandit (MAB) by using reinforcement learning (an advanced machine learning technique) to help SDN controller to learn the strategy adopted by the attacker. We also discuss that how the Irish Defence Forces will equip themselves for joint operations with UN/EU/NATO forces for SDN-enabled RPAS and what development should be implemented with professional and military education (PME).

Introduction – Why use Remotely Piloted Aircraft Systems?

Remotely piloted aircraft systems (RPAS)[1], drones, or unmanned aerial vehicles (UAVs) have numerous applications, both in urban and non-urban settings[2]. Recently, RPAS are used for commercial applications such as delivery of small packages and pizza delivery. RPAS have also been deployed to support intelligent transportation system, to serve as aerial base station[3] and for emergency drug delivery[4]. Another prominent area of RPAS' application is used in amateur applications[5] such as aerial photography, and for recreational use[6]. This wide applicability of RPAS in different urban and military applications is due to the advancement in ICT and availability of cheaper hardware devices.

RPAS are often lightweight and carry surveillance equipment over the regions which are dangerous to access by military personnel. Additionally, RPAS can be controlled remotely over several kilometres, thus decreasing precious military casualties at the cost of these low

[1] European Defence Agency Remotely Piloted Aircraft Systems: https://www.eda.europa.eu/what-we-do/activities/activities-search/remotely-piloted-aircraft-systems---rpas

[2] L. Gupta, R. Jain and G. Vaszkun, "Survey of Important Issues in UAV Communication Networks," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, (2016), pp. 1123-1152.

[3] Vishal Sharma, Navuday Sharma, Mubashir Husain Rehmani, Control over Skies: Survivability, Coverage and Mobility Laws for Hierarchical Aerial Base Stations, arXiv:1903.03725v1, 2019.

[4] Sedjelmaci Hichem, Sidi-Mohammed Senouci, Nirwan Ansari, and Mubashir Husain Rehmani, Recent advances on security and privacy in Intelligent Transportation Systems (ITSs), vol. 90, (2019), 101846, Elsevier Ad Hoc Networks.

[5] Z. Kaleem and M. H. Rehmani, "Amateur Drone Monitoring: State-of-the-Art Architectures, Key Enabling Technologies, and Future Research Directions," in *IEEE Wireless Communications*, vol. 25, no. 2, (2018) pp. 150-159.

[6] X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi and J. Chen, "Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges," in *IEEE Communications Magazine*, vol. 56, no. 4, (2018), pp. 68-74.

cost RPAS (if downed by the enemy). For tactical military operations, these RPAS are deployed redundantly and forming clusters so that mission critical tasks can be achieved - forming a RPAS network[7]. Recent examples have witnessed trials of RPAS networks as swarms, which co-ordinate with each other establishing a multi-hop communication network to increase the communication range, to relay Ground Control Centre (GCC) commands to the RPAS operating at the forefront and to achieve last mile connectivity for ground troops.

There may be few other application scenarios in the battlefield where RPAS can play its role. Imagine wireless sensor nodes are deployed in hostile environments and these sensor nodes capture different information such as images, coordinates, videos, and audio. Since these sensor nodes are energy-constrained devices, they cannot directly communicate this information to the GCC. Therefore, RPAS can visit them and collect the required information, which can then pass to the GCC for decisions, or the same information can pass to the ground battlefield troops.

5G and beyond 5G communication networks are suggested with the vision to improve user experience, more bandwidth and less delay. With these requirements in mind, the 5G public private partnership (5G-PPP) suggested to increase the number of deployed base stations, however, with such massive deployments of base stations at micro level, the expenditure to deploy, operate, and maintain i.e., capital/operational (CAPEX/OPEX) will increase. An alternative approach is to use RPAS for coverage where user traffic demands is increasing. Consequently, the resulting network will be a RPAS network. This same concept can be extended and used in battlefield environments to provide coverage and connectivity for troops on ground.

Setting the context – Network centric warfare using remotely piloted aircraft systems

Troops in the battlefield are not necessarily equipped with abundant ICT resources such as powerful wireless communication devices along with limitless energy available for them to operate[8]. It may be possible that the troops deployed behind the enemy lines may have resource constrained energy devices and wireless communication equipment. For instance, RPAS deployed for monitoring and image acquisition, wireless sensor nodes mounted on vehicles and wireless radio transceivers carried by the troops are few examples of such resource constrained energy devices.

The idea of network centric warfare was first developed by the Command and Control Research Program (CCRP), United States Department of Defence (DoD)[9]. The goal of this program was to improve the command and control activities by incorporating information and communication technologies[10].

[7] J. L. Burbank, P. F. Chimento, B. K. Haberman and W. T. Kasch, “Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology,” in *IEEE Communications Magazine*, vol. 44, no. 11,(2006), pp. 39-45.

[8] I. Zacarias, L. P. Gaspary, A. Kohl, R. Q. A. Fernandes, J. M. Stocchero and E. P. de Freitas, “Combining Software-Defined and Delay-Tolerant Approaches in Last-Mile Tactical Edge Networking,” in *IEEE Communications Magazine*, vol. 55, no. 10, (2017), pp. 22-29.

[9] D. A. Eisenberg, D. L. Alderson, M. Kitsak, A. Ganin and I. Linkov, “Network Foundation for Command and Control (C2) Systems: Literature Review,” in *IEEE Access*, vol. 6, (2018), pp. 68782-68794.

[10] A. K. Cebrowski and J. J. Garstka, “Network-centric warfare: Its origin and future,” US Nav. Inst. Proc., vol. 124, no. 1, (1998), pp. 28-35.

In network-centric warfare, the high ranked decision making echelons can use information and communication technologies (ICT) to monitor and guide troops deployed on ground leading to the creation of Network-centric RPAS system. Therefore, for a timely and informed decision, the importance of last mile connectivity of troops as well as real time information communication to both high rank decision making echelons to battle field troops is important to save lives and to avoid any collateral damage.

Advantages of using software defined networks enabled RPAS in tactical networks

The wireless spectrum bands over which the communication between the GCC and RPAS is established can be susceptible to jamming by the attackers. On top of this, since the operating scenarios of these RPAS are tactical military environments, therefore, there is high probability that offensive cyber operations may break the communication links/channels between GCC and the RPAS. This necessitates the need to incorporate resiliency within the communication network and this can be achieved by switching to reliable communication link frequently to the RPAS. On top of this, there are certainly challenges for proper functioning of these RPAS networks. These challenges include the availability of less computational on-board resources including power, best route determination, intermittent and frequent link disruption, and link jamming attacks through offensive cyber operations by the attackers.

Software defined network (SDN) is one such candidate technology which can help to support the above mentioned communication task in a flexible manner. SDN controller at GCC provides a global view of the whole RPAS network. All the activities ranging traffic and link conditions will be available to the GCC. This will help to take the global decision to facilitate longer lifetime of RPAS network and to achieve global optimal results. This global network view of RPAS network at GCC will also help enable to reduce computational power at RPAS. As a result, complex image processing algorithms as well as offline machine learning algorithms can be applied to achieve data-driven optimization.

Separation of the control and data plane with the help of SDN technology for RPAS will allow flexibility to use equipment, protocols, and algorithms, which are not vendor specific. This will also help to achieve security, as behind the enemy lines, the enemy will not be able to readily understand the working of underlying protocols. In the worst case, if the RPAS network is compromised, the SDN controller at GCC can quickly adapt to the network conditions and make the network secure and safe.

Another advantage that SDN technology will bring to RPAS network is to execute different services such as monitoring, tracking, image capturing, and co-ordinate tracking and all such services can be initialized without making any changes in the underlying hardware. Firmware update in RPAS (SDN switch) will no longer be a problem as SDN switches will be built on open source software. The same RPAS (UAV or drone) network can be used for urban setting and public safety communication. Thus, this drastically decreases the cost of maintenance and transition from one application to another. For efficient network management of these RPAS networks and to deal with fast handovers in the RPAS network, SDN seems to be an appropriate solution.

It is worth mentioning that use of technologies such as SDN to support network centric warfare is becoming prominent in military planning and operations. For instance, the United States Army proposed third offset strategy (TOS) as Department of Defence (DoD)'s innovation initiative in 2014[11]. The goal of TOS is to form long range research and planning program considering technological advancements in areas such as unmanned autonomous aircraft systems, lasers, and cognitive warfare, and other promising technologies[12]. Other similar efforts have been taken by research institutes in US such as Lincoln Laboratory in Massachusetts Institute of Technology (MIT)[13] to develop prototypes for RPAS and investigate research challenges and issues. In addition to these efforts, dedicated workshops have been taken place in US to discuss secure and reliable communication for multi-domain operations[14][15].

A reinforcement learning based counter strategy for software defined network enabled RPAS

This paper proposes to use software defined network enabled RPAS to achieve the aforementioned goals (cf. Section 2 and 3)[16]. As a result, the SDN controller on GCC will help RPAS to select reliable communication paths and thus good network performance can be achieved. The general idea is that the SDN controller at GCC will issue commands to change flow entries in RPAS (SDN switch). As a response, the RPAS (SDN switch) will update their flow tables and thus, be able to select reliable communication links/channels. Figure 1 shows the scenario depicting offensive cyber operations in tactical military environments.

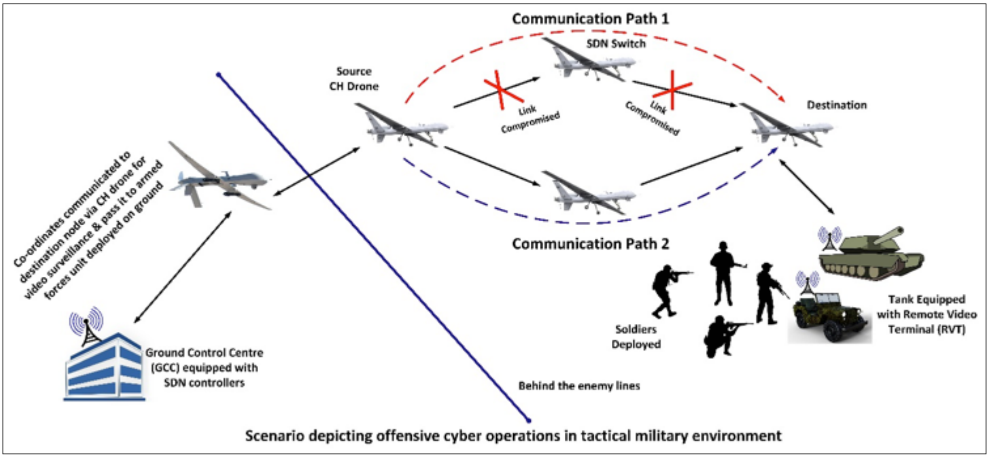

Communication Path 1
SDN Switch
Source
CH Drone
Link Compromised
Link Compromised
Destination
Co-ordinates communicated to destination node via CH drone for video surveillance & pass it to armed forces unit deployed on ground
Communication Path 2
Soldiers Deployed
Tank Equipped with Remote Video Terminal (RVT)
Ground Control Centre (GCC) equipped with SDN controllers
Behind the enemy lines
Scenario depicting offensive cyber operations in tactical military environment

Figure 1. Scenario depicting offensive cyber operations in tactical military environments

[11] https://www.iris-france.org/wp-content/uploads/2016/12/ARES-Group-Policy-Paper-US-Third-Offset-Strategy-December2016.pdf
[12] https://www.irishexaminer.com/breakingnews/business/tech/the-us-army-is-apparently-very-close-to-having-laser-weapons-723251.html
[13] https://www.ll.mit.edu/r-d/communication-systems/tactical-networks
[14] http://jointnetworks.dsigroup.org/
[15] https://futurenetworks.ieee.org/conferences/2019-workshop-tactical-and-first-responder-networks
[16] V. Sharma, F. Song, I. You and H. Chao, "Efficient Management and Fast Handovers in Software Defined Wireless Networks Using UAVs," in IEEE Network, vol. 31, no. 6, (2017), pp. 78-85.

The proposed strategy focuses on allowing the SDN controller to utilise SDN technology as an aid in learning the strategy being adopted by the attacker. [17]. Each RPAS will act as an SDN switch, which will get directions from the Ground Control Centre (GCC), where a centralized SDN controller monitors all the activities and dynamics occurring within the RPAS network. These dynamics also include the active monitoring of link characteristics. The SDN controller at GCC will be running reinforcement-learning algorithm using Multi-Armed Bandit (MAB) approach. For the sake of brevity, to avoid technical details and to consider the general audience of this article (Defence Forces Review), we ask the readers to consult Algorithm 1 of our recently published work to know the exact working of this MAB algorithm that can be applied for SDN based RPAS network[18].

In the proposed strategy, the RPAS will act as the SDN-enabled switch using OpenFlow protocol. OpenFlow protocol will be served as SouthBound Application Programming Interface (API) and help GCC SDN controller to pass the commands to the RPAS (SDN switches). A dedicated control channel will be used between GCC (SDN controller) and RPAS (SDN switches). The RPAS may be equipped with various medium access protocols (depending upon the operating environment) to communicate between each other. Note that though Satellite Communication (SATCOM) can be used to establish communication between GCC and RPAS, this research posits that it will increase the cost. Therefore, this paper suggests using IEEE L-Band, IEEE S-Band, and ISM Bands for such communications.

Professional and military education regarding SDN-enabled RPAS for Irish defence forces – A framework

The concept of RPAS based network centric warfare is not new from the EU context. For instance, the Spanish Ministry of Defence supported a two year project named DRONE for RPAS enabled network centric warfare[19]. The whole system of RPAS can further be improved by incorporating the contributions of SDN and the Irish Defence Forces can avail of the advantages of existing EU projects. In this context, the professional and military education regarding SDN-enabled RPAS for Irish Defence Forces should be provided to build the capacity of the DF.

What we are suggesting here is to promote the use of existing resources developed within Republic of Ireland to strengthen the Irish nation. We give an example of Department of Computer Science, Cork Institute of Technology (CIT) in which we have state-of-the-art online facilitates and programs. CIT has heavily invested on its private cloud infrastructure to deliver state of the art online MSc programs ranging from Cyber security to Cloud Computing and from artificial intelligence to software architecture and design[20]. These MSc program are one of its kind in the country, not only serving Irish students but students from EU and other international countries are widely taking online these courses. State-of-the-art topics regarding

[17] G. Secinti, P. B. Darian, B. Canberk and K. R. Chowdhury, "SDNs in the Sky: Robust End-to-End Connectivity for Aerial Vehicular Networks," in *IEEE Communications Magazine*, vol. 56, no. 1, (2018), pp. 16-21.
[18] M. H. Rehmani, F. Akhtar, A. Davy and B. Jennings, "Achieving Resilience in SDN-Based Smart Grid: A Multi-Armed Bandit Approach," *2018 4th IEEE Conference on Network Softwarization and Workshops* (NetSoft), Montreal, QC, (2018), pp. 366-371.
[19] I. Vidal, F. Valera, M. A. Diaz and M. Bagnulo, "Design and practical deployment of a network-centric remotely piloted aircraft system," in IEEE Communications Magazine, vol. 52, no. 10, (2014), pp. 22-29.
[20] http://cs.cit.ie/online

ICT can be taught to DF in consultation with CIT. Irish Defence Forces Training Centre (DFTC) can use the expertise developed in CIT. The Naval Service and CIT already have a strong collaboration in the shape of National Maritime College of Ireland and this collaboration can further be extended with Department of Computer Science, CIT and DFTC.

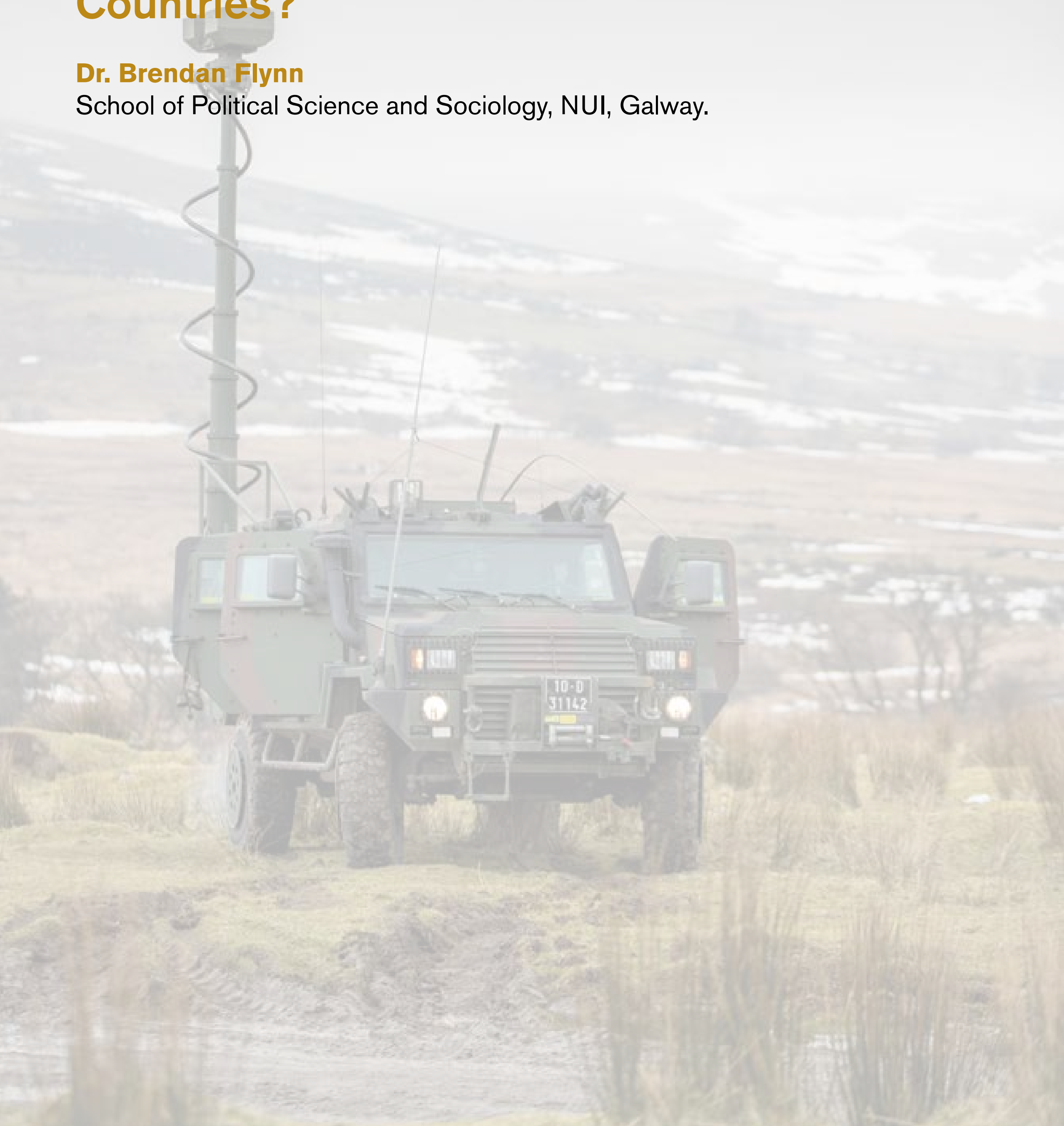
Conclusion

This paper has discussed how software defined network enabled RPAS can be used for network centric warfare to support the joint operations with UN/EU/NATO forces for SDN-enabled RPAS and what development should be implemented with professional and military education (PME) by DFTC. We also presented the advantages of using software defined networks in RPAS networks along with our proposed reinforcement learning based counter strategy to reliable RPAS communication. As plan of future work, we intend to deploy a testbed consisting of several RPAS and compare its results acquired after Mininet based simulation results. The goal is to deploy an attacker to disturb and jamming the communication between GCC and RPAS and then see how well the proposed strategy sustains under different jamming strategies and attacks.

Small States' Capability Enhancement for Peacekeeping:

What can Ireland learn from other Countries?

Dr. Brendan Flynn
School of Political Science and Sociology, NUI, Galway.



Abstract

This paper examines how small states manage technology for their future force profile in the specific domain of procurement for peacekeeping, crisis and humanitarian response missions. Given that small states typically have rather limited budgets, their ability to innovate is usually narrow. This paper explores, briefly, whether other countries offer lessons for the Irish military that are transferable? Three case studies on capability procurements are offered. These include New Zealand's procurement of a large multi-role vessel to give strategic sealift capabilities, Austria's purchase of Hercules transport aircraft conferring operational mobility, and Finland's ongoing investment in fleets of protected tactical vehicles for overseas deployments. While none of these procurements have been free from various political or technical problems, nor without significant costs, they each offer lessons in how small states can procure capabilities that offer greater operational and tactical flexibility, while enhancing their country's strategic reach and profile. The analytical point made here is that small states need to be ambitious, think flexibly and act creatively to equip their peacekeepers.

Enhancing military capabilities for small states: penny packets?

Technology and innovation will surely be central to the future force profile of all militaries, but for small states the challenges of managing such adaptations are daunting. Unlike the larger military powers, most small state militaries typically lack the scale or the large budgets to facilitate both the experiments or subsequent mainstreaming of high-tech future force innovation at the strategic, operational and tactical level. It is sometimes suggested that 'small states' can be nimble innovators, but this is usually limited to a handful of states that are either very wealthy (Singapore, UAE), or face huge military threats (Israel), and even at that they often innovate in relatively narrow areas. There is also the brutal fact of rising defence inflation associated with modern military weapons, platforms and capabilities[1]. Scale matters, and countries with limited budgets can easily end up with increasingly smaller and smaller amounts of quality capabilities-the so called 'penny packets' phenomenon[2].

Moreover, how can small states future-proof their force modernization given competing threats and demands? Peacekeeping and crisis missions are often a major focus for their militaries but require capabilities that may be of limited use for traditional territorial defence. Unfortunately, the days of doing peacekeeping on the cheap are over. While for UN operations, costs can be reimbursed albeit usually after a delay, EU peacekeeping operations generally work on a 'costs fall where they rise' principle meaning no, or only very limited, scope for reimbursement exists.

More seriously, peacekeeping operations are globally encountering greater complexity and more diffuse and lethal threats. It is not uncommon now for peacekeepers to be facing armed opponents, often non-state forces, who could employ small drones, social media, advanced anti-armour weapons, improvised explosive devices (IEDs) of a bewildering variety, sometimes combined with extreme tactics, notably 'suicide' vehicle based (VBIEDs). The future may well be a 'disrupted' scenario where aggressors threaten peacekeepers, and the populations under

[1] Hartley, Keith (2017) *The Economics of Arms*. Newcastle Upon Tyne: Agenda, pp.43-48.
[2] Till, Geoffrey (2014) "Are Small Navies Different?", pp.21–31 in Mulqueen, Michael, Deborah Sanders and Ian Speller (eds.). *Small Navies: Strategy and Policy for Small Navies in War and Peace*. Farnham: Ashgate. At p.23.

their protection, with a blend of old and new weapons, tactics and strategies: Kalashnikov and machete wielding militias with 3-D printed drones and mobile phone based offensive cyber hacking and jamming capabilities[3].

There has also been a shift in UN peacekeeping doctrine which places increasing emphasis on protection of civilians and human security, as much as force protection, and several UN missions have been criticized for neglecting the former, although depends on the details of a specific mandate as to how extensive such responsibilities can be. The implication of this is that tomorrow's peacekeepers will require a balance between assets that protect themselves, and the type of mobility and firepower that allows them to protect specific populations at discrete sites, such as refugee camps.

The days of deploying lightly equipped basic infantry units in soft-skinned vehicles, protected by their organic small arms and the blue UN flag are long gone. More flexible and joint forces seem required, blending air, naval, intelligence specialists with local and other friendly forces. Military co-operation with civilian decision-makers, agencies and NGOs has become essential. Peacekeepers must be situationally aware and have excellent intelligence, with greater levels of intrinsic force protection all of which tends towards numerically smaller deployments but with higher technology needs and often a greater logistical footprint.

For some small states, one can discern a trend towards providing tiny niche forces, sometimes following a Special Forces template, with the lightest of vehicles and weapons, de facto operating under the logistical and protective screen of larger forces. However, this often places such units at the operational mercy of other contingents, and the political influence of niche units is easily diluted. A small state that always contributes a sub-platoon sized detachment of Special Forces will not likely be given senior command positions or be much listened to at the operational mission level[4]. If small states want to be relevant and influential in peacekeeping, they need to figure out how to offer force packages that cross a threshold well beyond the tokenistic or niche nor have them burdened by excessive national political caveats that limit their operational flexibility. This implies land units of at least reinforced company size, and credible aerial and maritime assets as well. In the following sections three diverse small states are examined to draw lessons about force modernization with regard to specific procurements relevant for peacekeeping.

[3] On insurgent abilities for electronic and communication warfare see Gorman, Siobhan, Yochi J. Dreazen, and August Cole, "Insurgents hack US drones." *Wall Street Journal* December 17th, 2009, and Doubleday, Justin. "Russia-backed insurgents have' exceptional' jamming capability: US Army Joins Ukraine's Electronic-Warfare Fight Against Rebels." *Inside the Army* 27, no. 4 (2015): 4-5. For a more reflective piece: Weinbaum, Cortney, Steven Berner, and Bruce McClintock. S*IGINT for anyone: The growing availability of signals intelligence in the public domain*. No. PE-273-OSD. RAND Corporation Washington United States, 2017; On the ubiquity of new technologies such as mobile phones alongside old technologies see: Macdonald, Fraser, and Jonathan Kirami. "Women, mobile phones, and M16s: Contemporary New Guinea highlands warfare." *The Australian Journal of Anthropology* 28, no. 1 (2017), pp.104-119; See also: Lewis, Jeffrey William. "The Human Use of Human Beings: Suicide Bombing, Technological Innovation, and the Asymmetry of Modern Warfare." *Global Politics Review* 2, no. 2 (2016): 9-27. On insurgent use of drones see: Bunker, Robert J. *Terrorist and insurgent unmanned aerial vehicles: Use, potentials, and military implications.* Army War College Carlisle Barracks, P.A., Strategic Studies Institute, United States Army War College Press, 2015, https://apps.dtic.mil/dtic/tr/fulltext/u2/a623134.pdf; Esther, Ulrike. "The global diffusion of unmanned aerial vehicles (UAVs), or 'drones'," pp. 78-98 in Aaronson, Mike, Wali Aslam, Tom Dyson, Regina Rauxloh (eds.) Precision strike warfare and international intervention: strategic, ethico-legal and decisional implications. Routledge, 2014; On the lethality and prevalence of simple and old weapons like machetes see: Verwimp, Philip. "Machetes and firearms: The organization of massacres in Rwanda." *Journal of Peace Research* 43, no. 1 (2006): 5-22, or for a more general overview see Chapter 6 on "War" in Edgerton, David. The Shock of the Old: Technology and Global history since 1900. London: Profile, 2006.

[4] Note this observation is not a critique of contributing special forces to peace-keeping missions per se. They can provide excellent situational awareness, vital intelligence and are ideal for local forces training and interaction. The point is that such small force elements are not a substitute by themselves for a more substantive national peacekeeping presence.

New Zealand's procurement of a large multi-role vessel-buying into jointness?

Peacekeeping remains a core operational priority for the New Zealand Defence Forces[5], and while some of these operations have been classic UN led missions, such as UNTSO[6] in the Golan, or the Sinai based MFO[7], others have been more controversial and challenging, notably the deployment of NZDF special forces deployments in Afghanistan.

Peacekeeping operations close to home in East Timor (1992-2012), the Solomon Islands/ Bougainville (2003-2013), and Tonga (2006) were intensive and reinforced the importance of having credible maritime logistics and amphibious capabilities for remote regions. Aviation assets could not reach every location nor deliver bulky supplies economically. The NZDF have also engaged in peacekeeping or maritime stabilization operations much further away: an infantry force in Bosnia (1994-96), making a P-3K Orion available to NATO and then EUNAVFOR off the coast of Somalia and deploying a frigate in the Aegean with NATO's Operation Active Endeavor[8].

To be globally relevant, the small and geographically remote NZDF has had to adopt an expeditionary mindset as a default setting and the ways and means to give effect to this. Crucially this strategic orientation has been recognized in successive official policy statements[9] and in procurement decisions.

Accordingly, in 2004 the New Zealand government gave approval for a Multi-Role Vessel (MRV), which is a logistics ship with some amphibious operationally capability. This was commissioned into service in 2007 as HMNZS Canterbury. In fact, the idea for such a ship was a long-standing goal[10] and today there is a contemporary trend for MRV procurement with several designs available. To save money, the Canterbury was based on a modified commercial ferry.

[5] McDougall, Derek. "Peacekeeping from Oceania: Perspectives from Australia, New Zealand and Fiji." *The Round Table* 106, no. 4 (2017): 453-466. For an up to date list of NZDF deployments see: http://www.nzdf.mil.nz/operations/default.htm

[6] Typically, about 8 NZDF observers. See: https://untso.unmissions.org

[7] See: http://mfo.org/en

[8] On the New Zealand Navy, see: Paget, Steven. "The 'best small nation navy in the world'? The twenty-first century Royal New Zealand Navy." *Australian Journal of Maritime & Ocean Affairs* 8, no. 3 (2016): 230-256.

[9] See for example the Defence White paper of 2016, at pp.20-22. http://www.nzdf.mil.nz/downloads/pdf/public-docs/2016/Defence-White-Paper-2016.pdf

[10] In 2002 a Maritime Forces Review was conducted which suggested an entire integrated procurement programme, "Project Protector", which included dropping a third frigate for a more flexible multi-role vessel. Before that, in 2000, a report on Sea-lift capabilities had suggested such a vessel be procured. Tringham, Kate (2016) 'Canterbury tales re-told: RNZN multirole vessel deliver', *Jane's International Defence Review*, 8th June. Available at: http://www.defence.govt.nz/assets/Uploads/Canterbury-tales-re-told-RNZN-multirole-vessel-delivers.PDF

In retrospect it might have been better to go with a more conventional and proven amphibious support ship, because the initial entry into service was delayed by vessel handling, sea-keeping and ballast problems. However, buying a traditional amphibious warfare ship would have been much more costly, revealing a tension between being cost sensitive on the procurement of very large and expensive assets versus running higher project management risks of technical problems in meeting the desired specifications. Small states watching every penny can end up skimping which means in the end actually spending more!

Moreover, these technical woes became for a brief period quite politicized after a fatality aboard and no less than two separate court of inquiries and an independent expert commission appointed to investigate[11]. A number of technical fixes were quickly adopted, and the shipbuilders made a substantial financial settlement. Today it appears the NZ Navy are quite happy with the vessel and in 2016, it was hard at work responding to a cyclone hit Fiji islands.[12]

The lesson here is that large-scale technically complex procurements require careful project and political risk and communications management over the long-life cycle of the project, with swift action to mitigate problems. There was sufficient institutional leadership within the NZDF and the NZ Defence Ministry to see the project to its conclusion, a vital prerequisite for what has been on balance, a procurement success.

The vessel was deployed operationally, in 2009, after a Tsunami struck Samoa and again in dealing with the aftermath of natural disasters in Canterbury city (2011) and Vanuatu and Fiji (2015-2016). The vessel demonstrated a unique ability to deliver thousands of tons of aid and vehicles in roll-on-roll-off fashion, while also providing a secure offshore floating base for co-ordination in situ[13].

From the perspective of force modernization, Canterbury is the lynchpin for a Joint Task Force concept which integrates NZDF land elements with air force expertise on helicopters all in a combined tactically deployable and logistically resilient 'package'[14]. The NZDF can deploy a reinforced mechanized infantry company, their armoured vehicles and then sustain them from ashore for up to 30 days, including providing them with command, control and intelligence functionality from the ship as floating base, well beyond their entire Exclusive Economic Zone. In this way the vessel has become a laboratory for 'jointness' across the entire NZDF, and a good example of how some procurements have multiple force level benefits.

[11] Tringham, Op.Cit.
[12] See: http://www.navy.mil.nz/mtf/cant/default.htm
[13] Paget, p.238-239.
[14] Paget, p. 241-242.

Austria's purchase of Hercules transport aircraft: second hand heavy-lift for peacekeeping.

Like Ireland, Austria has a strong track record in peacekeeping, often in the classic UN led operations but with a strategic culture very different from New Zealand, avoiding the use of force or more kinetic roles[15]. Unlike Ireland, Austria is landlocked so does not require a navy, and Austrian neutrality historically was different from Ireland's experience, being originally imposed by the Soviet Union as a condition of the return to full sovereignty in 1955. Nonetheless, like Ireland, Austria remains outside of any formal military alliance and military spending is low, even though a small domestic arms industry exists.

Because Austria is land-locked, heavy air lift has become a vital issue for participation in overseas peacekeeping. Many European states have experimented with different ways to secure heavy airlift, which is not easy because the huge aircraft involved are very costly.

Since 2009, there is a so called *Heavy Airlift Wing*, based in Hungary, which pools a fleet of three C-17 strategic airlifters, access to which is shared among 10 NATO member states as well as Sweden and Finland. Since 2010, the European Air Transport Command (EATC), based in the Netherlands, is a consortium of seven EU states[16] that have agreed to pool their large aerial refueling aircraft and a suite of strategic and tactical airlift transporters (A400M, Hercules, C295, etc.). It has on its books (actually a rota of 'hours per tonne of cargo') over 200 aircraft or about 75% of the European air transport capacity[17]. Since 2006 the German led Strategic Airlift Interim Solution (SAIIS), has provided a pool of Russian AN-124 giant aircraft available for NATO and EU heavy lift requirements, however, since 2018 this contract has been non-functioning due to ongoing tensions with Russia[18].

For many years, the only air transport assets available to Austria were just two Shorts Skyvans. Austria has not participated in any of these 'pooling' arrangements because the decision was made in the late 1990s to procure their own heavy lift air transport assets, the only question being how to afford these. Three ex-RAF C-130K Hercules were procured in 2002-2003 in a

[15] Schmidl, Erwin A. (2013) 'Peacekeeping Contributor Profile: Austria', *Providing for Peacekeeping,* at http://www.providingforpeacekeeping.org/2014/04/03/contributor-profile-austria/

[16] Britain is leaving the EU but remains apparently committed to the EATC, so it is actually six: France, Germany, Netherlands, Spain and Italy, with Belgium operating its own and a single A400M for Luxembourg.

[17] See: See: https://eatc-mil.com/en

[18] Waters, Will, (2018) 'Volga-Dnepr confirms withdrawal from NATO SAIIS contract', *Lloyd's Loading List*, Tuesday, 01 May 2018. While other commercial air charters are available for military cargo, they cannot economically carry outsize loads such as helicopters and the heavier armoured vehicles.

government to government sale managed by the UK's MoD Disposal Service Agency, explicitly to support overseas peacekeeping. These aircraft were refurbished to a high standard[19] by Marshall Aerospace when originally delivered, and again after the Chad deployment in 2011 and 2013, including the fitting of some basic defensive aid suites[20]. The later expense probably reflected concern over risks of surface to air missile attack. As part of the deal, Marshall Aerospace were also contracted to provide technical service support and training was provided for up to 9 crews.

These reconditioned aircraft certainly proved their worth in 2009 in Chad: at least 125 flights were undertaken with 2,135 tons of cargo and the aircraft were also heavily tasked with support of Austrian peacekeepers in Kosovo and Bosnia. Another important mission was in response to the Asian Tsunami disaster in 2004. However, these assets are only enablers of mobility for peacekeepers and the Austrian's discovered during their 2009 Chad deployment that if the main airport in any particular theatre is seized by hostile elements there is no way such vulnerable aircraft can land, reinforcing the importance of joint capabilities to secure airbases[21].

Finland's ongoing evolution of protected tactical vehicles

The final case examined here concerns land mobility for peacekeepers, looking at Finland. The Finnish situation is quite different from Ireland, with their conscript armed forces oriented towards large-scale territorial defence. This means peacekeeping vies for salience with the need for a large mechanized land army (*Maavoimat*). There is also a domestic arms industry and therefore political pressure to buy Finnish.

The Finns (and Ireland) deployed the large, 1980s era, SISU *Pasi* armoured personnel carriers (APCs), successfully in the Lebanon during the 1980s and 1990s[22] However, the SISU's were relatively bulky and unwieldly, and while they had reasonable resistance to IEDs they had

[19] According to one source these revisions included: "structural upgrade, major servicing and installation of an automatic flight management system, upgraded avionics, a traffic collision avoidance system, INS navigation system, digital engine and fuel management systems and the Rockwell Collins FMR-200x colour weather radar." Ayton, Mark (2003) 'Herks for Austria', Air Forces Monthly, May, pp.68-69.

[20] Mader, Georg (2010) 'Survey Austria: On the Edge', *Air Forces Monthly*, Feb, pp.74-78.

[21] Early on in the Chad mission, rebels seized the Capital's airport which prevented an Austrian Hercules from landing and for a short while, French and Austrian forces were cut off and exposed. See: Tonra, Ben. "The (In) Justices of Peacekeeping: EUFOR Tchad/RCA." GLOBUS Research Paper 3 (2018), p.11.

[22] In an interesting precedent, some of these vehicles were actually bought by the United Nations and indeed the UN continues to be a buyer of armoured vehicles. By getting UNIFIL and the UN to adopt and pay for a fleet of APCs the *Maavoimat* had a ready pool of vehicles in situ. Semi-permanent overseas basing of vehicles and/or buying vehicles, perhaps through the auspices of the UN as a shared asset, are just two possible approaches which a country like Ireland could consider in future.

deficiencies in turret protection. For these reasons it became increasingly obvious they were not ideal. Both the Irish and Finnish army had encountered the South African RG31 mine resistant vehicles in the Lebanon and in Eritrea which were effective in reducing casualties.

Experience in Afghanistan, where since 2002 the Finns deployed a small contingent with ISAF under a UN mandate, offered a number of steep learning curves. In 2006, the Finnish army, concerned about deployability[23] and the IED threat, choose a much smaller (under eight ton) light armoured vehicle (LAV) from a non-national supplier, initially just six BAe RG32M which is a smaller development of the RG31 in some aspects[24]. This order was repeated in 2010 (26), in 2011 (23) and again in 2012 (25) bringing their total fleet to well over 70[25]. Interoperability with the EU Nordic Battlegroup countries may have influenced this procurement, as it's also used by Sweden (200 examples) and Ireland purchased 27 in 2010[26]. It is important to note that the RG32M is conceived of as a scout or reconnaissance vehicle, replacing the use of jeeps or Landrovers in such roles and offering some degree of protection from shelling, ambush and mines. However, it is not a vehicle designed for combat, lacking sufficient armour, nor is it a proper APC or MRAP.

The Finns deployed the RG32's in Afghanistan as soon as possible and in 2009 one of these was hit by an IED. The crew survived, albeit injured[27]. If there was a complaint, apart from cramped vehicle ergonomics[28], it was that there were never enough RG32s. Widespread use had to be made of unprotected trucks and G-Wagens alongside the older *Pasi*. Moreover, by 2011 it was evident such vehicles need better ability to protect themselves if ambushed, so manual weapon mounts/shields were procured, which are much cheaper than remotely operated weapon stations, and simpler to maintain overseas [29].

The Irish have also deployed the RG32M overseas, in UNIFIL and UNDOF. With its increased mine and kinetic protection, it is an ideal fit for an overseas environment. It has been learned however that it's important prior to deployment to adopt an holistic approach to training for operations and maintenance to maximize mechanical reliability and readiness. The Finns by buying different procurement batches have mechanical variations, which challenges maintenance, notably for the older vehicles[30]. However, there is dedicated Finnish maintenance company, MILORG, which provides advanced technical support for the *Maavoimat*.

The contrast with Ireland is interesting, because apart from the small batch of 'one off' RG32M purchased and deployed in small number, the Irish DF have consistently relied more on the

[23] BAE bought up the South African firm that produced the specialised mine resistant RG31 and the RG32 was a newer, substantially different, variant. Two RG32s fit in a Hercules transport plane. Unlike Austria, Finland does not have any of these aircraft although it has excellent C295 medium transports (a modern version of Irish Casa 235s). Yet Finland is a member since 2009 of the Heavy Lift Group, based in Hungary, which pools a fleet of just three huge C-17 strategic airlifters and gives access to these aircraft to the members of this group 10 NATO member states as well as Sweden.

[24] See: http://www.deagel.com/news/Finland-Orders-16-RG-32M-Armored-Vehicles_n000007337.aspx

[25] The costs of the final trance was estimated at €12.5m in 2012 values. See: Army Technology News, (2012) 'Finnish Army orders additional RG32M vehicles from BAE, 4th June', https://www.army-technology.com/news/newsfinnish-army-orders-additional-rg32m-vehicles-bae/

[26] The Irish Army variant is different.

[27] Overall Finland lost 2 soldiers and had 11 wounded in Afghanistan. See: https://web.archive.org/web/20160109100128/http://news.xinhuanet.com/english/2009-10/03/content_12178191.htm.

[28] Halvarsson A., Hagman I., Tegern M., Broman L., and Larsson H. (2018) 'Self-reported musculoskeletal complaints and injuries and exposure of physical workload in Swedish soldiers serving in Afghanistan', PLoS ONE 13(4), p.12

[29] http://www.asdnews.com/news-44536/finland_orders_weapon_stations_for_rg32m.htm

[30] Lepoaho, Jussi (2015) *Millog Oy Käytettävyyden Tuottajana – Partioajoneuvo RG32M-Millog as an availability service producer-Patrol Vehicle RG32M*, Masters Degrees Thesis, Jamk University of Applied Sciences,p.20-21, https://www.theseus.fi/bitstream/handle/10024/97287/Jussi_Lepoaho%20YAMK.pdf?sequence=1

heavier *Pirhana* vehicles, with the consequence that these must be either transported by sea or very elaborate arrangements have to be made for air heavy lift. The commercial market for outsize heavy lift aviation is dominated by Russian aircraft and companies, and given the current EU sanctions regime in place, political risk has now made such solutions unreliable.

This nicely illustrates how procurements are interlinked: because Ireland has invested in a *Pirhana* fleet as the primary vehicle for peacekeeping deployments, this makes a dedicated sea mobility solution the most logical and economic way of transporting the 14 *Pirhanas* typically required for an Irish infantry company. The Finns have other options because of their 'share' in the Heavy Lift Wing and because they have more than enough lighter RG32s to equip an entire company element if they chose to. New Zealand's Defence Force has the option of transporting large number of Pirhana sized vehicles on their Canterbury and they even have a few Hercules as well.

Drawing Lessons from other Small State Procurement

What are the general lessons to be drawn from these cases for peacekeeping related procurements?

The first two cases concerned strategic mobility, rather than enhancing firepower or protection. Austria in some ways must invest in heavy lift aircraft because it is land locked and has chosen the cost-effective way of refurbished second hand aircraft. While these aircraft have a good few years of service left, in the longer term some sort of pooling arrangement seems logical for countries like Austria. Ireland has excellent but rather small CASA 235 assets and if these were replaced in future, they could potentially be pooled with partner countries, to add value and reduce costs[31].

Ireland has much firmer plans to procure a Naval Service MRV[32], and the New Zealand experience suggests that while such an asset does not come cheaply, it provides force wide transformational benefits and a robust strategic mobility that is more resilient than heavy-air lift. In time, European navies may begin pooling their logistics and support vessels following the EATC template in some guise. The New Zealand MRV experience also suggests the merit of procuring proven designs and avoiding false economies. Such assets are a one in a generation capability and worth getting right.

Finland's evolving protected vehicle fleets offers a number of more specific lessons: (1) a special 'pool' of protected vehicles is required for overseas peacekeeping that are easily transportable and interoperable with other forces; (2) a sufficiently large number of vehicles is required to be built up over time-it is no good buying a once off small job-lot; (3) armour protection must evolve regularly in iterative updates, because threats against peace-keepers continue to evolve; (4) protection cannot be the only criteria to select vehicles, there also has to be a balance towards mobility/deployability and appropriate firepower. Crucially, like the experience with HMNZS Canterbury, if technical problems do arise, then a long-term life cycle management approach is needed using a Mid Life Upgrade to resolve any shortcomings. In this regard, one

[31] At the time of writing Ireland had an open tender process for replacement aircraft for the CASA235s. See: https://www.oireachtas.ie/en/debates/question/2019-02-20/81/

[32] At Para.6.5 Department of Defence. *White Paper on Defence.* Dublin, DoD, 2015. Available at: https://www.defence.ie/system/files/media/file-uploads/2018-06/wp2015eng_1.pdf

very positive Irish development is the commitment in the Irish White Paper on Defence (2015) to develop a funding model study that facilitates long-term planning and financing for life-cycle procurement and updates[33].

Overall, these case studies taken together reinforce the need for joint capability enhancement-allowing land, air and sea elements to combine and understanding the interactions between them. To be effective land units need mobility and air and sea assets confer this in different ways, but equally the protection offered by hardened land forces is essential if ships are to dock and aircraft to land.

All three examples are vehicles of some type, and this paper has not studied weapons procurement, or the many other essential items of equipment modern peacekeepers require. Nonetheless it should be evident that a balance needs to be found between procuring for force protection and investing in capabilities that will permit defending civilians and the ability to enforce mandates flexibly.

Finally, all of these cases show small states can be ambitious, creative in their thinking and flexible in their actions. Moreover, the clearest lesson perhaps is the importance of national political *ambition* to resource peacekeepers as best as they can. Even though Finland, Austria and New Zealand have actually lower levels of GNI per capita than Ireland[34], they have all found the required funding to purchase new capabilities that improve their peacekeeping presence in the world. Has Ireland's public and political leadership demonstrated that same level of support for ambition, creativity and flexibility in equipping our Defence Forces?

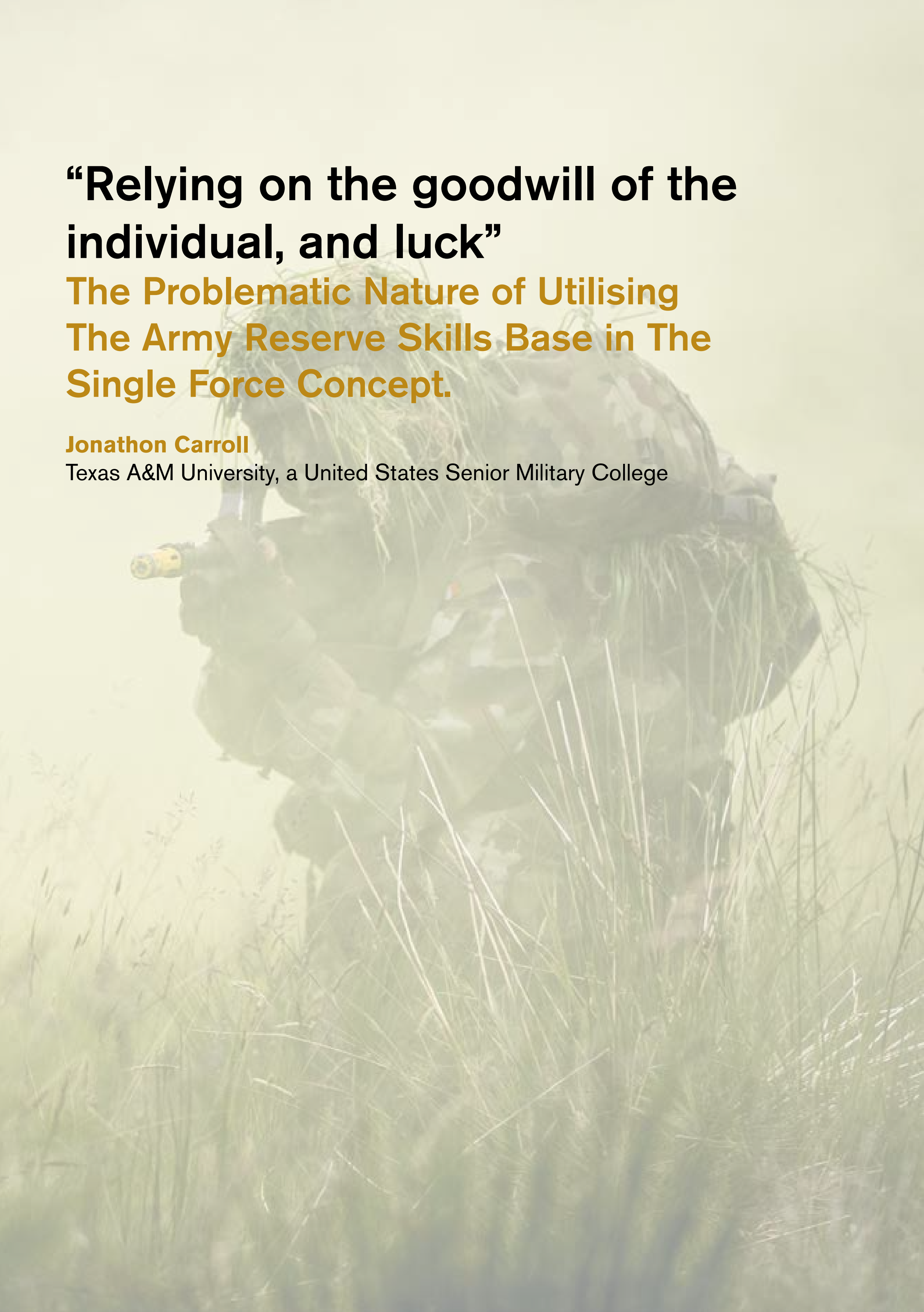
[33] See Para.10.4.3 in DoD, Op.Cit, 2015.

[34] Gross National Income is used rather than GDP which suffers from distortion, moreover it is easier to make comparisons at the per capita level with purchasing power parity (PPP). According to World Bank Data, Austria had a GNI PPP for 2018 of US$55,960; Finland of US$48,490; New Zealand of US$40,250 and Ireland was the 'richest' with US$66,810. See: https://data.worldbank.org/indicator/NY.GNP.PCAP.PP.CD?year_high_desc=true

“Relying on the goodwill of the individual, and luck”

The Problematic Nature of Utilising The Army Reserve Skills Base in The Single Force Concept.

Jonathon Carroll
Texas A&M University, a United States Senior Military College



Abstract

Recently, the role of reservists, particularly in the Communications Information Systems (CIS) Corps, in developing and enhancing technological solutions through the application of skills gained from civilian careers and educational qualifications has yielded interesting results. While showcasing the potential contributions reservists can make, such results should not be mistaken as capability-building, nor of the long-awaited harnessing of skills to the Permanent Defence Forces that reservists possess. Reservists in the CIS Corps have made excellent strides in technological innovation. However, such strides have only been made possible by a combination of the goodwill of these individual reservists, and luck. The example of the CIS Corps is the exception, not the rule. The Army Reserve by reason of legislation, and structural organisation is largely prevented from enabling the meaningful application of reservists' skills in technological innovation or in any area of specialisation beneficial to the wider Defence Forces. This paper draws on research conducted into the Army Reserve and the Single Force Concept to argue that there are significant obstacles preventing the Permanent Defence Forces from absorbing the skills base provided by the Army Reserve. Consequently, far from capability-building, any lasting application of skills in areas including technological innovation and development is almost impossible. In making this argument, this paper will examine factors enabling reservist skill contribution, including the example of the CIS Corps, but will also suggest that the current force structure, and organisational practices governing the Army Reserve prevent the efficient use of reservists' skills. Furthermore, the legislation surrounding service in the Army Reserve will also be examined to highlight the problematic nature of retaining skilled reservists, or even utilising skilled personnel where necessary. Finally, the Irish model will be compared briefly with international best practice. Any debate surrounding a 22nd Century military must acknowledge that in the Irish context, the mechanisms of utilising reservists' skills, are fundamentally outdated.

Introduction

In 2015, reservists in the CIS Corps developed a system of transmitting encrypted video and audio data via mobile phone signals. The system was tested for operational viability with the Nordic EU Battlegroup and was due to be used by the Irish contingent of the German-Austrian Battlegroup in 2016.[1] However, legislative barriers to reservists serving overseas meant the personnel who designed, and were best suited to operate this system, could not participate in the mission readiness exercise in Germany.[2] Their professional innovation, developed outside the Defence Forces, showcased both what reservists can contribute to the Defence Forces and the practical limitations of their engagement.[3] Reservists in the CIS Corps, however, are the exception, not the rule. In the age of growing cyber threats, the CIS Corps, arguably the corps with the most potential in harnessing reservists' skills, fell afoul of the reality that, for many reasons, the Defence Forces cannot effectively harness the specialised skills reservists possess.

[1] Commandant A (PDF), interviewed by author, January 2016.
[2] Commandant A (PDF), interviewed by author, January 2016.
[3] Commandant F (PDF), interviewed by author, January 2016.

Legislative Obstacles and Legislative Non-Existence.

The Defence Forces cannot harness reservists' specialist skills efficiently, meaningfully, or reliably due to legislative weakness. Modern militaries require a dependable skill base for capability development, skill maintenance and skill projection. This is critical where specific skills are in short supply or are to be found outside the regular military force. A lack of skilled personnel means reduced capabilities. Reserve forces mitigate this problem by providing a pool of skilled individuals. For instance, in 2013, during the wars in Iraq and Afghanistan, 38% of the British military medical infrastructure was staffed by reservists.[4] However, a reserve force is only as good as its legislative enablers. In the Irish context this is the Defence Act 1954, the principle legislation governing the Army Reserve and its utilisation. Reservists can be called up by the Minister of Defence in a "state of emergency", or in an Aid to the Civil Power scenario for the "restoration of the public peace."[5] While a mechanism exists for calling out the Reserve for large-scale emergencies, there is none for utilising skilled reservists on an individual basis in a situation not requiring full force deployment. Compounding the issue is the legal situation surrounding a reservist, if called up. Technically speaking there is no realistic punishment for not reporting for duty when required. The legal status of a "reservist" is also a grey area.[6] Added to this is the absence of any employment protection legislation, guaranteeing reservists' civilian employment if called up to extraordinary military service. Likewise, no legal obligation exists on employers to release reservists for duty, even in an emergency. Thus, the supply of specialist reservist skills to the Defence Forces depends entirely on the ad hoc goodwill of the individual reservist, and their employer. In a conflict of interest, between a reservists' military obligations and their civilian employment, who will the reservist more likely obey, their employer who pays their salary and governs their future employment and promotion prospects, or the Defence Forces offering neither substantial remuneration, nor job protection? Emergency scenarios aside, and dialling back the level of national calamity to the current benign setting, can reservists be expected to contribute specialist skills, and time, with all the pull factors being in favour of their employer whilst the push factors work against the Defence Forces? The simple answer is no, yet no action has, or is currently, being taken to change this calculus.

Employer Engagement

The problem could be eased, not solved, with meaningful employer engagement. Liaising with employers to facilitate reservists attending training and committing their skills to the Defence Forces was suggested in 1999.[7] After 20 years, the only output of employer engagement is the *Reserve Defence Forces Employer Information Booklet*, published in 2016. This merely encourages employers to look kindly on reservists by granting annual or unpaid leave to attend training. There is no mention of reservists being called up in an emergency, or that a skilled reservist

[4] Ministry of Defence, Reserves in the future force 2020 (London: Ministry of Defence, 2013), p.73.
[5] The Defence Act 1954, s.87 and s.90.
[6] Reservists are neither employees nor workers of the Department of Defence, they are classified as "volunteers." Dail Eireann 22 Apr. 2008, parliamentary debates; official report, vol. dclii, 2008 [no.2] (Dublin, Stationary Office). Furthermore, unlike members of the PDF, section 118 of The Defence Act 1954 states that reservists are only under military law, and subject to military discipline whilst in uniform. Moreover, section 243 of the same Act states that if a reservist fails to report for duty they can be charged with desertion or being absent without leave which only incurs a monetary fine as opposed to a custodial punishment. But, even if a reservist commits this offence they must present themselves, in uniform, to be charged. Therefore, theoretically, if an individual simply does not present themselves they will not be punished. Lt. Col. B (PDF), interviewed by author, January 2016.
[7] Department of Defence, Report of the steering group on the special study of the Reserve Defence Force (Dublin: Government Press, 1999), p.5.

might be required by the Defence Forces for an extended period due to their expertise.[8] Despite considerable work putting it together, the handbook does not tackle the problem at all. It assumes compliance and cooperation at all levels from employers without incentive, or an established tradition of cooperation. Other countries, such as Britain and America, that enjoy a strong societal martial tradition have nevertheless resorted to legislation to guarantee this cooperation.[9] That skilled individuals might be required by the Defence Forces may become a real possibility, indeed an opportunity for the Army Reserve, given the current personnel retention crisis. By failing to mention this, employers, who could have been geared up for the *possibility* years ago may consider the last-minute request for their employee to be absent for an extended period to be more trouble than it's worth. For their part, the committed reservist may be forced to choose between their sense of duty, and their employment.

The suggestion of employment protection legislation has been made consistently by those arguing the tangible benefits for the Defence Forces. In contrast, others argue such legislation is a "double edged sword" with the potential consequence of employers not hiring reservists due to their military obligations.[10] Justifying this is the reality that, despite Ireland's anti-discrimination laws, there are still cases where discrimination, based on gender for example, still occurs.[11] Nonetheless, such legislation would protect, at most, 3,869 personnel in the Army Reserve if at full strength. Illegal discrimination, were it to occur, would likely affect only small number of reservists, who would have legal redress. On balance, the decision lies between providing a credible Reserve with a pool of skilled personnel, and, avoiding instances of workplace discrimination. Thus far, there has been no appetite to amend legislation as it has been argued that there has never been the need to deploy the Reserve.[12] This ignores the large FCA deployments to the border during the Troubles, the regional deployments during the 2015 Shannon flooding and future possible contingencies arising from Brexit.[13] The double-edged sword cuts both ways as the government and Defence Forces are deterred from using the Reserve because reservists, in reality, can choose not to report for duty.[14] No system exists to compel or incentivise them to do so, and a material benefit to not contributing their skills exists in the form of keeping their job, and being paid adequately for their time.

[8] Department of Defence, Reserve Defence Forces Employers Information Booklet (Dublin: Department of Defence, 2016).

[9] In the British Army Reserve, the *Reserve Forces Act 1985* guarantees a reservists' employment if deployed. Furthermore, any employer who loses an employee due to overseas deployment with the Reserve is paid compensation by the government to offset any loss suffered and to facilitate the employment of a temporary replacement. Ministry of Defence, 'Rights and responsibilities for reservists and employers' (https://www.gov.uk/employee-reservist/financial-support-for-employers) (4 Jul. 2016). In the United States, the *Uniformed Services Employment and Reemployment Rights Act 1994* prohibits any discrimination or reprisals against members of the National Guard or the Reserve forces either in terms of being employed, or for being deployed. The Act dictates that reservists deployed overseas shall not suffer in their civilian employment as a result of having to serve. As such, in the event of deployment a reservists' position is guaranteed to be waiting for them upon their return with no loss of pay or career potential. The Act guarantees employment as if the deployment never occurred.

[10] Lt. Col. C (PDF), interviewed by author, January 2016.

[11] Main Political Party T.D. H, interviewed by author, April 2016.

[12] Main Political Party T.D. H, interviewed by author, April 2016.

[13] Beginning in 1969 the FCA provided garrison duties for a PDF that required time and the establishment of three new infantry battalions to adequately secure the border with Northern Ireland at the outset of the Troubles. This resulted in the formation of the 27th, 28th and 29th PDF Infantry Battalions; John P. Duggan, *A history of the Irish Army* (Dublin: Gill & MacMillan, 1991), p.281. Reserve personnel from 1st, 6th and 12th Infantry Battalions along with elements of 1st Brigade Transport Company were utilised in flood relief efforts in 2015. Mr. Neil Richardson, General Secretary RDFRA, interviewed by author, May 3, 2016.

[14] Lt. Col. B (PDF), interviewed by author, January 2016.

The Overseas Problem

The most practical application of specialist reserve skills in modern militaries is overseas deployments. For the Army Reserve this has been an issue of some cultural contention within the Defence Forces. The deployment of reservists overseas is illegal.[15] Internationally, the benefit of using reserve forces overseas has been clearly demonstrated. During Operation Iraqi Freedom in 2004, 37,000 of the 118,000 American troops in Iraq were reservists, and in 2005 half of American combat brigades were units of the Army National Guard.[16] Ireland is not at war, but an example exists showing the potential of harnessing skilled reservists being undermined by the system, or lack thereof. This is the abovementioned example of the reservists' contribution to the 2015 EU Battlegroup. Undoubtedly, the core rationale for these reservists serving overseas is that these individuals had the skills to operate the system they had designed, to troubleshoot malfunctions, provide on the spot technical expertise and to further develop the system based on field experience. These reservists were legislatively prevented from deploying for the Battlegroup exercise to put the fruits of their expertise and efforts into action. Even if legislation enabled reservists to serve overseas, their civilian employer would still be the final arbiter as to the Defence Forces having the benefit of their presence. It must be remembered that "overseas" for a reservist means anything outside the territory of the Republic of Ireland, even for just an exercise. The suggestion of sending suitably qualified individual reservists overseas has been repeatedly made in policy documents and reports.[17] A pilot program, possibly trying to circumvent the legislation, was established in 2009 for KFOR, and then quickly abandoned.[18] Policy ambitions and recommendations aside, the current legislation bars the deployment of reservists overseas. Consequently, the doctors, logisticians, cyber security specialists, engineers and many other skilled and experienced reservists remain unavailable to the Defence Forces, abroad, or even at home. Within the Defence Forces, senior officers have described this as "completely outdated" and "farcical" in comparison with international best practice.[19]

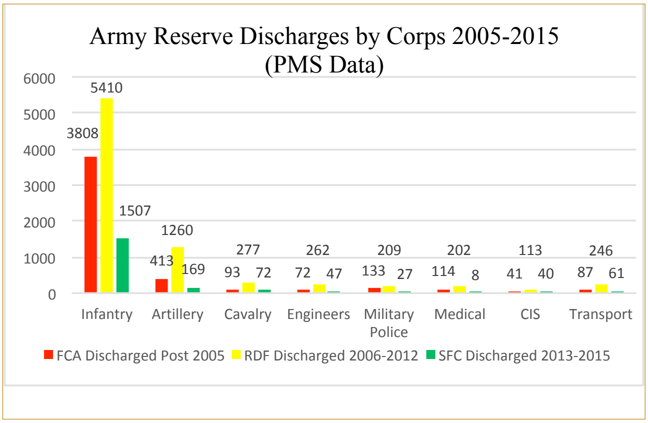
[15] *The Defence (Amendment) Act 1960*, *the Defence (Amendment) Act 1993* and *the Defence (Amendment) Act 2006* which legislate for the participation of Defence Forces personnel in UN peacekeeping missions, peace-enforcement missions and EU Battlegroups respectively all specifically state that such service is for members of the "Permanent Defence Forces," not reservists.

[16] Joel D. Rayburn and Frank K. Sobcjek, *The US Army in the Iraq War: Volume 1* (Carlisle: United States Army War College Press, 2019), p.260.

[17] Department of Defence, *White Paper on Defence 2015* (Dublin: Department of Defence, 2015),p.100; Department of Defence, Report of the steering group on the special study of the Reserve Defence Force (Dublin: Department of Defence, 1999), p.1.

[18] In 2009 a training syllabus was completed to allow reservists deploy to Kosovo with KFOR. The PDF was looking for doctors, engineers, medics, drivers, tradesmen and radio operators. The RDF Overseas Integration Course was to be a two-month upskilling course in CIS, CBRN, tactics, weapons handling, helicopter operations and unarmed combat. As mentioned the first issue with reservists deploying overseas is a legislative one and no amendments were made. Therefore, the plan was to enlist reservists into the PDF, thus legalising their deployment, for a one-year contract. Problematically, this contract amounted to obtaining the services of professional specialists for the lowest cost possible with no employment protection. Suitable reservists, who applied for overseas, regardless of their rank, were to be enlisted into the PDF at the rank of 2-Star Private and paid the equivalent wage. Unsurprisingly, there was a lack of volunteers with the desired professional qualifications and plans for reservists serving overseas were shelved in the financial crisis. Irish Defence Forces, *TS RDF INF XX/2009 RDF overseas integration course syllabus of training* (Dublin: Defence Forces Training and Education Directorate, 2009); Directorate of Reserve Forces, *Letter seeking expressions of interest for overseas service* (2 Sep. 2008); Reserve Defence Forces Representation Association, *Press release pertaining to the cancellation of overseas service for the RDF* (undated, 2009).

[19] Commandant D (PDF), interviewed by author, January 2016; Lt. Col. B (PDF), interviewed by author, January 2016.



The Problematic Force Structure

Another obstacle preventing efficient harnessing of specialist reservists' skills is the current force structure. The Infantry Corps of the Army Reserve is 74% of the total force with 2,804 personnel.[20] Adding in the Artillery and Cavalry Corps means 89% of the Reserve is combat oriented. The Medical, CIS and Engineering Corps', the decisive terrain for recruiting reservists with professional experience generated outside the Defence Forces, amounts to just 6% of the Reserve, or 198 personnel. On paper, this does not look too bad, but there are serious issues here. Firstly, there is geographic disposition. If a civilian engineer wants to join the Reserve they only have a choice between Athlone, or Cork. There is no reserve engineer unit in Dublin, despite a quarter of the population living there with a large pool of professionals who could be recruited. Similarly, for a medical professional, the choice is between two brigade headquarters' in Cork or Dublin. How far will a skilled professional be expected to travel with no remuneration to contribute their skills essentially free of charge?

The second force structure problem is organizational; reserve recruitment and training. Hypothetically, the average salaried professional in Ireland has four weeks leave a year. Factoring in a hypothetical family spending two of those four weeks on annual holidays leaves just two weeks a year for reserve full-time training (FTT). All reservists are trained as infantry soldiers, completing recruit and 2-star training courses with either infantry battalions or the artillery regiments. Both courses, required to become a 3-star private, take a combined four weeks FTT to complete. Usually, a reservist will complete one course a year. Some individuals can commit more time but on average it takes two years for most reservists to go from recruit to 3-star private. As these courses are mandatory for all reservists, it therefore takes two years before a qualified engineer, a cyber-security specialist, or an EMT can complete periods of FTT with their specialist unit. This depends on their sustained commitment for two years and luck as to whether they are eventually assigned to the specialist unit reflecting their skills. Only in the most recent 2019 recruitment competition could reserve applicants choose their preferred corps. From 2013 to 2018 applicants could only choose their preferred geographic location. Consequently, almost all those applicants were assigned to combat units, as these were the

[20] Irish Defence Forces, *Defence Force Regulation CS4: Numerical establishment of the Defence Forces* (Dublin: Department of Defence, 2013).

units managing their recruit training.[21] After two years infantry training, skilled specialists still can't do the job they, and the Defence Forces want them to do. Despite being qualified professionals, conversion courses must then be completed in relevant corps-specific areas. For some roles this makes sense, for others the system is inefficient. The Transport Corps provides a working example.

Reservists cannot carry out mechanical vehicle maintenance, despite a shortage of qualified mechanics in the PDF and many reservists being qualified civilian mechanics.[22] If a civilian articulated truck driver joins the Reserve no mechanism exists for a direct conversion to the equivalent military qualification.[23] The reservist must complete two years part time infantry training to reach 3 Star-Private just to be eligible for military standard driving courses. The equivalent military truck licence requires the further completion of three driving courses, taking another 18 months to complete if said reservist has had no problematic issues with their civilian employer. Consequently, for a professional truck driver to do the same job for the Defence Forces takes between three and four years, if the reservist can attend two weeks of FTT on a yearly basis. CIS Corps reservists cannot qualify as radio technicians despite there being a shortage in the PDF and there being a demonstrated talent pool of reservists who either already have the skills or could be trained.[24] If it takes three to four years for a truck driver on the outside to drive a truck on the inside, then what is the conversion timeframe for other professional skillsets? A tangible opportunity is being missed here. Some roles *could* be filled by direct-entry commissions, but every skilled reserve applicant cannot simply be made an officer.

For the various reasons set out above, a fundamental question must be posed. Is it efficient to maintain this force structure or organisational practice? Reserve combat elements are prudent, but with a shortage in the PDF of radio technicians, vehicle mechanics, doctors, air traffic controllers and cyber-security specialists to name but a few, a clear argument exists for change. Reducing the reserve personnel allocation to combat units in CS4 and increasing the allocations to specialist units would allow the Defence Forces a bigger net to catch skilled individuals willing to contribute their expertise. Supporting this argument is the Medical Corps. A 2009 review of medical capabilities found that the Medical Corps could only meet 40% of the needs of the Defence Forces, not including reserve requirements. The review recommended looking to the Reserve medical component to alleviate this. [25] At that time the Medical Corps had 226 reservists in three reserve medical companies.[26] The 2013 Single Force Concept reduced that Reserve medical component to just 32 personnel. The recommendations of the review were ignored, leaving the Defence Forces with just 32 spots, instead of 226, for medical specialists or doctors to fill. Personnel Management System (PMS) data clearly shows that specialist reserve units have higher personnel retention rates compared to the combat units, where the reserve

[21] Pesonnel Management System (PMS) Data for recruitment shows that from the inception of the Single Force Concept in 2013 to 2015 there were 461 new recruits to the Army Reserve, they were assigned as follows: The Engineering, Medical and CIS Corps'(one recruit each), the Transport Corp (two recruits), the Cavalry Corps (eleven), the Artillery Corps (seventy-eight) and the Infantry Corps (366 recruits). This is despite the Infantry, Cavalry and Artillery Corps' discharging 1,748 personnel in the same period.

[22] Commandant G (AR), interviewed by author, January 2016.

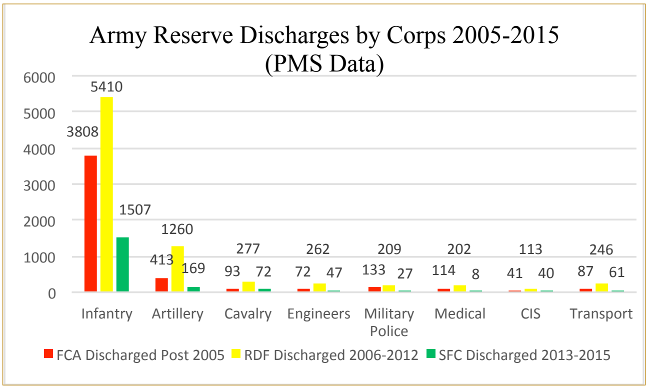
[23] Said individual would have to begin with a Module 2B (Nissan Jeep) course, then a Ford Transit minibus course followed by the Module 3B Truck course; Irish Defence Forces, *TI 03/2011 Defence Forces driver training policy* (Dublin: Defence Forces Training and Education Directorate 2011).

[24] Commandant A (PDF), interviewed by author, January 2016.

[25] PA Consulting Group, *Defence Forces Medical Services Review* (Dublin: PA Consulting Group, 2009), p. 40-46, 97; Commandant G (AR), interviewed by author, January 2016.

[26] The 62nd, 54th and 31st Reserve Logistics Support Battalions headquartered in Dublin, Galway and Cork each had a medical company within the battalion.

infantry component is unable to hold on to personnel.[27] This suggests that where reservists can bring, and apply, their civilian skills in the military, they stay longer than if they have nothing to bring to the table. There is no real civilian equivalent for infantry, artillery or cavalry. For military logisticians, medics, combat engineers and communications specialists, there is. This should be capitalized upon.



[28]

This brings up the cultural view of the Army Reserve by the Defence Forces, with varying attitudes among PDF unit commanders towards the Reserve. Some believe it unreasonable to expect personnel, with many external commitments, to work for free with no supporting legal framework.[29] The Medical Corps does not have the capacity to meet the needs of the Defence Forces, yet reserve medical officers cannot be utilised to alleviate this as they would be unwilling to perform a military function for free that they are paid for in a civilian capacity.[30] Others argue reservists don't "join for the money" and want to get away from their civilian jobs to do something different.[31] If the Defence Forces hope to recruit specialist skills, then expecting those skills for free is, at a minimum, optimistic. Furthermore, specialist units maintaining better strength levels argues that reservists join specifically to use their skills, not get away from them. Some argue that the Defence Forces does not buy into the potential of the Army Reserve and fails to assess the broad skill base reservists have.[32] This is hard to dispute. The suggestion of a comprehensive survey of reservists' skills and qualifications was made in 2003.[33] To date no comprehensive survey has ever taken place.[34] Consequently, the Defence Forces does not actually know who, what or how many skilled personnel the Army Reserve has

[27] PMS Data records that in the 2005-2015 period the reserve infantry component recruited 4,346 new recruits but discharged 10,725 personnel.

[28] PMS Data shows that in the wake of the 2005 reorganisation from the FCA to the Army Reserve, 4,761 FCA personnel were discharged over time from the Defence Forces. PMS Data does not explain why these personnel did not transition into the Army Reserve. Many local FCA posts were closed with the 2005 reorganisation due to the smaller organizational size of the new Army Reserve, this may explain some of the personnel not continuing their service. A further 7,979 personnel were discharged from the Army Reserve between 2006 and the 2013 reorganisation to the Single Force Concept. Post Single Force Concept to 2015 an additional 1,931 were discharged for a total of 14,671 discharges between 2005 and 2015 with an average of 1,467 personnel per year.

[29] Commandant F (PDF), interviewed by author, January 2016.

[30] Lt. Col. J (PDF), interviewed by author, January, 2016.

[31] Lt. Col. C (PDF), interviewed by author, January 2016.; Commandant E (PDF), interviewed by author, January, 2016.

[32] Commandant K (PDF), interviewed by author, March, 2016.

[33] Department of Defence, Department of Defence and Defence Forces strategy statement 2003-2005 (Dublin, Department of Defence, 2003), p.10.

[34] Mr. Neil Richardson, General Secretary RDFRA, interviewed by author, June 14, 2019.

to offer. Such data, quite easily obtained, should be the guiding principle behind designing the force structure of the Reserve.

International Best-Practice.

Other militaries have tackled this problem in every way that Ireland has not. Legislation in New Zealand, Canada, Australia, the United Kingdom and the United States guarantees a reservists' employment if deployed.[35] Failure to report for duty can result in periods of imprisonment.[36] Punitive impetus to report for service, coupled with legislative support, allows these nations to have a usable reserve skills base. There is also no "voluntary unpaid training" as all reserve service is incentivised, and in some cases pensionable.[37] The Irish Army Reserve, by comparison, has none of these enablers.

	Ireland	New Zealand	Australia	Canada	UK	United States[38]
Defence Acts	Yes	Yes	Yes	Yes	Yes	Yes
Legislative Enablers for Reserve Forces	No	Yes	Yes	Yes	Yes	Yes
Integration with Regular Forces	Yes	Yes	Yes	Yes	Yes	No
Employment Protection	No	Yes	Yes	Yes	Yes	Yes
Voluntary "Unpaid" Service	Yes	No	No	No	No	No
Deployment Overseas	No	Yes	Yes	Yes	Yes	Yes

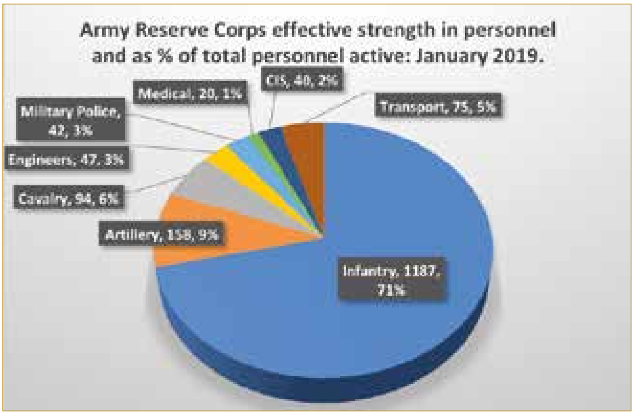
Furthermore, in terms of force structure, these other reserve forces are designed to harness significant amounts of specialist skillsets in areas such as medicine, military intelligence, cyber-security, engineering and logistics. This allows the regular armies to benefit from the professional experience gained by civilian employment in specialist areas, via their reserves. While the Canadian Army Reserve is primarily combat oriented, almost half of the Australian and New Zealand Army Reserves are combat service support units. This reflects an acknowledgement of what the regular army needs in terms of skills, thus allowing reserve forces to act as force-multipliers. Tipping the scale completely in favour of specialist skills, the American National Guard and Army Reserve combined have more medical, engineering, military intelligence, and logistics units than the regular US Army. For the British, most of their medical establishment is also in their Army Reserve, along with almost half of their intelligence and logistics units. In both the American and British forces, there are almost twice as many specialist units compared to combat formations of equal size. Legislatively, and organisationally, the Irish Army Reserve is out of step with international best practice. Ireland may be neutral, while these comparators are

[35] The relevant legislation is as follows, *The Defence Act 1990* (New Zealand), *The National Defence Act 1985* (Canada), *The Reserve Forces Act* (UK), *The Defence Reserve* (Protection) *Act 2001* (Australia) and the *Uniformed Services Employment and Reemployment Rights Act 1994* (United States, applying equally to the Army National Guard and the Army Reserve).
[36] All pieces of legislation noted above dictate custodial penalties relevant to that country's military or civil law.
[37] All training nights and weekends are fully paid, as are any travel expenses incurred due to reserve service. Furthermore, in the British model reservists are paid a bounty, similar to the Irish gratuity scrapped in 2012, for attaining set annual training obligations with the bounty increasing incrementally every year. There is also a pension contribution for reserve service. Ministry of Defence, *Rates of Pay 2015* (London: Ministry of Defence, 2015). Ministry of Defence, *Reserves in the Future Force 2020: Valuable and Valued* (London: Ministry of Defence, 2011), p.8.
[38] The United States Army reserve component is a combination of the Army National Guard, which focuses primarily on providing combat units in the form of Brigade Combat Teams with some Combat Support units, and the United States Army Reserve which primarily focuses on Combat Service Support.

not, but neutrality does not matter. Security environments merely dictate the size of military forces, and the priority and division of contingent capabilities within those forces. However, regardless of neutrality, all modern militaries strive to develop and retain contingent capabilities, the only difference is the matter of scale. The Defence Forces should be no different.

The Reality

Conceptually, the British *Future Reserves 2020* policy argues, “if Defence routinely asks more than reservists or employers can reasonably give, then it is unlikely that Defence will have the reservists needed to deliver an assured contribution to national security.”[39] Data suggests that the Irish Army Reserve has consistently asked more than reservists’ can give. Without legislative support, meaningful employer engagement, and an ever-increasing emphasis on unpaid service, 14,671 reservists were discharged between 2005 and 2015.[40] In 2013, when the Single Force Concept was launched the effective strength of the Army Reserve was 3,410 personnel. By the end of 2015, it was 2,434. In January 2019, it was just 1,620.[41] With an establishment of 3,869, the Army Reserve teeters at circa 30% strength or less.[42] Clearly, reservists have voted with their feet. In addition, any unit commander will admit the big difference between *effective* strength and reservists on parade. The reality is, the Reserve may stand at 20-25% strength. A record low numerically, proportionally and historically. It should be noted that, of the 1,620, 313 were recruits or 2-stars, with another 626 being aged 45 or older.[43] This is the result when relying solely on the goodwill of the individual.



[39] Ministry of Defence, *Reserves in the future force 2020* (London: Ministry of Defence, 2013), p.28.
[40] Irish Defence Forces, *PMS Reports on annual discharges 2005-2015*. PMS Data shows that in the wake of the 2005 reorganisation from the FCA to the Army Reserve, 4,761 FCA personnel were discharged over time from the Defence Forces. PMS Data does not explain why these personnel did not transition into the Army Reserve. Many local FCA posts were closed with the 2005 reorganisation due to the smaller organizational size of the new Army Reserve, this may explain some of the personnel not continuing their service. A further 7,979 personnel were discharged from the Army Reserve between 2006 and the 2013 reorganisation to the Single Force Concept. Post Single Force Concept to 2015 an additional 1,931 were discharged for a total of 14,671 discharges between 2005 and 2015 with an average of 1,467 personnel per year.
[41] Mr. Neil Richardson, General Secretary RDFRA, interviewed by author, June 14, 2019.
[42] Defence Forces Regulation R5, the regulation governing the Army Reserve, an “effective” reservist merely has to attend a minimum of 24 two-hour unpaid training nights, or 48 cumulative hours made up of training nights and training weekends annually. Personnel not achieving this are categorised as “non-effective” and ultimately discharged. Attending paid training to be classified as effective is not a requirement. Undoubtedly a reservist who has attended paid, full time training periods, in conjunction with the obligatory 48 hours is a higher trained soldier than one who has only met the 48-hour minimum requirement. Thus, the effective strength is indicative of the quantitative, not qualitative strength of the force.
[43] As of January 2019, the average age of a reserve Captain or Lieutenant was 50 and 44 years old respectively. In terms of non-commissioned officers, the average age of a Sergeant was 49, and a Corporal, 39. Mr. Neil Richardson, General Secretary RDFRA, interviewed by author, June 14, 2019.

Conclusion – It's now, or never.

Over the past 65 years the conduct of warfare, the global threat environment, the nature of military service itself has evolved. The Army Reserve, the legacy issues, legislative barriers and organizational problems have thus far remained unaddressed. Yet the expectation of what reservists can do, of harnessing the unique skills earned by their civilian professional experience and education remains juxtaposed with the reality that the current Army Reserve is not designed to supply skilled reservists to the Defence Forces, and in many ways is prevented from doing so. The 2013 reorganisation was a rebranding, nothing more, bringing nothing new and no meaningful change. After all, reservists have worn black berets and been integrated before.[44] Members of the Army Reserve are mainly unpaid, and when paid, are paid on the lowest increment on the scale according to rank, regardless of time in rank. They have no pension benefits, no allowances and the annual gratuity payment was withdrawn. They have little opportunity to utilise their military training or meaningfully bring their civilian skills to the table. The media is currently full of headlines about skilled personnel leaving the Permanent Defence Forces due to substandard remuneration. In such an environment how can skilled reservists be expected to continually contribute almost free of charge, when the data shows the continual decline of personnel in the organization? The innovation in the CIS Corps came *despite* the system, not because of it. It only occurred because the right reservists, with the right skills, were in the right unit at the right time, with flexible employers, and were willing to give their time and expertise freely. It was a result of the goodwill of the individual reservist, and luck. What might be possible if the structures and supports existed to institutionalise this? None of this, however, should be confused with capability development. There is no middle ground in modern militaries when it comes to capabilities. The Defence Forces either *has* a usable pool of skilled reservists when and where needed, or it does *not*. Currently it is the latter, for the reasons identified in this paper. If the force disintegrates, any future attempts to rebuild will be that much harder. With the Reserve at its lowest strength in history and significant data showing that the current model is unsustainable, meaningful change is now needed if the force is to survive, especially if the Defence Forces wants the valuable skills on offer. Of paramount importance, any change needs to be *informed* by what the Defence Forces *needs* and a realistic appraisal of what the Reserve can *provide*. Fundamentally, the system should facilitate the efficient absorption of reservists' skills into the Defence Forces, not prevent it. It is time to bring the Irish Army Reserve into line with other modern militaries, before the Reserve ceases to exist.

[44] The FCA numbered less than 25,000 when it was integrated with the PDF in 1959. Integration resulted in FCA units having regular army commanders and training staff attached to each unit to provide the Irish Army with six integrated brigades of regular and reserve personnel. After separation from the PDF in 1979, the FCA had a revised organisational establishment of 22,110 personnel. John P. Duggan, *A history of the Irish Army* (Dublin: Gill & MacMillan, 1991), p.238.

REMOTELY PILOTED AIRCRAFT SYSTEMS:

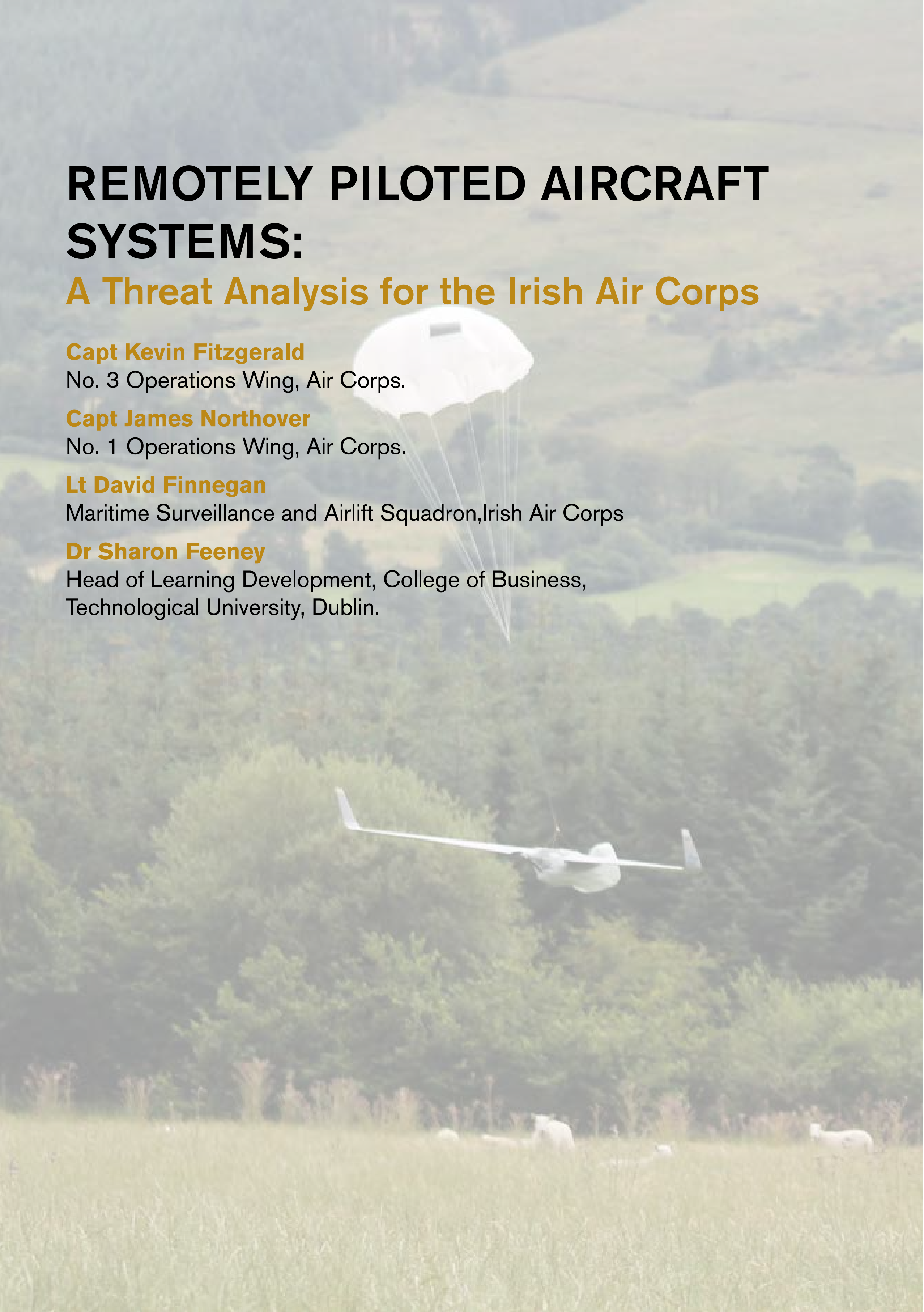
A Threat Analysis for the Irish Air Corps

Capt Kevin Fitzgerald
No. 3 Operations Wing, Air Corps.

Capt James Northover
No. 1 Operations Wing, Air Corps.

Lt David Finnegan
Maritime Surveillance and Airlift Squadron,Irish Air Corps

Dr Sharon Feeney
Head of Learning Development, College of Business,
Technological University, Dublin.



Abstract

Remotely Piloted Aircraft Systems (RPAS) are the next generation of field aviation. They have emerged in recent years and are proving to be more accessible, and more flexible than traditional crewed aircraft.

The industry is in its infancy, and it is clear that the required controls have not kept pace with the rapid expansion of the market. Legislation has only emerged in the past couple of years. Many national aviation authorities around the world are still without strict rules to control their use. The methods of preventing, protecting and intervening in the misuse of RPAS are equally primitive. These elements combine to create an environment where the next generation of aviation is posing a real threat to the current generation.

This study is the first of its kind to be conducted in Ireland. It provides a brief overview of literature, along with findings from a questionnaire that was distributed to all pilots, aircrew and air traffic controllers in the Irish Air Corps (IAC), which provided insights into the extent to which RPAS poses a threat to the current and future flight operations of the IAC.

The results of this study show that the international, national and IAC regulations governing RPAS are insufficient. Flight statistics have shown a rapid acceleration in the number of incidents involving RPAS.

Introduction

The issue of civilians using drones near civilian and military aircraft is an emergent issue for pilots. This paper will examine the threat that these drones [also known as Remotely Piloted Aircraft Systems (RPAS)] pose to aviation. The RPAS referred to in this study are operated by civilians and are primarily comprised of a small electric motor powering a number of rotors, and are piloted using handheld remote control devices or mobile phones. They are generally small in size and are used for short distance operations, for example for aerial photography, filming, conservation, and other missions. At present RPAS operate exclusively in airspace that is segregated out for them. The operators of RPAS tend not to be professional aviators or even aviation enthusiasts. This paper is the first to assess the levels of education and awareness of RPAS among flight crews in the Irish Air Corps.

Context

Legislation has struggled to keep pace with the rapid expansion of emerging technology and in the case of RPAS technology, regulation has been slow to appear. The majority of academic research in this area has been carried out in the US although it is argued that[1], the Federal Aviation Authority (FAA) are "seriously behind" in the race to implement useful legislation. Sanz *et al.* [2] take the view that the legislation required can only be reactive, and cannot have the capability of controlling operators in the same way as manned aviation. They suggest that the burden of regulation needs to fall on the manufacturers as it is a futile exercise to attempt to

[1] Perritt, H. H. and Sprague, E.O. (2014). RPAS. *Vanderbilt Journal of Entertainment and Technology Law*, 17 (3), 672 – 749.

[2] Sanz, D., Valente, J., del Cerro, J., Colorado, J., & Barrientos, A. (2015). Safe operation of mini UAVs: a review of regulation and best practices. *Advanced Robotics*, 29(19), 1221-1233

maintain absolute control over the skills of individual operators. It is inevitable that there will be malicious or incompetent people who will misuse drones, which may ultimately threaten aviation safety. This potential is exacerbated greatly by the fact that the operators of drones are not exclusively aviation enthusiasts or hobbyists, and are far more likely to be casually uninformed or uninterested in flight safety. So the balance must be restored by focusing on the regulation of the aircraft. The authorities cannot be sure whether an operator will transgress, and therefore every effort must be made to ensure that the drone itself cannot transgress[3]. RPAS use has not yet been studied in an Irish context so a series of questions are considered in this paper in order to provide some insight into the Irish experience to date.

Methodology

This study seeks to ascertain the extent to which RPAS use is a threat to IAC flight operations. Consequently there are three main research questions identified:

1. To what extent are RPAS a threat to flight safety in IAC?
2. To what extent is national and international legislation sufficient to protect IAC flight operations in the area of RPAS?
3. Are IAC personnel sufficiently educated on the capabilities and threat potential of RPAS with respect to flight safety?

Given that the interaction between piloted and remote aviation affects all aircrew involved in the safe execution of flight operations, it was decided to administer a questionnaire to all pilots, helicopter crew and air traffic controllers employed in the Irish Air Corps. The decision to include pilots is obvious given the high likelihood that they would encounter RPAS in their flying careers. Helicopter crew were chosen given the nature of their role in helicopter flight operations: they are responsible for keeping the helicopter free from all obstacles and other traffic when the helicopter is being operated in confined spaces away from the controls and protection of airports. Air Traffic Controllers are also responsible for the separation of all air traffic and provide an advisory role to aircraft of anything that has the potential to impact the flights safe execution. The questionnaire response rate is provided in Table 1 below.

Specialisation	Distributed	Responses	% of Respondents
Pilot - Fixed Wing	35	31	89%
Pilot - Rotary Wing	24	20	83%
Aircrew	26	24	92%
Air Traffic Controller	14	11	79%
Total	**99**	**86**	**87%**

Table 1 – Response Rates to Questionnaire

[3] Ibid., 1221-1233.

Findings

The findings of the study are presented below with each research question is taken in turn.

To what extent are RPAS a threat to flight safety in IAC?

Findings from the survey suggest that RPAS poses a significant threat to flight safety in IAC. Question number 12 in the Survey asked "In your opinion do RPAS pose a credible flight safety threat to IAC flight operations?" 95% of those surveyed agreed that RPAS pose a threat to flight safety in the IAC (see figure 1 below). The survey participants have a direct exposure to airborne threats in the course of flight operations, and therefore have a personal stake in the outcome of this study. Furthermore, the participants in the survey are privy to aircraft flight safety reports, and conduct annual courses that encourage the development of an organisational culture that promotes flight safety. This may engender a more cautious and conscientious attitude to the threat of RPAS to Irish Air Corps Flight operations.

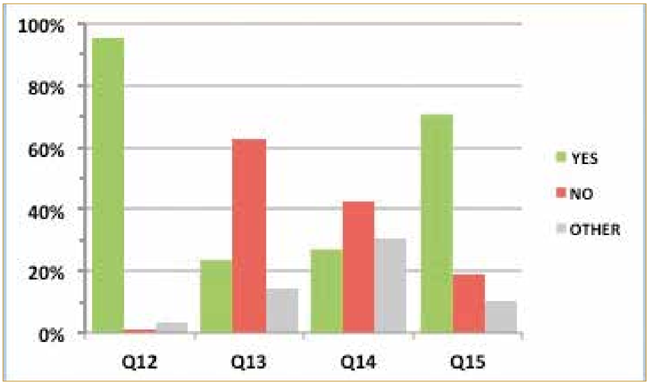


Figure 1: Responses on the perceived threats to flight safety

The research also looked the perceived ability of Air Traffic Control (ATC) to mitigate against the threat that RPAS poses. Question number 13 asked, *"Do you regard our ATC service as being in a position to mitigate against the threat that RPAS may pose to flight operations?"* It is interesting to note that only 24% of personnel participating in the survey believed that ATC was in a position to protect flight operations from the RPAS threat. Question 14 *"Do you think the IAC have adequately mitigated the risk RPAS may pose to flight operations?"* shows that over 40% of respondents do not believe that IAC have adequately mitigated against the risk RPAS might pose to flight operations. Question 15, *"Considering the recent rise in nuisance laser attacks on IAC aircraft, do you foresee RPAS being utilised in a similar way to hinder or endanger flights?"* shows that RPAS is perceived to be a growing threat to flight safety, with over 70% agreeing that RPAS is foreseen as having the possibility to be utilised to hinder or endanger flights.

To what extent is the national and international legislation sufficient to protect IAC flight operations?

At the time of completing the survey, new rules and regulations were being finalised by the Irish Aviation Authority. These were well publicised in the national media and will likely have influenced the responses to question numbers 16, 17 and 18. Question 16 asked, *"Do you agree that An Garda Siochána are fully aware of the industry of RPAS in this country?"* More than half of the respondents answered 'no' to this question, with less than 20% reporting that they believe that An Garda Siochána are fully aware of RPAS (see Figure 2 below). This is significant in the context of upholding some of the regulations for users, and the likelihood of members of An Garda Siochána to initiate prosecution for non-compliance and endangering citizens. Similarly, question 17 asked, *"Do you agree that An Garda Siochána are adequately prepared to protect the airspace from RPAS operators on the ground?"* Again, the majority of respondents (80%) answered 'no' to this question. This is interesting in the context of the Garda Air Support Unit (GASU), which is a helicopter unit comprising members of An Garda Siochána and piloted by IAC personnel that operates from the IAC Baldonnel base. All helicopter operations are carried out at a low level and in urban environments where RPAS usage would be higher. Only 6% of respondents agreed that An Garda Siochána are adequately prepared to protect the airspace (see Figure 2 below)

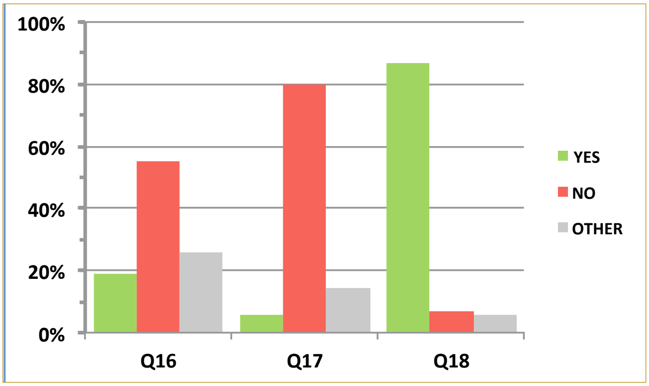


Figure 2: Responses on awareness and assessment of legislation

Question 18 asked, *"do you believe, from a base security perspective, a specific set of orders should be drafted in order to protect IAC aircraft from the potential threat of RPAS overflying the airfield boundaries?"* This is a salient sample, given that the personnel responding to the survey have a direct responsibility for the security of the base, in the normal course of their duties. The sample are, therefore, fully aware of the challenge of maintaining adequate security at all times. It is interesting therefore, that 87% respondents agreed that a specific set of orders need to be created in order to address the emerging threat of RPAS being used for malicious purposes or in an illegal manner, and in such a way as to contrive the safety of IAC. See Figure 2, above. This finding has implications for other Defence Forces establishments throughout Ireland, as each premises must maintain adequate security at all times.

Are IAC personnel sufficiently educated on the capabilities and threat potential of RPAS with respect to flight safety?

The topic of education provided the most definitive findings in this study, with very little division of response. Question 19 in the survey asked, "*In your opinion is there sufficient education currently being provided to personnel in your current role in relation to RPAS?*" A particular focus of this study was to examine whether personnel believed the information currently being supplied on RPAS and the growth of the industry in Ireland was at the appropriate level required. The overwhelming majority felt that the current level of RPAS education being supplied to personnel was inadequate, with only 13% of respondents indicating that it was sufficient and some 80% of respondents answering 'no' to this question (see Figure 3, below).

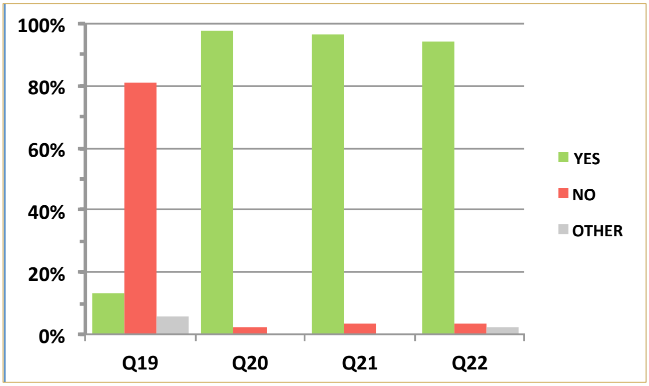


Figure 3: Responses on education on RPAS within the IAC

With regard to the suggestion that more formulaic RPAS training be instituted in the IAC, the results were very clear. In answer to Question 20, which asked, *"The IAA has proposed that An Garda Siochána deliver a module on RPAS to new entrants training in Templemore. Do you think that the IAC would benefit from incorporating such a module into Pilot, ATC, and Aircrew initial courses?"* A resounding 98% of respondents agreed that RPAS education should be incorporated into the initial training of the pilot; aircrew and ATC courses (see Figure 3 above). Questions 20 and 21 dealt with issues relating to the knowledge management system in the IAC, known as 'IKON'. Question 20 asked *"Do you agree that the Irish Air Corps would benefit from having a designated RPAS IKON portal incorporating education, legislation and flight safety lessons learned?"* and Question 21 asked, "Would you interact with such a portal if it was to be introduced?" Interestingly, over 90% of respondents agreed with both questions 20 and 21, which suggests there is an appetite to record legislation updates and flight safety lessons learned in relation to RPAS activities (see Figure 3 above). This finding has implications for other Defence Forces components and for their premises throughout the country, and it raises an important matter that could warrant further research.

Eight questions in the Survey were dedicated to ascertaining the level of awareness of RPAS in the IAC, these are summarised in Figure 4, below. Question 4 in the Survey asked *"Have you ever witnessed an RPAS operating in your airspace during the course of your career?"* and, question 5 asked *"Have you ever heard a colleague discuss an encounter with an RPAS operating in their airspace?"*. The responses were consistent in that 34% of respondents reported having witnessed an RPAS operating in their airspace during the course of their career (see Figure 4 below). Many of these were helicopter pilots who operate at a lower flight level. Of the total group of respondents, 66% had heard a colleague discuss an encounter with an RPAS. Interestingly when the results include just helicopter pilots, the number that had heard a colleague discuss an encounter with an RPAS rose to 100%.

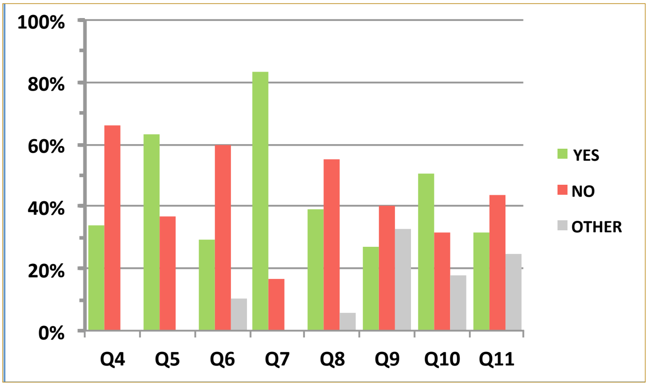


Figure 4: Response on awareness of RPAS within the IAC

In relation to respondents reporting their familiarity with the RPAS industry and the emergent regulatory requirement for RPAS in Ireland, the survey contained six questions. Question 6 asked *"Do you consider yourself well informed on the RPAS industry in Ireland?"* while question 7 asked *"Are you aware that the IAA introduced new regulation in December 2016 in response to the rapid growth in RPAS operators in Ireland?"* Question 8 asked, *"Do you consider yourself well informed on the IAA regulation that governs the use of RPAS in Irish airspace?"* Question 9 asked, *"Do you think that the IAA regulation adequately controls the use of RPAS in this country"*

Of the total group taking the survey, only 29% of the group considered themselves well informed on the current industry in Ireland. Yet despite the fact that a greater proportion of helicopter pilots experience RPAS in flight, 36% profess themselves well informed. Some 80% of respondents reported that they were aware of the regulation introduced by the IAA in December 2016 in response to the rapid growth in RPAS operators in Ireland, however, just over 40% of respondents consider themselves to be well informed on the IAA regulation that governs the use of RPAS in Irish Airspace, with just over 50% reporting a no answer to this question (see Figure 4 above). Fewer than 30% of respondents reported that they think the IAA regulation adequately controls the use of RPAS in this country, with 40% reporting a no response, while just over 30% reported 'other' in their response (see Figure 4 above).

Question 10 asked, *"Do you agree that the IAC are properly aware of the RPAS industry?"* and question 11 asked *"Do you regard the IAC as being adequately prepared to deal with the RPAS industry?"* Some 50% of respondents reported that they agree that the IAC are properly aware of the RPAS industry, with just under 40% reporting a no answer to this question. Finally, just over 30% of respondents report that they regard the IAC as being adequately prepared to deal with the RPAS industry, with less than 50% reporting a no response to this question (see Figure 4 above).

Conclusion

It is clear from the study that concerns surrounding RPAS operations is increasing in the IAC. The data analysed in this study suggests that most Air Corps personnel are concerned about the effects that RPAS operations can have on Air Corps flight operations. The overwhelming concern from operators in the IAC is that RPAS pose a threat to flight safety. The questionnaires directly highlight the high level of concern that IAC personnel had with regard to RPAS. The findings from this research suggest that the threat to flight safety from RPAS is reaching a critical level. This threat is also relevant for civilian flight safety, although that is not the focus of this particular study. Indeed, some incidents at civilian airports (e.g. Gatwick Airport, UK in December 2018) have demonstrated the serious economic and social consequences that an RPAS incident can have due to flight safety concerns. It is apparent that measures are needed to combat a quickly evolving and uncontrolled RPAS market. It is recommended that in order to mitigate the threat to IAC flight safety a coordinated effort must occur between the IAA, IAC and An Garda Siochána. Training modules need to be delivered to officers in the IAA, IAC and An Garda Siochána, with inputs from all three bodies (the IAA, IAC and An Garda Siochána personnel) to ensure that emerging regulation and legislation are fully enforced.

To what extent is the national and international legislation sufficient to protect IAC flight operations?
The issue of national and international legislation and regulation being sufficient to protect IAC flight operations is a critical one. The majority of research in this area to date has been focused on the legislative framework of the FAA. This paper represents the first attempt to document the usability and efficacy of the Irish regulation. It should be noted that the IAA were among the first regulators in the world to establish a framework of regulation around the use of RPAS. However, the need to regulate the manufacture of RPAS is of primary importance, if suggestions from the European Aviation Safety Agency (EASA) with regard to geo-fencing or electronic identification are to be realised.

The conclusion from the survey was that IAC personnel are well informed about the recent legislation and regulation regarding RPAS. However, the overwhelming opinion unveiled by this paper is the belief that current legislation is not sufficient to protect IAC flight operations. This may also have repercussions for civilian flight operations also. Stricter regulations need to be implemented. In the interest of traceability it is imperative that every RPAS needs to be registered with the IAA. This would greatly deter unauthorised usage, while also contributing to effective policing in the event that that rules are breached. These findings have relevance to other Defence Forces activities and premises, as well as to other State organisations, including the IAA and An Garda Siochána. Further research into these issues might be timely and important, particularly in the context of flight safety, airport operations and flight operations.

PUSHING THE DEFENCE TECHNOLOGY FRONTIER: A Role for the EU?

Dr. Daniel Fiott
Security and Defence Editor, EU Institute for Security Studies

Abstract

With the introduction of Permanent Structured Cooperation and the European Defence Fund, much of the attention has been placed on how these initiatives can assist the EU member states fill capability gaps and enhance defence cooperation. However, these new initiatives also symbolise an important development in relation to the way the EU thinks about and invests in defence technologies. This paper explores the ways in which the EU can manage its present and future technological and capability needs.

Introduction – a radical shift for the EU on defence?

With the introduction of the European Defence Fund (EDF) and Permanent Structured Cooperation (PESCO), the European Union (EU) has taken a step forward in security and defence cooperation. PESCO binds 25 EU member states into closer defence cooperation over the longer-term, ensuring that the Union acts in a more structured way when it comes to developing defence capabilities, investing in defence and being more credible with regard to operational deployments. PESCO is also currently home to 34 defence capability projects that are aimed at enhancing the strategic autonomy of the Union and ensuring that the EU fills strategic gaps. Although more projects will be agreed by the end of 2019 and then in 2021, the current set of 34 projects include cyber rapid response teams, a high atmosphere airship platforms, medical command, the Eurodrone, integrated unmanned ground systems and more. Ireland participates in projects such as the training centre for EU mission deployments[1] and maritime surveillance.[2]

The EDF, which sees the European Commission become a much more important actor in EU defence, is earmarked to have €13 billion from 2021-2027 under the next multi-annual financial framework (MFF) for the purposes of defence research and defence capability investments. For defence research, the European Commission has a requested €4.1 billion over 7 years and €8.9 billion for defence capability development over the same period.[3] Whereas the €4.1 billion for defence research will cover up to 100% of the eligible costs of a project, the €8.9 billion will cover a base line of 20% for programmes. This means that EU member states will have to make up the remaining 80%, implying that the EDF could leverage more defence investment (i.e. €1 billion worth of EDF investment in capabilities could unlock a further €5 billion in government contributions – meaning €35 billion over 7 years).[4]

The Commission has also made clear that it will dedicate about 5% (€700 million) of the overall €13 billion to disruptive technologies. This investment is geared to unlocking the EU's potential when it comes to emerging technologies such as artificial intelligence, robotics, nanotechnologies, etc. Such technologies are vital not only to support the competitiveness of the European defence market, but also to ensuring that the Union has the defence technologies required to continue to be a defence actor. The EU has already began to invest in defence innovation. A pilot project has already seen €1.4 million dedicated to a study on the feasibility of unmanned swarm systems ("EuroSWARM") and the possibility of combining

[1] With Germany, Czech Republic, Spain, Italy, France, Luxembourg, Netherlands, Portugal, Austria, Romania and Sweden.

[2] With Greece, Bulgaria, Spain, Croatia, Italy and Cyprus.

[3] European Commission, "EU Budget for the Future: The European Defence Fund", June 13, 2018, https://ec.europa.eu/commission/sites/beta-political/files/budget-may2018-eu-defence-fund_en_0.pdf.

[4] European Commission, "European Defence Action Plan: Towards a European Defence Fund", Press release, November 20, 2016, http://europa.eu/rapid/press-release_IP-16-4088_en.htm.

unmanned systems, sensors and data for urban combat ("SPIDER"). Furthermore, under the EU's preparatory investments on defence research the Union has invested up to €90 million in technologies such as maritime surveillance, adaptive camouflage, soldier communication systems and advanced body armour.

Although these figures may seem relatively small when compared to say the defence budget of the United States (US) or even some of the larger EU member states, this is a radical step forward for the Union in the area of defence. Nevertheless, the EU's venture into defence research and capability development raises a set of questions. First, what capabilities and technologies should be prioritised by the EU given the fixed envelope of €13 billion under the EDF? Second, in what measure should the EU balance investments in existing capability shortfalls compared to emerging technology domains? Third, why does the EU need to invest in defence capabilities in the first place and for what purpose?

Balancing capability shortfalls and emerging technology

One of the biggest challenges facing the EU in terms of defence capabilities is how to balance the need to plug long-standing shortfalls in the areas of intelligence, surveillance and reconnaissance, communications and strategic airlift with future technology needs. Clearly, there is no simple scientific formula for what proportion of investment should go on capability shortfalls and on emerging technologies. Each EU member state government will have to decide how it balances capability development and defence innovation, but there is an EU (and even NATO) dimension to these national discussions. In fact, at the EU level the 2018 Capability Development Plan (CDP) revision is a consolidated plan to manage this balancing act and this means that national decisions are not made in complete isolation from broader EU-wide plans.

In what measure a member state decides to invest in capability shortfalls rather than emerging technologies depends on national circumstances. A country may have the capital required to both procure identified shortfalls and invest substantial amounts of money into defence innovation. Other countries lacking in a defence industrial base may prioritise purchases of systems and equipment that they lack. Other countries may want to promote niche technology markets despite lacking prime defence firms that assemble high-tech weapon systems. Either way, whatever decision is taken will affect the European defence market. For example, a decision to simply fill capability gaps by buying off the shelf equipment from a third-country outside of the Union may be a quick (although not necessarily cheaper) fix, but at what cost to European industry?

Furthermore, the dichotomy that usually characterises the discussion between capability shortfalls and future technologies misses the fact that many capability shortfalls require continuous technological improvement to stay relevant in defence. In this regard, it is necessary to think of capability shortfalls and technological frontiers in the same breath. Research shows that existing capabilities profit from technological innovations that usually emanate from the civil sector.[5] So when we think about how the EU might push the defence technological frontier, it is a question about harnessing new technologies but in a way that keeps costs for

[5] Renaud Bellais and Daniel Fiott, "The European Defense Market: Disruptive Innovation and Market Destablization", *Economics of Peace and Security Journal*, vol. 12, no. 1 (2017), pp. 37-45.

weapons in check and allows Europe armed forces to profit from high quality systems and equipment.

This is why it is promising to see how the European Commission has crafted its first work programme calls on the preparatory programme for defence capabilities (i.e. the European Defence Industrial Development Programme (EDIDP)). Indeed, in 2019 the Commission published a call for proposals for 9 key capability areas including: the protection and mobility of military forces in areas such as counter CBRN and drones (a package worth €80 million); intelligence, secured communication and cyber for enhanced situational awareness, early warning and maritime surveillance (€182 million); conduct of high-end operations through ground-based precision strike and future ground, air and naval systems (€71 million); innovative defence technologies such as artificial intelligence, virtual reality and cyber technologies (€27 million) and a package for two PESCO projects on the Eurodrone and support for interoperable and secure military communications (€137 million).[6]

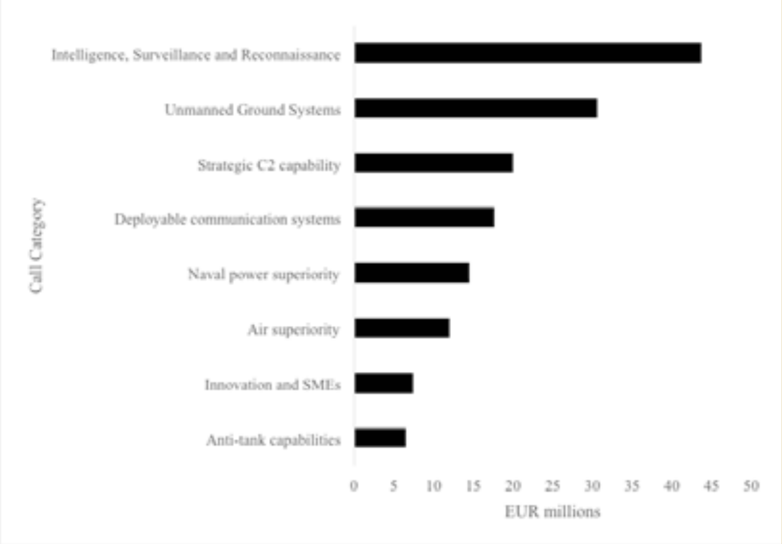


Figure 1 – The 2019 Call for Proposals under the EDIDP

(Source: European Commission, 2019)

Such investments prove that the Commission is thinking about future technology needs whilst also factoring in capability gaps in the EU's defence armoury. Such steps also recognise that if the EU gets left behind on the defence technology curve, this will come with significant political and military costs. First, there are already political and technological gaps opening up in NATO between the US and Europe NATO allies. Without European capabilities, the alliance is likely to be lopsided and the long-term invest of the US in NATO could be questioned. Second, the strategic landscape is shifting to such a degree that even basic Common Security and Defence Policy (CSDP) missions and operations will in the future be deployed in less permissive

[6] European Commission, "European Defence Fund on track with €525 million for Eurodrone and other joint research and industrial projects", March 19, 2019, https://ec.europa.eu/growth/content/european-defence-fund-track-€525-million-eurodrone-and-other-joint-research-and-industrial_en.

environments characterised by the existence of third powers (i.e. China and/or Russia in the neighbourhood) and technological innovations (e.g. weaponised dual-use technologies such as civil drones and cyber defence). Technology is one way for the EU to offset waning asymmetry in parts of the world if thought were permissive for European forces.

The EU as a defence actor in a shifting strategic context

Of course, conversations about what types of defence technologies and capabilities the Union should invest in are strongly related to ideas about what type of defence actor the EU is (or might become). When one looks at the changing nature of warfare, it is clear that new technologies and approaches such as cyber, automation, miniaturisation and durability are forcing European armed forces to think about how "disruptive technologies" could affect the way they plan for and fight wars. The current defence-technological context includes developments such as directed energy weapons, hypersonic missiles, automated robotics, artificial intelligence, etc. The question for the EU is, how far should it invest in such technologies or the narratives accompanying them?

On the face of it, the EU is potentially limited in terms of the defence actor it can become because of the EU treaties, which calls on the Union to prepare for crisis management operations and missions outside of the borders of the EU. Since the introduction of the EU Global Strategy (EUGS), the EU's principal task of crisis management has been joined by two further responsibilities including capacity building for partners and protecting Europe.[7] Capacity building for partners is not such a controversial tasking, as the EU has a history of supporting partners with security sector reform and training through military and civilian CSDP. What is interesting, however, is the focus on 'protecting Europe' and the way the EU could help with policies such as border management and hybrid threats by potentially engaging CSDP tools, mechanisms and structures.

The lines between internal and external security and defence are becoming blurred, and this means that the CSDP is having to evolve in line with the wishes of EU member states. This is important to keep in mind because CSDP is evolving from purely a crisis management tool into something potentially much broader in scope. While CSDP has been largely geared to planning for the 'Petersberg Tasks'[8] which included peacekeeping, disarmament, separation of forces, humanitarian tasks, etc., today the EU must also plan for potential continental security contingencies under Article 42.7 TEU[9] and Article 222 TFEU[10]. This, of course, does not mean that the EU has suddenly entered the nuclear or conventional deterrence game, but it does mean that it may need to plan for defence tasks that might occur on the territory of the EU and for which NATO might not have a mandate (i.e. for non-NATO EU member states). This evolution in the way we think about CSDP or EU security and defence more broadly relates directly to the defence capabilities and research the EU could invest in. To put

[7] "Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy", June 2016, http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf.

[8] See this glossary of terms for the full list of tasks: https://eur-lex.europa.eu/summary/glossary/petersberg_tasks.html.

[9] This is otherwise known as the 'mutual assistance clause' and it states: 'If a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power...'

[10] This is otherwise known as the 'solidarity clause' and it states: 'The Union and its Member States shall act jointly in a spirit of solidarity if a Member States is the object of a terrorist attack or the victim of a natural or man-made disaster. The Union shall mobilise all the instruments at its disposal, including the military resources made available by the Member States…'.

it bluntly, if the EU needs to protect sea lines of communication as stated in the EUGS does this mean that the EU should invest in a carrier group? Or, in order to prevent Russia from invading a non-NATO EU member state should the EU invest in a new generation of tanks? What about the Council Conclusions of 14 November 2016[11] on the need to plan for close air support; should the EU invest in stealth fighter jets? The reality is, of course, that the Union may have to invest in all of these areas and more if it is to credibly fulfil its role as a strategically autonomous defence actor.

The problem is that debates over what capabilities should be prioritised in an EU setting are political – not only because EU governments want to use PESCO and the EDF to fund projects of national interest, but because industrial interests ensure that the debate is not just about defence capabilities but also about *juste retour*, technology partnerships, skills, jobs and more. This is even more reason why the EU needs to get capability prioritisation right. This begins with calibrating correctly initiatives such as PESCO, EDF, the Coordinated Annual Review on Defence (CARD) and the CDP but also by having a frank discussion at the EU level about what precisely it is the EU should strive to achieve in the defence domain.

Such a conversation is needed now more than ever. Discussions in Brussels about EU 'strategic autonomy' in security and defence are sensitive and are usually seen as either duplicating or detracting away from NATO.[12] Of course, EU defence initiatives have been set up in such a way as to reinforce the European pillar in the alliance. Yet, it is necessary that governments in the EU develop a better sense of strategic autonomy. The US has made it plain, for example, that it will dedicate its political and military energies to China and this means that Europeans will have to do more for their own defence. Politically, the EU needs defence capabilities as a way to leverage its political independence. Let us picture future scenarios where war breaks out between the US and China or the US and Iran. In both cases, sea communication channels in the Indo-Pacific and Strait of Hormuz could be blocked. Would the EU join the US in such conflicts? Probably not, so who will protect Europe's strategic interests in such cases?

Conclusion

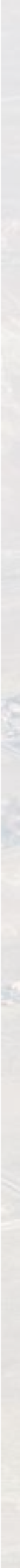
In terms of defence, it is clear that the EU is not yet in a position to compare itself with larger players such as the US or China. It does not appear to be the Union's intention to "compete" in the traditional strategic sense. Nevertheless, it is still necessary for the EU to protect the interests of its citizens and its territory. Whether it be peacekeeping, crisis management, border management or protecting the global commons, the Union clearly has to strive for a certain level of strategic autonomy. The US has repeatedly called for this, but the EU does not need Washington to remind it of its responsibilities in the area of security and defence. An increasingly shifting global context means that the Union must fend for itself and one way of achieving this is to ensure that Europe's armed forces have the equipment they need now and in the future, plus making sure that the competitiveness of the European defence industry is safeguarded. In short, without a defence industry and capabilities the EU will struggle to secure its objectives in a global order that is being contested by partners and new and old powers alike.

[11] Council of the EU, "Council Conclusions on Implementing the EU Global Strategy in the Area of Security and Defence", 14149/16, Brussels, November 14, 2016, https://www.consilium.europa.eu/media/22459/eugs-conclusions-st14149en16.pdf.

[12] Daniel Fiott, "Strategic Autonomy: Towards 'European Sovereignty' in Defence?", *EUISS Brief,* No. 12, November 2018, https://www.iss.europa.eu/content/strategic-autonomy-towards-'european-sovereignty'-defence.

Fortunately, EU member state governments have recognised this fact and this is why they have committed to PESCO and the EDF. History will eventually tell us how far the Union was able to push the technological frontier and its own defence, but it is clear that for the time being there is not a minute to lose in developing defence capabilities. This means that the Union's institutions must continue to play a key role in overcoming national jealousies and mediating between national capability and industrial preferences. If the EU is really going to push the frontiers of defence technology for the benefit of its own security and defence, then difficult choices will have to be made over what type of defence actor the EU needs to become and the capabilities it needs to this end. Not seeing through the dramatic shifts in EU security and defence will be too costly for the Union in the current and future global strategic landscape.

**The views contained in this paper do not necessarily reflect the views of the European Union.*



BEWARE THE BOOMERANG EFFECTS:

Western Risk Society and the Strategic Backlashes of Military–Technological Modernisation

Eoin McNamara
University of Tartu, Estonia.

Abstract

The transatlantic security partnership formed between the EU and the US has long sought to maintain a stable international order. Changing levels of social acceptance towards the use of military force combined with increased discord in transatlantic diplomacy over recent years has led to fears that the Western commitment required to maintain the military security burden that international stabilisation requires is swiftly deteriorating. This article argues that Western governments are today confronted by a challenging domestic-strategic contradiction. On one hand, most Western societies continue to perceive it as crucial that the contemporary international order remains stable. Conversely, these societies have become more risk-averse than ever before. This has reinforced a popular reluctance towards the deployment of ground forces often required for security management tasks. Centred on the US military-industrial complex, social change has been an important catalyst to propel Western governments to invest substantially in risk-efficient military technologies. This has arguably been the primary means employed to ease this domestic-strategic predicament. Military drone technology has revolutionised US counterterrorism policy over the past decade. While fostering many obvious strategic benefits, this article will argue that the utilisation of this military technology also harbours several severe strategic side effects.

Introduction – social change and dangerous modernisation

This article's analysis perceives Western social change through the concept of risk society first introduced by Ulrich Beck during the 1980s.[1] The risk society outlook provides a broad macro-level conceptualisation for the main patterns that define contemporary social change. The concept can be divided into two interrelated strands. The first strand emphasises globalisation; increased "individualisation" in society; the accelerated disappearance of self/other divides; and a "presence of the future" consciousness as defining conditions in contemporary Western society.[2] These background trends combine with the more specific conditions of the second strand relating to society's increasingly reflexive character and include a social obsession with the "management" of risk and the inevitable "boomerang effects" that manifest as side-effects from technological modernisation in particular.[3] When Western approaches to war have previously been perceived through the risk society concept, the most important headline argument has been that policy for recent Western-led military operations: encompassing those in Kosovo; Afghanistan; and Iraq have been rationalised through the logic of risk management in one form or another.[4]

Anthony Giddens has argued that the complete arrival of the Western risk society has meant both "the end of nature" and "the end of tradition".[5] Bound-up in the sometimes, negative unintended side effects of modernisation, "the end of nature" is conceptualised as today's inextricable intertwinement between the natural world and its social equivalent. Global climate change has developed as an unexpected side effect of past and current industrial modernisation. Nuclear energy is regularly explained as a seminal manifestation of risk technology. As a solution

[1] Ulrich Beck, *Risikogesellschaft: Auf dem Weg in eine andere Moderne* (Franfurt am Main: Suhrkamp Verlag, 1986).
[2] Ulrich Beck, *Risk society: Towards a new modernity* (London: Sage, 1992).
[3] Beck, Op. Cit.
[4] Yee-Kuang Heng, *War as risk management: Strategy and conflict in an age of globalised risks* (Abingdon: Routledge, 2006).
[5] Anthony Giddens, "*Risk and responsibility,*" The Modern Law Review, 62, no.1 (1999): 3.

for many of industrialisation's problems, the nuclear energy option spells a significant reduction in carbon emissions while ensuring an economically affordable energy supply. Nevertheless, nuclear energy production also comes with the terrifying side effect that any negligence or sabotage pertaining to its management could gravely endanger human habitation.[6] The "end of tradition" relates to the dilution of many traditional collective institutions in favour of the greater "individualisation" of society. In earlier modernity, Western societies were structured by a diverse set of collective institutions, including the main Christian Churches; the welfare state; the social class-system; and organisations that promoted strong community-based social capital. As many of these institutions have faded, social expectations now place individual responsibility to form one's own biography and social outlook in the foreground.[7] Collective social institutions were once the building blocks for the cohesive nation-state. This cohesion created a relatively orderly social context that benefited governments implementing policy. The eclecticism of today's individualised Western societies means that government decision-making is a more disruptive process by comparison. This is a point that holds particular resonance for security policy. The risk society literature offers many über large-frame perspectives relating to society's ongoing modernisation trajectory. By narrowing the scope of this logic to the military-technological sector, this article argues that the "dangers of modernisation" and government policy at risk of disruption are important background factors to consider when analysing the West's evolving approach to the deployment of Remotely Piloted Aircraft Systems (RPAS), alternatively described as drones.

What Beck outlines as the "boomerang effect" can provide considerable insight concerning the unintended side effects of Western military strategy today. The "boomerang effect" is a social condition that Will Atkinson has described as "the reacting back of risks on those who produced them".[8] The next section will examine the Western hegemonic security burden and the domestic-strategic contradiction created for its risk societies because of this. The article will then develop the argument that strategic side-effects from military drone utilisation can be identified in three important areas. First, drone strikes can create the backlash of stronger "siege mentalities" among the non-combatant population in conflict areas. This risks galvanising radicalisation leading to the emergence of "accidental guerrillas". Second, unrivalled technological superiority can produce military doctrines that depend excessively on this advantage. As an influence on force planning, this can leave ground forces unprepared and underdeveloped, with the "versatility" that they specialise in still crucial for effective stabilisation operations. Third, there is an eventual risk that Western-pioneered military technologies will later disperse at different rates to aspiring strategic competitor states and terrorist organisations seeking to destabilise Western strategic objectives. This article's conclusion will reflect on emerging military technologies within the context of the security strategies of smaller states.

Dilemmas of the hegemonic security burden

Social change has ensured that Western societies have become increasingly risk-averse in producing the collective action that is required for international security management. With the NATO-led International Security Assistance Force (ISAF) in Afghanistan, this risk-aversion has

[6] Beck, Op. Cit, 60-61.

[7] Darryl S.L. Jarvis, "Risk, globalisation and the state: A critical appraisal of Ulrich Beck and the world risk society thesis," *Global Society*, 21, no. 1 (2007): 26-28.

[8] Will Atkinson, "Beck, individualization and the death of class: a critique," *British Journal of Sociology*, 58, no. 3 (2007): 352.

been transparently on display for more than a decade. While politically compelled to contribute militarily to Afghanistan's stabilisation, many NATO allies imposed stringent national caveats to limit the combat exposure of their military deployments.[9] This problematically exacerbated the complexity of ISAF's operational planning structure. Military fatality counts taken at different intervals for ISAF routinely place the US and the UK, the missions leading states, within the top five most affected participants. Other regulars in this bracket have included Denmark, Estonia and the Netherlands, smaller states where a relatively low number of fatalities can still produce a large per capita figure.[10] Among NATO's larger states, owing to less combat exposure, France, Germany, Italy, Poland and Spain all display significantly lower military fatality rates per capita compared to the US and the UK.[11] As well as discourse around an unfair distribution of combat risk, US perceptions stressing a European over-dependence on US military capabilities for expeditionary operations were further galvanised after Operation Unified Protector (OUP) in Libya.[12] In 2011, US Secretary of Defence Robert Gates gave a landmark speech in Brussels to highlight widening transatlantic ruptures. Gates warned of the grave problem of NATO becoming a "two-tiered" alliance divided between allies that can make a tangible military contribution and others unable to do so.[13]

In seeking to capture the deeper social roots shaping Western society's increased risk-aversion pertaining to the military burden for international security, Christopher Coker has combined the risk society outlook with postmodern social theory. Central to this is the concept of "liquid societies" first developed by Zygmunt Bauman.[14] Just as liquids "do not hold their shape for long", postmodern "social bonds" are also extremely fluid. Many formative social bonds are increasingly temporary in substance.[15] The idea of "liquid alliances" fares well to explain recent experience in NATO alliance politics. Political and military liaisons have become increasingly flexible, with commitments undertaken on a contingent basis and long-term strategic perspectives often conspicuously absent.[16] These underlying social tendencies illustrate a worrying pattern considering the vast range of socio-economic "public goods" that have traditionally accumulated from the West's management of international order.

Military power remains vital towards ensuring a stable and predictable international order. Different military instruments are required to curb the prevalence of terrorist networks; to reduce opportunities for transnational organised crime; and to manage the resurgence of revisionist states orchestrating limited destabilisation for their own strategic ends.[17] Should the West disengage its military power from these functions, Richard Haass has a pessimistic view towards the "non-polar" international order that might follow. Haass' argument again captures the domestic-strategic contradiction that currently confronts Western risk society. While desired by some aspiring non-Western powers, enhanced multi-polarity will redistribute power too chaotically within the international system. Finding the consensus required to manage

[9] James Sperling and Mark Webber, "NATO: From Kosovo to Kabul," *International Affairs*, 85, no. 3 (2009): 507.

[10] Steve Coll, "Burden Sharing," The New Yorker, March 11 2010, accessed September 2 2019, https://www.newyorker.com/news/steve-coll/burden-sharing .

[11] Coll, Op. Cit. For constantly updated data on NATO military fatalities in Afghanistan, see "iCasualties", accessed September 2 2019, http://icasualties.org/App/AfghanFatalities .

[12] James M. Lindsay, "George W. Bush, Barack Obama and the future of US global leadership," *International Affairs*, 87, no. 4 (2011): 779.

[13] Robert M. Gates, "Remarks by Secretary Gates at the Security and Defense Agenda, Brussels, Belgium", US Department of Defence, press release, June 10 2011, accessed July 1 2019, http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=4839.

[14] Zygmunt Bauman, *Liquid modernity* (London: John Wiley & Sons, 2000).

[15] Christopher Coker, *War in an age of risk* (Cambridge: Polity, 2006): 20.

[16] Coker, Op. Cit., 20.

[17] For explanation of "limited war" as a form of destabilisation in the conflict between Russia and Ukraine, see Lawrence Freedman, "Ukraine and the art of limited war," *Survival*, 56, no. 6 (2014): 7-38.

many severe security risks will prove arduously difficult under such circumstances.[18] Should Western military hegemony decline, control will be further loosened on actors holding the potential to destabilise international order.[19] Despite the well-flagged risks that a reduction in Western security management would likely create, the common transatlantic commitment to undertake the responsibilities necessary for this continues to come in for doubt. "Burden-shifting" remains a problematic practice.[20]

As a recent evolution of "burden-shifting" in Europe, it has been argued that once the US stations a modest military deployment to support an allied state, populations in many of the hosting states become less willing to commit resources to their own national defence.[21] Such attitudes tacitly portray a preference for the various risks of collective defence to be transferred to Washington. Tense alliance politics over the thorny issue of NATO burden-sharing is not new. Speaking in 1970, Harlan Cleveland, the US ambassador to NATO, described the alliance as "an organised controversy about who is going to do how much".[22] However, while a prominent transatlantic theme up until the Obama presidency, President Donald Trump's rhetoric on this subject has sometimes been especially abrupt and abrasive.[23] Little chastisement has been spared for some European NATO members that Trump perceives to be avoiding their fair share of NATO's collective defence responsibilities.[24]

Risk-aversion and the US strategic posture

Despite Washington's long-standing frustrations towards its European allies, it can be argued that the US has itself also become increasingly risk-averse in its security policy over recent years. Seen primary through its approach to the Syrian war; the US has grown cautious concerning ground force deployments.[25] According to Mikkel Vedby Rassmussen, rather than the traditional security dilemma, US foreign policy for the unipolar era has instead been challenged by a "reflexive security dilemma". The US and its allies have not as yet had to contend with "a serious military threat from any [competing] power".[26] US security management has instead focused on a fluctuating strategic environment that continuously generates an uncertain set of risks. Under these circumstances, the challenge for Western policymakers involves the rationalisation of "what conflicts or security issues in general, are important to one's security".[27] When military force needs to be applied in the absence of well-defined strategic parameters, policymaking becomes open-ended. Policy questions surrounding the correct utility and measure of military force become vital to effectively manage a particular risk. Highlighted by the calamitous destabilisation caused by the US-led intervention in Iraq in

[18] Richard N. Haass, "The age of nonpolarity: What will follow US dominance," *Foreign Affairs*, 87, no. 3 (2008): 50-52.

[19] Ibid., 51-52.

[20] Wallace J. Thies, *Friendly rivals: Bargaining and burden shifting in NATO* (Armonk, NY: M.E. Sharpe, 2003): 7.

[21] Jo Jakobsen and Tor G. Jakobsen, "Tripwires and free-riders: Do forward-deployed US troops reduce the willingness of host-country citizens to fight for their country?," *Contemporary Security Policy*, 40, no. 2 (2019): 135-164.

[22] Harlan Cleveland cited in Tomáš Valášek, "A new transatlantic security bargain," *Carnegie Europe*, May 23 2017, accessed September 2 2019, http://carnegieeurope.eu/2017/05/23/new-transatlantic-security-bargain-pub-70050 .

[23] Eoin Micheál McNamara, "Between Trump's America and Putin's Russia: Nordic-Baltic security relations amid transatlantic drift," *Irish Studies in International Affairs*, 28 (2017): 74-77.

[24] Katrin Bennhold, "German Defense spending is falling even shorter. The US isn't happy," *The New York Times*, March 19 2019, accessed July 1 2019, https://www.nytimes.com/2019/03/19/world/europe/germany-nato-spending-target.html.

[25] Andreas Krieg, "Externalizing the burden of war: the Obama Doctrine and US foreign policy in the Middle East," International Affairs, 92, no. 1 (2016): 97-113.

[26] Mikkel Vedby Rasmussen, "'A parallel globalization of terror': 9–11, security and globalization," *Cooperation and Conflict*, 37, no.3 (2002): 328.

[27] Rasmussen, Op. Cit., 328.

2003, Western policymakers have sometimes got this balance profoundly wrong. Failure here has contributed to "war fatigue" across Western societies, creating a path-dependency that has shaped only tentative approaches towards more recent conflicts. Despite this pattern, inaction is regularly perceived as strategically unaffordable. Therefore, risk-efficient military technologies have become increasingly crucial for Western security management. These technologies can reduce the need for ground force deployments, thus easing the risk of military casualties. Nevertheless, the Western military embrace of advanced technologies such as surveillance and fighter drones will also inevitably harbour unintended "boomerang effects" that can later unexpectedly undermine the West's strategic objectives.

Accelerated by the Revolution in Military Affairs (RMA) that flourished during the 1990s, precision-strike technology has since transformed NATO's approach to peace enforcement. The primacy of NATO airpower was seen in earnest with Operation Allied Force (OAF) against Serbia's military actions in Kosovo in 1999. However, it was the NATO-led OUP in Libya in 2011 that illustrated how ineffective airpower on its own can be when stabilisation is the ultimate strategic objective. Colin S. Gray argues that it is crucial to see war as "about the peace it will shape".[28] Beyond the initial phases of an intervention, this is a task that airpower alone is unable to service. An international peacekeeping presence was not agreed after OUP, Libya's fragile state institutions have since failed to prevent a descent into violent deterioration. One major "boomerang effect" from OUP has been the dense outward refugee flows from war-torn Libya. The subsequent management of these flows has created some severe political discord within the EU since 2015.

Drone warfare has emerged as a central feature in the US approach to security management over the past decade. Barack Obama has frequently been described as America's "first drone president".[29] The extensive use of drone strikes to combat suspected terrorist networks and insurgency strongholds has continued under the Trump administration. President Trump has approved legislation that reverses previous transparency concerning civilian deaths occurring from US drone strikes outside Afghanistan and Iraq.[30] US drone strategy is consistent with the deeper "presence of the future" anxieties of the Western risk society. The logic of "targeted killing" is preventative in its focus; it aims to disrupt or destroy important nodes in terrorist or insurgent networks before these can coordinate attacks on American citizens or the US military presence abroad. Risk-aversion has been a primary social condition that has underpinned the evolution of drone warfare. Attempting to persuade the US population of the ethical virtues of drone use, Obama has emphasised the headline message that "drone strikes have saved lives".[31] With the objective to dismantle terrorist networks, drone strikes have been described as a risk-efficient and "convenient" substitute for ground force deployments.[32] According to Daniel Byman, further advantages include constant disruption of the mobility of terror group members; a light military footprint that only minimally violates the sovereignty of a state where a strike takes place; and a decreased dependency on counterterrorism cooperation

[28] Colin S. Gray, "How has war changed since the end of the Cold War?," *Parameters*, 35, no. 1 (2005): 21.

[29] Jared Keller, "America's long history of hiding airstrikes," *Pacific Standard*, October 6 2015, accessed July 1 2019, https://psmag.com/news/americas-long-history-of-hiding-drone-deaths.

[30] "Trump revokes Obama rule on reporting drone strike deaths," BBC News, March 7 2019, accessed July 1 2019, https://www.bbc.com/news/world-us-canada-47480207.

[31] "Barack Obama: 'drone strikes have saved lives'," *The Guardian*, May 24 2013, accessed July 1 2019, https://www.theguardian.com/world/video/2013/may/24/barack-obama-drone-strikes-save-lives-video.

[32] Daniel L. Byman, "Why drones work: the case for Washington's weapon of choice," *The Brookings Institution*, June 17, 2013, accessed July 1 2019, https://www.brookings.edu/articles/why-drones-work-the-case-for-washingtons-weapon-of-choice/.

with intelligence services from states with severely poor human rights records such as Pakistan and Yemen.[33]

Drone technology and flawed exaggerations

Despite these strategic benefits, drone warfare does not render the US or its allies immune from the "boomerang effects" that the utilisation of this technology can create. Drone strikes for preventative counterterrorism or counterinsurgency operations put severe pressure on the vulnerabilities of the Western intelligence community. Mistakes with intelligence were intrinsic to the profoundly flawed pre-emptive strategy employed by the US-led coalition for the Iraq war in 2003.[34] Decision-making for preventative drone strikes is heavily guided by intelligence information. This information is gathering through an imperfect process. Mistakes and misjudgements routinely occur. This increases the risk that drone strikes will find unintended targets. These errors facilitate the destruction of innocent civilian life as well as critical physical infrastructure.[35] In earlier modernity, military strategy was defined by "means-end rationality".[36] With drone strikes an important focal point, the rigidity of this thinking is now very problematic. Contrary to an "end", there is instead often a spill-over into second-order risks. While meeting the first objective to destroy or disrupt a terrorist or insurgent network in a particular location, drone strikes can still undermine the West's wider strategic objectives after this.

The attitude of the local civilian population is perceived by many strategists as the "centre of gravity" that decides today's counterinsurgency campaigns.[37] While a formidably difficult task, ground forces still have opportunities to gain the cooperation of local populations and thus shape this "centre of gravity" more in their favour. By contrast, the ruthlessness and facelessness of "targeted killing" through drone strikes carries high potential to create a "siege mentality" against Western strategic objectives in a conflict area that cannot be counteracted.[38] This pattern of events has occurred in Pakistan's Federally Administered Tribal Area (FATA), a Taliban stronghold and a considerable menace for the NATO forces that have sought to stabilise southern Afghanistan. Persistent US drone strikes in the FATA have constantly agitated local residents. At the same time, NATO has had no "political presence" in the FATA to ease the risk of aggrieved local residents becoming "accidental guerrillas".[39] This risk should not just be seen as locally contained. With today's strategic conditions sometimes described as the "globalisation of civil war", the transnational imagery of "targeted killing" can strengthen the position of the "recruiting sergeants" that seek to bolster terrorist organisations in different locations.[40] Grievances elsewhere can still act as an asset for those seeking to radicalise "foreign

[33] Byman, Op. Cit.

[34] Robert Jervis, "Why the Bush Doctrine cannot be sustained," *Political Science Quarterly*, 120, no. 3 (2005): 351-377.

[35] Chantal Grut, et al., *Counting drone strike deaths* (New York: Columbia University Law School Human Rights Institute Report, 2012), accessed July 1 2019, https://www.law.columbia.edu/sites/default/files/microsites/human-rights-institute/files/COLUMBIACountingDronesFinal.pdf.

[36] Mikkel Vedby Rasmussen, *The risk society at war: Terror, technology and strategy in the twenty-first century* (Cambridge: Cambridge University Press, 2006): 13.

[37] Isabelle Duyvesteyn, "Hearts and minds, cultural awareness and good intelligence: The blueprint for successful counter-insurgency?," *Intelligence and National Security*, 26, no. 4 (2011): 456.

[38] Frank Sauer and Niklas Schörnig, "Killer drones: The 'silver bullet' of democratic warfare?," *Security Dialogue*, 43, no.4 (2012): 372-373.

[39] Leila Hudson, Colin S. Owens and Matt Flannes, "Drone warfare: Blowback from the new American way of war", Middle East Policy, 18, no.3 (2011):126. The radicalisation process for "accidental guerrillas" is covered in detail in David Kilcullen, *The accidental guerrilla: Fighting small wars in the midst of a big one* (New York: Oxford University Press, 2011).

[40] Matha Crenshaw, "Why America? The globalization of civil war," *Current History*, 100 (2001): 425-432.

fighters" into attacking Western societies or to disrupt Western stabilisation efforts within a particular conflict area as a means of retaliation.[41]

The possession of sophisticated military technologies can lead to institutionalised over-exaggerations that misguide force planning. Observing US military engagement in Afghanistan and Iraq as well as Israel's war against Hezbollah in south Lebanon in 2006, Herbert R. McMaster draws the inference that technological superiority did not significantly reduce the most important uncertainties, or the "fog of war", typically encountered by state armed forces fighting in asymmetric conflicts.[42] The convenience of superior technology can misguide those planning these operations into putting "theory before practice".[43] For McMaster, an obsessive emphasis on technological solutions distracts attention away from military force preparation geared towards the "human, psychological, political and cultural dimensions of conflict".[44] This remains crucial for the Western military organisations that seek to improve as agents of stabilisation as their adversaries "use terrain, intermingle with the population, and adopt countermeasures to technological capabilities" to frustrate their objectives.[45]

Risk and technological dispersal

At the level of strategic competition between the great powers, today's intensified development of Western-pioneered drone and a robotic technology also creates reflexive security concerns. Peter W. Singer warns that there is never a "permanent first mover advantage" for the militaries that initially achieve a technological advantage.[46] Nevertheless, with the "rise of the rest" touted as a consequence of the continuing redistribution of the international balance of power, debate still persists concerning the speed at which sophisticated military technologies will disperse to the states that seek to impede Western strategic objectives. Frank Sauer and Niklas Schörnig outline that the US has utilised surveillance or fighter drones in states such as Iran and Syria that possess considerable anti-aircraft capabilities. If a Western-manufactured drone is captured, hostile forces can obtain the remains of the technology. Damaged drones retain important clues for those seeking to replicate their design.[47] As demonstrated by China, when Western drone technology has been duplicated, the replicating manufacturer has been able to add modifications to accommodate the strategic purposes of the procurer.[48] Nevertheless, it has been argued that it is important not to exaggerate the speed at which Western drone technology might disperse. According to Andrea Gilli and Mauro Gilli, the most sophisticated drone systems, capable of precise or maximised devastation, are incredibly complex to produce.[49] The management of immensely complex "industrial, organisational and infrastructural" capacities is required to retain an edge in the development of military drone technology. The drone manufacturing programmes of the most industrially advanced states in the world the US, the UK, Germany and France have all occasionally suffered severe setbacks.[50]

[41] Sauer and Schörnig, Op. Cit., 327.

[42] Herbert R. McMaster, "On war: Lessons to be learned," *Survival*, 50, no.1 (2008): 26-27.

[43] Ibid., 25.

[44] Ibid., 27.

[45] Ibid., 27.

[46] Peter W. Singer, "The future of war," in *Ethical and legal aspects of unmanned systems*, ed. Gerhard Dabringer (Vienna: Institut für Religion und Frieden, 2011): 79.

[47] Sauer and Schörnig, Op. Cit., 371-372.

[48] Ibid., 371-372.

[49] Andrea Gilli and Mauro Gilli, "The Diffusion of drone warfare? Industrial, organizational, and infrastructural constraints," *Security Studies*, 25, no. 1 (2016): 50.

[50] Gilli and Gilli, Op. Cit., 50.

Spurred on by the RMA's focus towards Information Technology (IT), complexity in military technology manufacturing has increased exponentially over recent decades. For Gilli and Gilli, the more the complexity, the more "incompatibilities and vulnerabilities" are generated within the production system.[51] Through open-source information; conventional intelligence gathering; and cyber espionage, China's military-industrial base has been broadly exposed to Western technological manufacturing practices. The research and development systems that Beijing possesses for its military's technology are still yet to cope with the same levels of complexity as Western equivalents.[52] While possessing a military-industrial base advantaged by deeper historical foundations, Russia's problems in the same area are more nuanced. President Vladimir Putin has proclaimed Moscow's ambition to "lead the world" in the development of Artificial Intelligence (AI).[53] However, as evidenced by the failure of his predecessor Dmitri Medvedev's "modernisation from above" initiative for Russia's civilian economy, a society that is perpetually riddled with "Endemic corruption, no protections for private property, and a pervasive state security apparatus" is unlikely to stimulate the innovation required to achieve Putin's lofty objective.[54] These deeply entrenched structural weaknesses connected to the respective Chinese and Russian military-industrial complexes should provide US and EU policymakers with some relief that the dispersal of advanced Western technologies will not rapidly accelerate and thus majorly assist Russia's or China's military prowess over the immediate term.

Nevertheless, while plausible from the angle of great power competition, this analysis has the crucial flaw in that it does not account for non-state terrorist and insurgent organisations and the profound harm that even rudimentary imitation of Western drone technologies can still cause. Drone technology has been improvised by an anti-government militia in Yemen to target a ceremonial parade attended by many of that state's military elite. As it exploded in the air to rain shrapnel on those below, the drone utilised by rebels resembled a remote-controlled "dirty bomb".[55] In a brutal conflict where many grievous human rights atrocities have been committed, Saudi Arabia has militarily intervened to support Yemen's beleaguered government. Exchanges between the Saudi military and Yemen's Houthi militias provide further lessons on how even rudimentary drone utilisation can strategically advantage guerrilla forces. Houthi rebels have been able to use drones of modest sophistication to interfere with the radar systems that guide Saudi Arabia's US-manufactured *Patriot* anti-missile batteries. With these temporarily nullified, Houthi militias have gained the opportunity to shower missiles onto Saudi Arabia's neighbouring territories.[56] In a globalised world, effective insurgent tactics assisted by improvised technologies can be quickly replicated elsewhere. The emerging centrality of different drone technologies in contemporary conflict strategies is a "boomerang effect" with its source in the modernisation led by Western states. Concerning the US development of drone technology specifically, Conor Friedersdorf surmised the unintended repercussions

[51] Andrea Gilli and Mauro Gilli, "Why China has not caught up yet: Military-technological superiority and the limits of imitation, reverse engineering, and cyber espionage," *International Security*, 43, no. 3 (2018/19):149.

[52] Gilli and Gilli, Op. Cit., 187-189.

[53] Radina Gigova, "Who Vladimir Putin thinks will rule the world," CNN, September 2 2017, accessed July 1 2019, https://edition.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html.

[54] Aaron Bateman, "Russia's quest to lead the world in AI is doomed," *Defence One*, June 12 2019, accessed July 1 2019, https://www.defenseone.com/ideas/2019/06/russias-quest-lead-world-ai-doomed/157663/.

[55] Conor Friedersdorf, "The unstoppable spread of lethal drones," *The Atlantic*, January 31 2019, accessed July 1 2019, https://www.theatlantic.com/ideas/archive/2019/01/killer-drones/581722/.

[56] Friedersdorf, Op. Cit.

with the outlook that "The United States [has] hastened the proliferation of a weapon that diminishes its relative power".[57]

Conclusion – risk technologies and smaller states

As the domestic-strategic contradiction continues to affect the security management approaches taken by Western societies, the first-order strategic benefits that RPAS and other advanced military technologies can offer will become insatiable for many governments. Many of the second-order risks connected to the utilisation of these technologies, a sample of which this article has discussed, so-far tend to only be seriously evaluated at a later stage, and often "after the horse has bolted" where dangerous proliferation is concerned. The spread of today's advanced military technologies is not just a preserve for great power politics. In crafting their military postures towards the 22nd century, demand for these technologies among many smaller states will also be considerable. With the Baltic states as a potential European example, autonomous, unmanned or unpiloted military technologies that are risk-efficient in terms of manpower will prove particularly attractive for smaller states seeking to enhance deterrence as a solution for asymmetric defence predicaments. The management of a perpetually war-torn strategic environment in the Middle East will continue to attract other smaller states such as Israel and the Gulf states towards the advantages of the same technologies as they evolve. With RPAS already a firm fixture in many conflict areas, the large-scale debut of AI-directed autonomous weapons systems is now an inevitable and imminent prospect.

This outlook indicates a conundrum for Ireland's security policy. The 2018 US National Defence Strategy (NDS) foresees that the globalised civilian commercial sector will continue to lead in the production of emerging military technologies. This includes "advanced computing, 'big data' analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology".[58] The larger incorporation of these technologies with the military-industrial complex has rendered "dual-use" components; interchangeable between military and civilian adaptations, ever more common. These components will be vital for the continuing development of remote-controlled and AI-driven autonomous weapons systems. The proliferation of these weapons will risk a further separation between the practice of war and humanitarian ethics. Ireland's open economy is tightly interlinked with the global supply-chains that integrate many military and civilian technologies. This is, therefore, not a pattern that Irish society can ethically detach itself from. Projecting a prominent and informed voice to lobby for stronger normative frameworks to regulate the flow of emerging military technologies will allow Ireland's foreign policy to make a responsible contribution to international security affairs as the 22nd century approaches.

[57] Friedersdorf, Op. Cit.

[58] James Mattis, Summary of the 2018 *National Defence Strategy of the United States of America: Sharpening the American military's competitive edge* (Washington DC: US Department of Defence, 2018): 3.

MULTI-DOMAIN OPERATIONS:
The Need to Develop Resilience and Capability.

Comdt Gavin Egerton
Deputy Chief Instructor, EUTM, Mali.

Abstract

This paper examines the concept of Multi-Domain Operations and its emergence as the widely accepted template for managing contemporary and future conflict. The paper adopts the position that Ireland as a country, but the Defence Forces specifically, would benefit from a more pro-active approach to defence, developing a comprehensive set of capabilities across increasingly important but less traditional domains. The author will argue that the Defence Forces should adopt such an approach not just to develop resilience to a multi-domain attack, but also invest in acquiring an offensive capability.

The paper will offer historical context to doctrinal change, and how the Defence Forces could benefit from studying how other countries have adopted change; using the U.S Army's implementation of Air Land Battle as an example. The paper will illustrate how the multi-domain battle plays out, and how other militaries embraced change and made significant leaps in doctrine and capability.

The paper will outline how a mind-set based on adherence to the 'Mission Command' leadership philosophy and the subscription to the 'Manoeuvrist Approach' will serve as a foundation for building a multi-domain capability. The Defence Forces' adoption of both these philosophies has conveniently provided it with the doctrinal and cultural starting point for Multi-Domain Operations. However, successful implementation of a new concept and subsequent doctrine will be contingent on an open-minded approach to future force structuring as well as securing necessary capital investment.

Introduction

Traditionally, dominance of the heretofore universally accepted three domains of operation – air, land, and sea – has provided a conventional military force with a more than favourable chance of victory over a similar opponent operating in or near those domains. However, there is an increasing acceptance amongst contemporary militaries and academics that "historical approaches to achieving superiority in the air, land, and sea domains may no longer be valid"[1]. There has emerged, a new contemporary operating environment which extends into multiple different domains. Some of the factors driving this change include the affordability and accessibility of high-end technology, particularly in the air, space and cyber domains, and the advent of information warfare. While on one hand Remotely Piloted Aircraft System (RPAS) platforms are becoming smaller, cheaper, and more capable; on the other hand information is becoming increasingly weaponised, and the willingness of governments to engage in information warfare is growing rapidly.

Although the fundamental nature of war is unlikely to change, the ways and means in which it is fought are evolving; expanding beyond the theory and practice of combined, joint operations to include numerous traditional and emerging domains concurrently. This paper will introduce the reader to the concept of Multi-Domain Operations, and highlight

[1] Dr Jeffery M. O'Reilly, "Multi-Domain Operations: A Subtle but Significant Transition in Military Thought", *Air and Space Power Journal,* Spring (2016): 61-73

the opportunity presented to the Defence Forces to initiate and promote early discussion on this topic, mitigate its impact, and develop a range of capabilities in this area.

What is Meant by 'Multi-Domain Operations'?

The concept of Multi-Domain Operations is not new. The close relationship between actions across the air, land, and maritime domains has been the key to success in many wars throughout the 20th century. One just has to consider the Operation Overlord 'D-Day' landings at Normandy for a historical example. However, the domains the Allies operated in during Overlord were not as expansive as what today's battlefields present. The 2017 United States Army/Marine Corps white paper 'Multi-Domain Battle: Combined Arms for the 21st Century' recognises the limitations of a two or three domain approach to military operations. It posits that future wars will be fought across the "physical domains of air, land, sea, and space, the 'abstract' domain of cyberspace, as well as the electromagnetic spectrum (EMS), the information environment, and the cognitive dimension of warfare"[2]. While warfare will likely continue to be focused on land, the integration of assets from other domains adds to the existing challenges facing land component commanders. Looking at current trends, the "number of actors able to employ capabilities in the air, sea, space, and cyberspace domains increases"[3]; meaning a conventional land force can no longer enjoy dominance of that domain, and can be threatened by relatively low-cost technology from the air, and cyberspace domains.

The aim of Multi-Domain Operations is to overwhelm one's opponent with multiple, disparate yet interdependent problems, overloading decision making processes and ultimately rendering defensive forces ineffective. By way of a definition, Multi-Domain Operations;

> *"provide commanders numerous options for executing simultaneous and sequential operations using surprise and the rapid and continuous integration of capabilities across all domains to present multiple dilemmas to an adversary in order to gain physical and psychological advantages and influence and control over the operational environment"[4].*

This is reflected in current U.S. Army doctrine, where according to the recently revised U.S. Army field manual on operations: "All Army operations are multi-domain operations, and all battles are multi-domain battles"[5].

Implementing Doctrinal Change

Prior to examining Multi-Domain Operations in detail, it is pertinent to look to the recent past where a significant evolution in U.S. military doctrine was successfully devised and implemented. The introduction of new doctrine in the early 1980s and how it was adopted gives an indication as to how the transition to Multi-Domain Operations might occur. A small military like the Irish Defence Forces (DF) can draw inspiration from larger organisations as to how they embrace change.

[2] "United States Army-Marine Corps White Paper: Multi-Domain Battle: Combined Arms for the 21st Century", Jan 18 (2017),
[3] Gen. David G. Perkins, "Multi-Domain Battle, The Advent of Twenty-First Century War", Military Review, Nov-Dec (2017): 8-13.
[4] U.S. Army Training and Doctrine Command. "Multi-Domain Operations", Oct 10 (2018). Accessed Jun 24 (2019). url: https://www.tradoc.army.mil/Publications-and-Resources/Article-Display/Article/1655556/multi-domain-operations/
[5] Department of the Army. "FM 3-0: Operations". Oct 06 (2017): 1-17

In an attempt to bridge the gap between doctrinal text books and units executing tactical tasks, the U.S. Army, in the early 1980s, devised a multidimensional warfighting doctrine called 'Air Land Battle'. Inspired by the combined arms German 'Blitzkrieg' of World War II, it was seen as a "shift from a focus on low-intensity, small-unit, decentralized counterinsurgency operations to larger-scale operations, heavily dependent on sophisticated technology for decisive operations fighting outnumbered"[6]. This was a conscious migration from the Vietnam era warfare to the potential European war against the Soviet Union; should the Cold War heat up. Air Land Battle focused on the successful integration of land forces such as tanks, armoured infantry, and mobile artillery; with close combat aviation support (i.e. attack helicopters) to destroy enemy armour, and Air Force support to strike the enemy's rear areas in order to restrict the flow of logistics. It was devised in parallel with large scale procurement projects such as the AH-64 Apache attack helicopter, the M1A1 Abrams main battle tank, the M2 Bradley infantry fighting vehicle, and the UH-60 Black Hawk utility helicopter; recognising and exploiting new capabilities and integrating them together for combined arms operations. The Air Land Battle concept was rehearsed, refined, and repeated throughout the 1980s until it was finally tested in combat in 1991. This trial by fire was not against the anticipated foe of the Soviet Union, but rather Saddam Hussein's vast Iraqi army during Operation Desert Storm in the Persian Gulf. The joint offensive capability demonstrated during Desert Storm justified the extensive investment in combined arms and joint training throughout the 1980s and established the United States of America as the dominant world power; in military terms at least. But this hegemony was challenged in the first decade of this century, by the shift from conventional warfighting to asymmetric, terrorist, and hybrid warfare, forcing western militaries to rethink their doctrine.

Relatively inexpensive improvised explosive devices in Iraq and Afghanistan caused significant casualties, and continue to do so. During the lifetime of the NATO-led International Security Assistance Force (ISAF), NATO and coalition forces suffered 1,401 deaths to IEDs, just over 50% of total combat losses[7]. This is despite the presence of the most advanced combat and force protection equipment ever produced and employment of a thoroughly rehearsed and battle-proven combined, joint doctrine.

The United States' adversaries or potential future adversaries have studied the performance of the U.S. military during the Gulf War and are "adapting their methods of warfare, while accelerating the modernization and professionalization of their combat forces"[8]. Instead of trying to match or out-gun the U.S. military they strive "to gain strategic advantage by offsetting the advantages [the U.S. military has] enjoyed over the last twenty years"[9]. Essentially, asymmetry in terms of mass or combat power is no longer a decisive factor in battle.

[6] Col. Scott King, U.S Army retired; Maj. Dennis B. Boykin IV, U.S. Army retired: "Distinctly Different Doctrine: Why Multi-Domain Operations Isn't Air Land Battle 2.0", Association of the United States Army, Feb 20 (2019). Accessed Jun 25 (2019). https://www.ausa.org/articles/distinctly-different-doctrine-why-multi-domain-operations-isn%E2%80%99t-airland-battle-20.

[7] Areppim. "Afganistan War: Coalition Deaths 2001 – 2014", Feb 17 (2015). Accessed Jun 28, 2019. url: http://stats.areppim.com/stats/stats_afghanwar_ied.htm

[8] Gen. David G. Perkins, "Multi-Domain Battle, The Advent of Twenty-First Century War", Military Review, Nov-Dec 17: 8-13.

[9] Ibid

Emergence of the Multi-Domain Operations Concept

The widespread promulgation of the phrase 'multi-domain battle' can be attributed to then U.S. Army General, David G, Perkins. In 2016 Perkins proposed a future warfare concept[10] that saw space and cyberspace being added to the heretofore hegemonic paradigm of 'joint operations' utilising the air, land, and maritime domains. Perkins suggests that the close synchronicity of interdependent and simultaneous assaults on the enemy from as many domains as possible would overload enemy decision making, disrupting their command and control. This saturation of the enemy with disparate and competing problems would frustrate efforts to engage on multiple fields simultaneously. For example, a land force attacking a similarly equipped force, would not only continue to operate with the traditional joint support from air and maritime fires as with Air Land Battle doctrine, but could enjoy disproportionate advantages by neutralising the enemy's communications, harassing domestic populations with economically and socially catastrophic cyber-attacks, targeting forward forces with numerous cheap, low profile RPAS, whilst dominating public opinion via a well-scripted narrative in the media to discredit the enemy's activities and behaviours as illegitimate.

The DF cannot afford to ignore the advent of such warfare, and by engaging in healthy discussion early, it can offset the potentially catastrophic impact of operating in such an environment. Whilst the DF doesn't necessarily need to prepare to engage in all of the methods listed above, by maintaining a basic capability in a number of specific areas, relevant to national defence needs, it would be able to develop a resilience based on a professional working knowledge. The creation of a national security and defence strategy would provide a point of reference for identifying and prioritising which capabilities the DF should pursue.

For example, the threat of cyber-attack is quite relevant to Ireland from an economic espionage/terrorist perspective so the cyber domain should be considered a priority area in which to develop a capability. Cyber-attacks are "becoming more of an issue globally with data breaches, DDoS and ransomware attacks, financial scams and state-sponsored hacking incidents all on the rise"[11]. The inherent responsibility for Ireland to protect the European headquarters of the many large multinational corporations based here should be reason alone to develop defences and capabilities in this area. The likely outcome of a cyber-attack would be "widespread disruption for businesses and public agencies, but would also lead to serious reputational damage"[12].

Currently, Ireland as a community is quite vulnerable to cyber-attacks of smaller or greater scales to that outlined in the previous paragraph. This creates an imperative to identify low cost/no cost defences against such threats in the short term, whilst embarking on a capital investment programme to develop more robust defences for the future. Potentially, Ireland but the DF specifically could develop a world-leading cyber defence capability. However, the study and preparation for operating in the emerging multi-domain environment must not be shackled solely to building resilience from a defensive, or passive, mind-set. Instead, the DF should actively pursue the structures to conduct a multi-domain battle organically, and thus build a limited but credible offensive cyber capability. This has the potential to serve as a deterrent against similar attacks against the DF.

[10] Gen. David G. Perkins, panel discussion to Association of the United States Army audience, 04 Oct 16.

[11] Charlie Taylor, "Ireland vulnerable to cybersecurity attack, says industry leader", Oct 18 (2018). Accessed Jun 27 (2019). url: https://www.irishtimes.com/business/technology/ireland-vulnerable-to-cybersecurity-attack-says-industry-leader-1.3666946

[12] Ibid.

Multi-Domain Operations in Practice

The Russian military were early adopters of Multi-Domain Operations. Starting in 2008, the Russian Army began a period of reorganising and modernisation, to "eliminate redundancies and increase lethality and efficiency…creating organizations, equipment, and tactics to synchronize operations across domains"[13]. Russian military doctrine has been adapted to embrace Multi-Domain Operations down to the lowest possible level with battalion tactical groups availing of air, electronic warfare, and cyber assets, as evidenced on multiple occasions throughout 2014 in the Ukraine conflict[14]. An illustrative example of the multi-domain approach at tactical level is perhaps best articulated by the 11 July 2014 strike on Zelenopillya. This was a pre-emptive strike against four Ukrainian brigades as they waited in assembly areas preparing to launch a large scale attack against apparent Russian and Russian-backed partisan forces[15]. Tactical level target acquisition RPAS and complex cyber-attacks against Ukrainian communications systems preceded the strike, followed by an artillery and rocket barrage that killed 30 Ukrainian soldiers, wounded many more and destroyed two battalions worth of combat vehicles[16], thus rendering that Ukrainian force no longer combat capable.

What is significant about the Zelenopillya attack is the marriage between higher level strike assets with tactical level target acquisition and electronic warfare capability. This allowed the rapid employment of higher formation fire support assets at the battalion level, giving the smaller, apparently Russian or Russian-backed partisan unit the confidence and capacity to pre-emptively engage a much larger conventional, armoured Ukrainian force; neutralising them in their assembly areas, and thus preventing their planned assault.

How Should Ireland Invest Time and Resources in Multi-Domain Operations?

In part due to the DF's comparatively modest budget (Ireland spends 0.3% of GDP on Defence; the lowest in the EU[17]), it has never been an exemplar at keeping up with advancing military technologies; predominantly due to their prohibitively (from the DF's perspective) expensive nature. Furthermore, the traditional absence of a comprehensive approach to national defence (and security), has resulted in a consequential lack of joined-up thinking. However, most of the capabilities mentioned above would be far cheaper to defend against – or to develop an offensive capability in – than large scale conventional threats; and would offer utility to a cross-cutting myriad of national areas of interest. For the first time, Ireland might be in a positive position to develop a specific set of military capabilities early and henceforth offset potential threats far in advance, and potentially future-proofing its continued economic prosperity.

As the DF maintains and enhances its conventional capability through robust and realistic training, coupled with continued combat equipment procurement, it should also seek to acquire and maintain capability in emerging domains. As outlined above, cyber is an area that should be given prioritisation and pursued immediately. By developing a resilience to cyber-

[13] Griesemer, Thomas S., "Russian Military Reorganization: A Step Toward Multi-Domain Operations", Over The Horizon Journal, Nov 19 (2018), accessed Jun 27 (2019). url: https://othjournal.com/2018/11/19/russian-military-reorganization-a-step-toward-multi-domain-operations/
[14] Ibid.
[15] Amos, "The Russian–Ukrainian War: Understanding the Dust Clouds on the Battlefield", Modern War Institute, Jan 17 (2017), accessed Jun 29 (2019), url: https://mwi.usma.edu/russian-ukrainian-war-understanding-dust-clouds-battlefield
[16] Ibid
[17] "How Much is Spent on Defence in the EU?", Eurostat, May 18 (2018), accessed Jun 29 (2019), url: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20180518-1

attack (and associated potential information warfare attack) it would reap benefits for both on-island and overseas operations across all three DF components, as well as offering utility to other State agencies. The potential reputational damage for Ireland as a nation, and the associated multinational forces the DF deploy with is enormous, should an overseas Irish Army infantry battalion or Naval Service ship be compromised via a deliberate or opportunistic cyber-attack. By expanding this to an offensive capability at the tactical level – even just as a deterrent – the DF could enhance force protection and increase the chances of mission success if deployed on a robust crisis management operation, or if it found itself engaged in combat.

The threat of electronic warfare should not be overlooked. By ensuring its communications networks are resilient to interference, the DF could protect its communications networks from the type of electronic attack employed at Zelenopillya as outlined above, as well as guarding important communications capabilities vital to the many overseas peace support operations the DF are currently deployed upon. Finally, RPAS is an area the DF could quickly expand beyond its current capability, pushing large numbers of (relatively) low-cost aerial surveillance into the hands of tactical commanders both on-island and overseas, increasing situational awareness, intelligence collection, and ultimately enhancing force protection.

Is the Defence Forces Ready for Such Change?

One could argue that the DF is perhaps already cognitively and doctrinally prepared for Multi-Domain Operations. The DF capstone doctrine states that it recognises the 'Manoeuvrist Approach' to operations, utilising "an indirect method to defeat the belligerent's will…through the creative application of effects against their critical vulnerabilities"[18]. The illustrative example of Multi-Domain Operations in practice outlined above shows how apparently Russian-backed separatists in Ukraine employed creative (indirect) use of low-cost, available air assets to target concentrated (and thus vulnerable) Ukrainian formations, combined with cyber-attack to defeat critical but vulnerable Ukrainian communications. DF doctrine also states that the Manoeuvrist Approach is "multi-dimensional and involves capabilities from the different arms and services of the Defence Forces across the different environments"[19] which is essentially a paraphrasing of what Multi-Domain Operations entail.

Furthermore, as stated in DF leadership doctrine, the organisation adopts the 'Mission Command' philosophy[20]. This decentralised approach to tactical command is encouraged on career courses for both officers and NCOs and one of the Infantry Soldier Principles is to "Promote Mission Command"[21]. This empowerment "allows decision making and freedom of action to be pushed down to the lowest level possible, empowering junior leaders"[22]. The DF could draw inspiration from the Russian model of reorganisation discussed above. The integration of ordinarily higher level assets to the tactical level such as the addition of low-cost RPAS, cyber, and electronic warfare capabilities to battalion (or even company) level, or indeed to Naval Service ships, would likely meet little cognitive resistance or friction in its implementation.

[18] "Defence Forces Capstone Doctrine DFDM – J1", Oct (2015): 50
[19] Ibid.
[20] "Defence Forces Leadership Doctrine" DFDM – J2, Apr (2016): 3-3.
[21] "Infantry Ethos: The Combat Arm – An Lámh Comhrac", May (2018).
[22] Ibid.

Conclusion

Success for the DF in the multi-domain era will be largely contingent on a comprehensive approach to procurement, preparation, and operation. Using the familiar DOTMLPFI spectrum – doctrine, organisation, training, materiel, leadership, personnel, facilities, the DF and Department of Defence will need to be pragmatic in its implementation. This means developing new doctrine, and adapting existing tactics, techniques and procedures, redesigning and adopting a force structure that is far more joint, far more multidisciplinary (all arms, all domains) at the tactical and operational level, and far more flexible. The next generation of procurement of weapons, equipment, and communications infrastructure will need to be future-proofed against cyber and electronic attack, resilient to conventional attack, and capable of operating in the multi-domain environment in all phases of war.

Multi-domain is not new and the close relationship between operations across the air, land, and maritime domains has been the key to success in many wars throughout the 20th century. However, dominance of one or more of those domains is no longer a guarantee of victory. The contemporary operating environment and the likely nature of potential future conflicts require commanders to consider the close integration of space, information, and electromagnetic capabilities. The proliferation of low cost technologies such as RPAS, increased access to cyber capabilities, and the weaponisation of information, means conventional militaries such as the DF must be one step ahead of potential belligerents and spoilers. For the DF to move forward into the Multi-Domain Operations environment, the key to success lies in the convergence of services into a truly joint force, rather than the co-operation and integration of independent service capabilities as is currently the case. This will take an open-minded approach by both the DF and the Department of Defence, particularly where future force design and capital investment are concerned. Perhaps inspiration can be drawn from this excerpt from the first doctrinal manual published by the DF in the era of the newly emerging independent Ireland in 1926:

> *"Our forces are not equipped as liberally as those of large armies, but a sound understanding of all modern means of combat, including those which we do not possess (Aviation, numerous and heavy Artillery, Tanks, etc.) will enable us to find the ways and means to sustain a struggle against an enemy equipped with them."*[23]

[23] "Defence Forces Regulations, Tactical Drill", 1926, as quoted by Colonel (retd) Tom Hodson, "*The College: The Irish Military College, 1930-2000"*, Dublin, The History Press, 2016.

‘FIRST WITH THE TRUTH’

The Paradox of Future Information-led Conflict

Dr. David Reindorp
Execuitve Director, Opportuna: Insight Consulting.

Abstract

‘It is precisely facts that do not exist, only interpretations’[1]

In 2015, the Irish Government published a Defence White Paper which, among other points, emphasised the Irish Defence Forces (DF) ‘continual (and continuing) involvement in UN peacekeeping operations’.[2] In 2018, a seminar directed by the author challenged conventional wisdom regarding the practice of Command and Control (C2). The primary witnesses were the UK commander of perhaps the final pre-information age conflict, and a recently retired UK Chief of Joint Operations. They concluded that C2 as currently practiced is not fit for purpose, and observed that while the UK had closed the gap between today’s capabilities and tomorrow’s wars, it had not made similar progress with regard to concepts. Many of which remain unchanged at a time when the operating environment to which they relate is becoming more complex. The seminar audience acknowledged that closing this intellectual gap will be difficult. They were, however, convinced of the need to do so, to avoid the future practice of C2 being constrained by yesterday’s ideas.

Introduction

The UK Defence Doctrine and Concepts Centre’s (DCDC) Joint Concept Note (JCN) 1/17 offers a Joint Action model where all military activity comes together into a single output labelled ‘*influence*’.[3] The prime enabler of which is to be a technology-enabled capability to analyse and use *information* to make better decisions at the operational and strategic level.[4] This is further developed by JCN 2/18, which introduces the concept of *Information Advantage* and the idea that ‘information … is (now) a fully-fledged national instrument of power’.[5] On the surface these publications offer a compelling thesis, but deeper within questions begin to emerge. For instance, can something intangible and the sum of everything (i.e. *influence*) also be a unique source of power, which can generate advantage over an adversary? There is also an element of assumed novelty to this thinking along with an assumption that information alone can deliver conflict-winning benefit. However, the use of information for military purposes is not new,[6] and there is little doctrine associated with the practice of using information as a source of power.[7]

Meanwhile, and building on this idea of ‘influence’, a recent multi-national command post exercise sought to develop narrative-led campaign plans, each attempting to synchronise information with other activity in an effort to be ‘first with the truth’, thus implying there is a single truth to tell.[8] However, given the increasingly relative nature of political (and thus military) truth, and the declining levels of trust in governments and their institutions, is this a viable objective?

[1] Friedrich Nietzsche, *The Will to Power*, trans. Walter Kaufmann and R. J. Hollingdale (New York: Random House, 1967), 481.

[2] Irish Government Ministry of Defence, ‘White Paper on Defence’ (Dublin, 2015) 32. Available at https://military.ie/en/public-information/publications/.

[3] Defined as ‘the capacity to have an effect on the character, or behaviour of someone or something’.

[4] The author and Vedette Consulting are supporting the UK’s Defence Science and Technology Laboratory (Dstl) Operational Decision Support Tools (OpDST) and Innovative Models, Methods and Techniques (IMMT) projects. Both seek to engage with industry to develop decision-enhancing technology such as military chatbots and Course of Action testing models for use in component-level HQs.

[5] UK Government Ministry of Defence, *Information Advantage*, Joint Concept Note 1/18 (Swindon: Development, Concepts and Doctrine Centre, 2018), iii.

[6] The necessity to know you enemy is enshrined in literature while the use of deception and thus (mis)information is at the heart of the campaign planning process. Sun Tzu and Clausewitz both support this view. The latter suggesting knowledge in warfare to be ‘a factor more vital than any other’.

[7] Although there is doctrine for public relations, media operations and strategic communications, none addresses how a measurable military effect can be achieved by or through influence and information alone.

[8] Observed by the author during a conversation between a 2* UK Commander and his Strategic Communications Advisor on Exercise Joint Venture 2018.

This paper will explore the questions outlined above while avoiding a metaphysical discourse on the nature of truth. From a premise that the truth – in political terms at least – is invariably contested, it will posit that there is an emerging paradox at the centre of this information-led renaissance which will challenge current approaches to strategy, planning, and thus the practice of Command and Control (C2) and military decision making.

Smart and Soft

So where does this new fascination with influence and information begin? According to Utting 'the British military has (now) elevated the importance of soft power ideas (to) the central ... purpose of all military activity ... as the proponents of this approach argue, it is now smart (i.e. clever) to be soft'.[9] This emphasis on being soft is usually linked to Nye's apparent observation that 'it is not (now) whose army wins, but whose story wins'.[10] While Nye acknowledges Arquilla as the originator of this idea, his thinking does shape the smart-to-be-soft agenda.[11] Particularly, that soft power or 'getting others to want the outcomes you want' enables peaceable co-option rather than forcible coercion.[12] Here lies the genesis of the idea that information alone can deliver advantage and win.[13]

Truth and Trust

Trust and truth are linked. For a persona to possess the former, it must also possess the latter. Thus, for an institutional persona such as a military commander to be 'first with the truth' they must be trusted by their audience. However, trust in institutions is declining. According to Lagarde, then chairman of the International Monetary Fund, the world '... is facing a crisis of trust in institutions across all sectors that shows no sign of abating. In 20 out of the 28 countries surveyed by the Edelman Trust Barometer for 2018, average trust in government, business, NGOs and media was below 50%'.[14] Many reasons are offered for this decline: an increasing lack of accountability; the centralisation of power; a growing and often unelected bureaucracy; and increasing opacity in government policy and position.[15] All underpin the rise of 'Distributed Trust' or the idea that an audience instinctively no longer believe what a single institutional source suggests to be true. [16] Rather, they prefer to trust what others say, often as narratives or memes distributed and amplified by networks such as Twitter or the internet. Thus removing the power of determining what is or is not true from a single institutional source, and distributing it across a wide range of disparate sources.

Distributed trust is enabled by technology specifically designed to harness the power of data (i.e. the building blocks of information) via advanced analytics such as machine learning and artificial intelligence. This allows the harvesting and analysis of input from multiple data sources,

[9] Kate Utting, "Strategy, Influence, Strategic Communication and British Military Doctrine" in *Propaganda, Power and Persuasion,* edited by David Welch (London: IB Tauris & Co: 2014) 167. Utting is referring here to JCN 1/17. This use of the word 'smart' in this context should not be conflated with Nye's later development of 'smart power' as a combination of both hard and soft manifestations.

[10] Ibid.

[11] Joseph Nye, "The Information Revolution and Soft Power", *Current History*, 2014 - 113(759): 19-22. Arquilla's actual suggestion being '… in today's global information age, victory may sometimes depend not on whose army wins, but on whose story wins'.

[12]Ibid.

[13] Many others contributed to the development of this concept. For a good review see John Arquilla and David Ronfeldt, ed; In *Athena's Camp* (Santa Monica: Rand 1997).

[14] Christine Lagarde, 'There's a reason for the lack of trust in government and business: corruption', *The Guardian*, May 04, 2018.

[15] Maxine-Laurie Marshall, 'The rise of distributed trust', Oct 2018, https://www.i-cio.com/big-thinkers/rachel-botsman/item/the-rise-of-distributed-trust.

[16] See Rachel Botsman, *Who Can You Trust – How Technology Brought Us Together and Why It could Drive Us Apart* (London: Penguin 2018).

as controlled, and to an extent assured, by algorithms that learn what users are interested in. It is this developed-as-understood process that generates the echo chamber effect of digital media and its ability to turn a relatively innocuous story into a 'shitstorm'.[17] The cumulative outcome of which is an increasing mistrust of the single truth of an institution, and a corresponding increase in belief of the views of individual commentators or communities. As Botsam suggests, '… the idea is that trust, and alongside it power … can now flow directly between individuals without the need for traditional institutions'.[18] And here lies the first element of the paradox of information-led conflict, in that the technologies used to harness the power of *information*, and underpin the concept of *influence*, are also enabling the rise of distributed trust. Making those who seek to be 'first with the truth' less likely to be trusted.

Control and Chaos

Outlining the second element of this paradox requires a return to theory specifically that of the Post-modernists and Foucault who imagined the rise of politically powerful non-state actors long before they became of interest to military practitioners.[19] They argued, presciently, that an increase in the accessibility of information would weaken the international system and challenge state monopoly on global control mechanisms.

Foucault was perhaps the first to explore the utility of information (or more representatively the accretion of information into knowledge) as a source of power. He posited that knowledge, geography and culture were inseparable. This linking of knowledge to place is important for it suggests that a truth can be constantly redefined though education, communication and the reinforcement of political and cultural ideals. In short, information power is subject to the norms of region and thus culture. Truth can thus be relative and arguably little more than a political discourse about the rules according to which the true and false can be distinguished. As Foucault wrote, 'truth … induces regular effects of power… (but) each society has its regime of truth, and its "general politics" of truth: that is types of discourse which it accepts and makes function as true'.[20] Contemporary political behaviour clearly evidences this view.[21] So, while debating the nature of truth remains outside the scope of this paper, acknowledging its contested nature is absolutely necessary. As it is remarking that, this will challenge the endeavour to be 'first with the truth'.

For the commander fighting an information-led battle there is a more prosaic concern within Foucault's thinking. While the use of soft power is arguably not a form of coercion, it is inextricably linked to the establishment of control. It has to be given the role of *Influence* to persuade an adversary to behave in a more advantageous way. Control being usually achieved by focusing power in the hands of a few or removing it from the many. Foucault, however, suggests that knowledge or informational power is both diffuse and pervasive – it 'is everywhere' and

[17] 'Shitstorm' - a term of art applied to social media's ability to spread information rapidly to unlimited amounts of users, turning relatively innocuous memes into a crisis and thence an online attack against a particular person, brand, idea etc as the counter-message 'goes viral'. Its origin is unknown but the term can be found in numerous online dictionaries and also in Durden, the German equivalent of the Oxford English Dictionary. See https://www.theguardian.com/books/booksblog/2013/jul/04/shitstorm-german-dictionary-duden-shitschturm.

[18] Marshall, Op. Cit.

[19] For instance see Michel Foucault, *Power/Knowledge: Selected -Interviews and Other Writings* 1972-1977, (ed. By C Gordon) (New York: Pantheon) 121 – 190. Here Foucault suggests his rethinking of how information operates as power will allow it to 'cut off the King's Head' (i.e. state power) and 'bring into being new schemas of politicisation' that can be exercised by bodies other than the state.

[20] See Paul Rabinow, ed, The Foucault Reader: An Introduction to Foucault's thought (London: Penguin, 1991).

[21] For instance, the rise of the 'false news' debate and agenda.

'comes from everywhere'.[22] Unlike the more traditional concepts of diplomatic, economic and military power, that are confined by policy, law and thus practice to the institutional few, informational power can be gained and exploited for overt political benefit by anyone with the ability to disseminate it. It gains in strength through dispersal, not concentration, and where power is not, or cannot be centralised or contained, it tends to the opposite of what power has traditionally been used for.

This then is the second element of the paradox of information-led conflict. In that its primary enabler – the dissemination of information – dilutes the very power it seeks to create. It reverses the adage that knowledge is power, and thus access to it should be restricted to the few, by providing power to the many. Moreover, where no one group has a monopoly on power, legitimate or otherwise, chaos tends to follow. Chaos, of course, being the antithesis of control and not a normal objective of any planning and decision making process.

Making the Intangible Tangible, or Vice Versa

The possession of power has long been associated with material or tangible resources –wealth, equipment, networks etc. In contrast, information has been seen as intangible and abstract. However, for information to be conceived of as a unique source of power, it must be able to generate a measurable benefit. Indeed, according to JCN 2/18, it must be able to deliver a physical advantage over an adversary. So is information becoming more tangible, or is the concept of power becoming more intangible?

To some this may be a purely academic debate, but to those who first imagined *warfare in the information age* it will lead to some 'interesting implications for the theory and practice of warfare and strategy'.[23] Arguably, we are beginning to see some of these. Perhaps one of the most notable being the initial battle for Fallujah in 2004, which was described as 'the (first) use of global political and propaganda power by insurgents to defeat an otherwise successful (kinetic) attack'.[24] If this assessment is correct, what does it mean for the practice of warfare in general and C2 in particular? Practice here being defined as the decision making necessary to implement strategy by planning and delivering military operations that generate advantage and thus win.[25]

The accepted military discourse on strategy and planning is rooted in the language of tangibility. Its constituent parts are the rules or building blocks of strategy and operational planning such as end states, objectives, centres of gravity, decisive conditions and supporting effects. To which are added other tangible constraints. Joint Operating Areas (JOAs) confine activity geographically. Timescales, often politically imposed, confine temporally. Rules of engagement define and thus confine what and who can be targeted. There are some exceptions to this tangibility, Clausewitz's 'fog' and 'friction' being two examples. However, his counterpoint ideas of culmination and rational calculus are physical in conception and thus tangible. As

[22] Foucault's ideas on power and information are spread across multiple works, many not instantly associated with strategic thinking. Nevertheless they are relevant to the idea of Influence and Information Age warfare and conflict. This interpretation is abstracted from Michel Foucault, *The History of Sexuality: The Will to Knowledge Vol1* (New York: Pantheon Books 1978) 63 – 65. Retrieved from http:\\ suplaney.files.wordpress.com/2010/09/foucault-the-history-of-sexuality-volume-1.pdf.
[23] John Arquilla and David Ronfeldt, "Information, Power and Strategy", in *In Athena's Camp*, ed John Arquilla and David Ronsfeldt (Santa Monica: Rand 1997) 142.
[24] David Welch, "Opening Pandora's Box" in *Propaganda, Power and Persuasion*, ed David Welch (London: Tauris 2014) 13.
[25] The author acknowledges this is an incomplete definition but suggests it is sufficient for the purposes of this (short) article.

is the standard Plan, Refine, Execute, Assess (PREA) cycle adopted by NATO, UK and US operational HQs. The governance of which is metric based and thus by definition, tangible.

Yet information-led conflict need not follow any of these rules. For example, the power of information rests in its diffusion or spread, thus it is not confinable by geography. Unlike conventional military power (air, land, maritime etc.) which can be developed before being used, informational power is developed while being used. It cannot, therefore, be confined within arbitrary and usually short, contingent timeframes. As Rothrock wrote in 1994, the information-led battle '*will not happen quickly … it will probably be years to decades …* (and for) *employment in long-term campaigns such as the 'war of ideas''*.[26] How, therefore, are decisive conditions and supporting effects to be measured and assessed? If power is now intangible, how are centres of gravity derived? In addition, if progress is now indeterminable, how is culmination assessed and a rational calculus differentiated? In sum, how does a commander design a viable theory of military information and/or influence-led change, and then command and control its delivery?

Here, then, is the third and final element of the paradox of information-led conflict. Informational power may generate advantage, and thus *Influence* may be the most apposite high-level conceptualisation of military output. However, both will challenge the current principles of strategy development and operational-level C2. Moreover, until addressed, they will leave military decision makers playing a new game with old rules or fighting tomorrow's battles with yesterday's concepts.

Conclusion

This paper suggests there is a widening gap between the concepts used to think about warfare today and the capability to actually practice it tomorrow. It further posits that this gap particularly effects C2 and military decision making. As evidence, it identifies an emerging paradox at the centre of the current focus on the ability of information and Influence to generate advantage and win.

This paradox has three components. First that the technologies used to become 'first with the truth' also enable the 'distributed trust' which makes it less likely to be believed. Second, and similarly, that by disseminating information the power of it declines, and with it the ability to gain the control being sought. Indeed, and as the Fallujah example suggests, informational power tends as much to chaos (in the form of counter-narratives) as control. Third, and somewhat more prosaically, regarding information as power challenges the current building blocks of operational planning and strategy. End states are diffuse, timescales potentially endless and geographical boundaries no longer relevant. Consequently, previously tangible planning tools such as centres of gravity, decisive conditions and supporting effects become increasingly difficult to define, if not potentially obsolete.

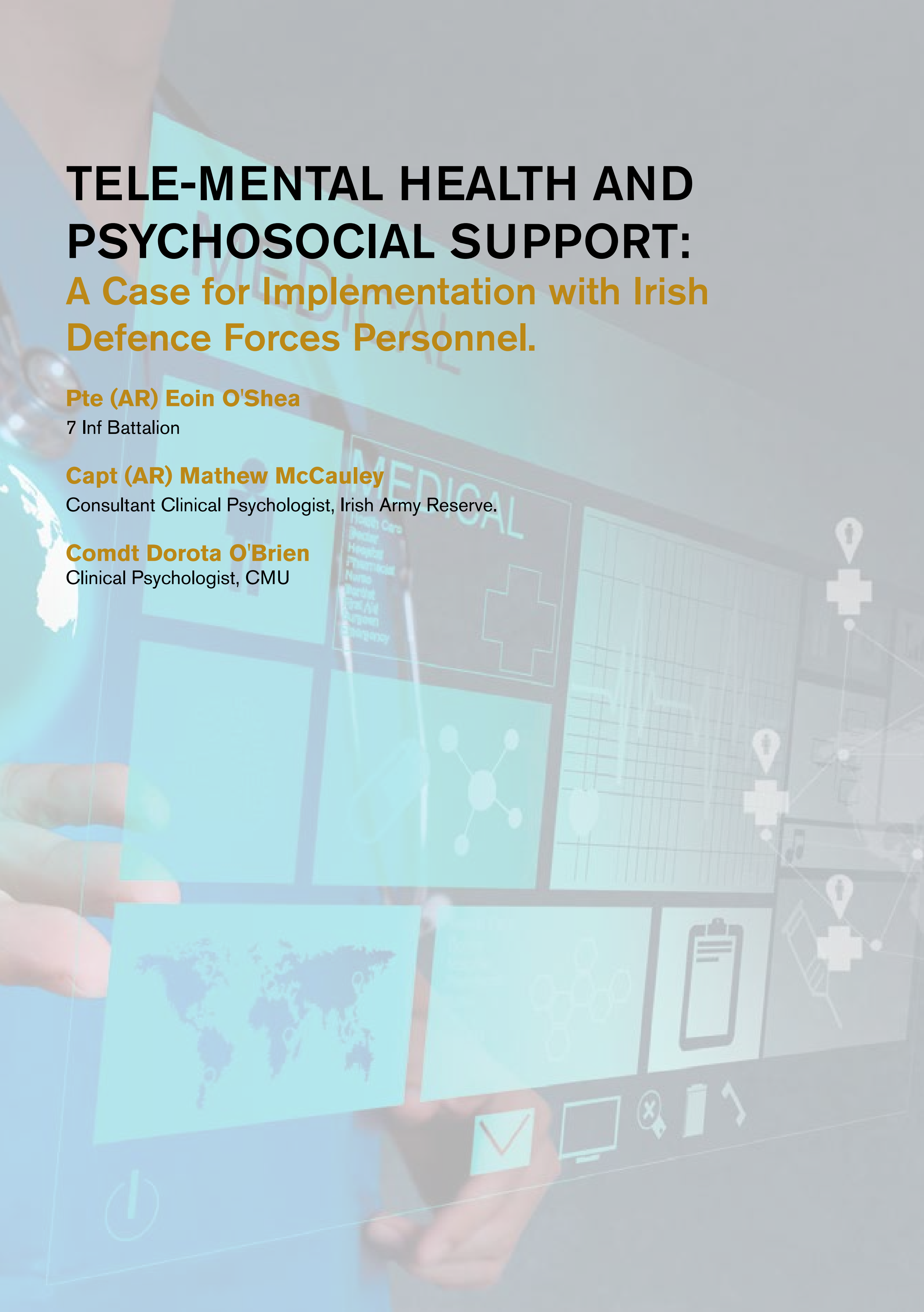
Nevertheless, the military utility of information is clearly undergoing a renaissance. However, whether it can be usefully conceptualised as a unique source of power has yet to be established. Arguably, information in the form of a coherent narrative has the power to deny, at least in political terms, the otherwise battle-winning capability of a more advanced adversary.

[26] John Rothrock, "Information Warfare: Time for Some Constructive Scepticism", ed John Arquilla and David Ronsfeldt (Santa Monica: Rand 1997) 219.

This, though, is not quite the same as being able to win or deliver victory. What this will mean for traditional warfighting practices such as operational-level planning, campaign assessment and C2 has yet to fully emerge. Nevertheless, that it will change them is beyond doubt. In the interim, today’s commanders, despite being invited to do so, will find it challenging to be ‘first with the truth’. They may be first with their truth, but in the information age, this will not be enough.

So, to return to the beginning, the 2015 (Irish) Defence White Paper and the IDF’s history of involvement in peacekeeping operations. The former offers a list of the tasks most closely associated with this honourable tradition, including: ‘peace enforcement, peacekeeping, disarmament, truce supervision, and/or observation, military training and education, international humanitarian law and human rights law missions’.[27] All of which involve the maintenance of control by a trusted agent of the UN or some other similar institution. Predominantly via the use of normative influence or messaging activity. However, as this paper suggests, such trust is declining, and with it, the value of the ‘story’ – not the army – that will deliver an information age ‘win’. It is arguable; therefore, that the paradoxical nature of information-led conflict will pose a proportionately greater challenge to those – such as the IDF - whose mission is to interpose, than those – such as the UK armed forces - who mission is to defeat.

[27] Irish Government, Op Cit, 32.



TELE-MENTAL HEALTH AND PSYCHOSOCIAL SUPPORT: A Case for Implementation with Irish Defence Forces Personnel.

Pte (AR) Eoin O'Shea
7 Inf Battalion

Capt (AR) Mathew McCauley
Consultant Clinical Psychologist, Irish Army Reserve.

Comdt Dorota O'Brien
Clinical Psychologist, CMU

Abstract

This article investigates the utility and efficacy of Tele-Mental Health (TMH) in the context of enhancing military mental health services and operational psychosocial support structures. This involves a review of research concerning the effectiveness of TMH in military populations. Papers reviewed included those published since 2010 that report empirically observed benefits on numerous outcomes, which relate to mental health and wellbeing; whilst also focusing on those that include technologies and processes of viable application in moderately sized military organisations such as Ireland's Defence Forces (DF). Results are presented in terms of modality or format (e.g. audio-visual platform, email, online support groups) and demonstrated effectiveness for service recipients. The article considers a potential service provision model deliverable through both the DF's Medical Corps as well as its Personnel Support Service (PSS). Distinctions between both the DF Medical Corps mental health capability and the wellbeing support provided by the PSS in this regard are explored, recognising the differences in remit between both entities.

Introduction

TMH has received considerable interest and support through international research. TMH broadly refers to any form of mental health and wellbeing support provided over distance through technological means; common examples include audio-visual interfaces (e.g. Skype, Defence Forces Intranet) for assessment and treatment consultations, online support groups, psychoeducational informational resources, and email support.[1] More specifically, the application of TMH in assisting military personnel and their families has been demonstrated to represent an effective and viable option in mental health and wellbeing service provision.[2][3] TMH may address barriers to effective care for these populations related to accessibility, cost-effectiveness, and provision of more specialist medical corps interventions (e.g. clinical psychologist, psychiatrist) for those serving on operational deployments overseas or at home.

Military Mental Health & Psychosocial Support

Current research concerning the mental health of military populations suggests a range of factors that may place such personnel at an elevated risk of problem development during and following operational service.[4][5] Much of the English-speaking studies since 2010 have referred to both the U.S. and U.K. operations in Iraq (i.e. Operation Iraqi Freedom/OIF; Op Telic) and Afghanistan (i.e. Operation Enduring Freedom/OEF; Op Herrick). Caution must therefore be advised in generalising such findings to those serving in United Nations

[1] Barak, A., L. Hen, M. Boniel-Nissim, and N. Shapira. "A comprehensive review and a meta-analysis of the effectiveness of Internet-based psychotherapeutic interventions. National Library of Medicine. PubMed Health. 2008 [cited 2015 Sep 26]." (2016).

[2] Luxton, David D., Larry D. Pruitt, Amy Wagner, Derek J. Smolenski, Michael A. Jenkins-Guarnieri, and Gregory Gahm. "Home-based telebehavioral health for US military personnel and veterans with depression: A randomized controlled trial." *Journal of Consulting and Clinical Psychology* 84, no. 11 (2016): 923.

[3] Bounthavong, Mark, Larry D. Pruitt, Derek J. Smolenski, Gregory A. Gahm, Aasthaa Bansal, and Ryan N. Hansen. "Economic evaluation of home-based telebehavioural health care compared to in-person treatment delivery for depression." *Journal of telemedicine and telecare* 24, no. 2 (2018): 84-92.

[4] Vogt, Dawne. "Mental health-related beliefs as a barrier to service use for military personnel and veterans: a review." *Psychiatric services* 62, no. 2 (2011): 135-142.

[5] Vaughan, Christine A., Terry L. Schell, Terri Tanielian, Lisa H. Jaycox, and Grant N. Marshall. "Prevalence of mental health problems among Iraq and Afghanistan veterans who have and have not received VA services." *Psychiatric Services* 65, no. 6 (2014): 833-835.

(U.N.) operations (e.g. peace-keeping, peace-enforcement, humanitarian relief), the likes of which represent greater relevance to Ireland's DF personnel. As examples of such elevated risk among the personnel of countries that have engaged in expeditionary war fighting, a U.K. study[6] found, among U.K. Iraq- and Afghanistan-deployed personnel, a prevalence of 6.2% for probable Post-Traumatic Stress Disorder (PTSD), 21.9% for common mental disorders (i.e. anxiety and depression), and 10.0% for alcohol misuse. These figures might be compared with equivalent analyses of prevalence among the U.K. general population, such as a study by the Mental Health Foundation [7] that places rates of PTSD and common mental disorders (i.e. depression and anxiety) at 4.4%, and 17% respectively. Similarly, a large meta-analytic study[8] on British military personnel (N=21,746) found that, despite rates of detectable PTSD and alcohol misuse not changing based on duration since deployment (i.e. over a 3-year period), psychological distress did. Such findings may underscore the importance of providing military mental health and wellbeing services across the deployment cycle.

Nevertheless, as it has been pointed out[9]: "the operational characteristics (and mental health consequences) [of U.N.-mandated peace-keeping missions] have similarities to those of humanitarian assistance, disaster relief and combat missions (p.3)". As of 2018, a total of 3,767 fatalities have occurred across all U.N. peace missions since 1948.[10] This has occurred within the common peace-keeping operational rules of engagement, which are found across such missions. Specifically, U.N. peace-keepers are prohibited from using force except in the defence of either the mandate and/or themselves.[11] Previous research concerning such U.N. personnel suggest a wide range of deleterious mental health outcomes including PTSD, depression, substance misuse, increased hostility, and suicide.[12] [13] [14] To date, there has been no research conducted concerning the prevalence of mental health disorders among Irish DF personnel.

Challenges exist in accurately assessing an exact prevalence of some mental disorders among such U.N. personnel, as exemplified by a study[15] of rates of PTSD among those serving on such missions. The authors' meta-analysis of previous work found decidedly heterogeneous results between studies, with rates of indicated PTSD ranging from 0.05% to 25.8%. Clearly, more research with standardised methods and timeframes of assessment is required in this regard. A 2010 study[16] more broadly examined distress, mental disorders, and suicide. It found some studies suggesting a higher incidence of problems correlating to greater levels of experienced

[6] Stevelink, Sharon AM, Margaret Jones, Lisa Hull, David Pernet, Shirlee MacCrimmon, Laura Goodwin, Deirdre MacManus et al. "Mental health outcomes at the end of the British involvement in the Iraq and Afghanistan conflicts: a cohort study." *The British Journal of Psychiatry* 213, no. 6 (2018): 690-697.

[7] Mental Health Foundation. "Fundamental Facts About Mental Health 2016", (2016): Mental Health Foundation: London.

[8] Rona, Roberto J., Howard Burdett, Samantha Bull, Margaret Jones, Norman Jones, Neil Greenberg, Simon Wessely, and Nicola T. Fear. "Prevalence of PTSD and other mental disorders in UK service personnel by time since end of deployment: a meta-analysis." *BMC psychiatry* 16, no. 1 (2016): 333.

[9] Shigemura, Jun, Masanori Nagamine, Nahoko Harada, Masaaki Tanichi, Kunio Shimizu, and Aihide Yoshino. "Peacekeepers deserve more mental health research and care." *BJPsych open* 2, no. 2 (2016): e3-e4. 3.

[10] United Nations. *"UN Peacekeeping Operations Fact Sheet: 31 August 2018."* UN, 2015. Accessed June 15, 2019. http://www.un.org/en/peacekeeping/documents/bnote1015.pdf.

[11] Sareen, Jitender, Brian J. Cox, Tracie O. Afifi, Murray B. Stein, Shay-Lee Belik, Graham Meadows, and Gordon JG Asmundson. "Combat and peacekeeping operations in relation to prevalence of mental disorders and perceived need for mental health care: findings from a large representative sample of military personnel." *Archives of general psychiatry* 64, no. 7 (2007): 843-852.

[12] Shigemura, Jun, and Soichiro Nomura. "Mental health issues of peacekeeping workers." *Psychiatry and Clinical Neurosciences* 56, no. 5 (2002): 483-491.

[13] Souza, Wanderson Fernandes, Ivan Figueira, Mauro V. Mendlowicz, Eliane Volchan, Carla Marques Portella, Ana Carolina Ferraz Mendonça-de-Souza, and Evandro Silva Freire Coutinho. "Posttraumatic stress disorder in peacekeepers: a meta-analysis." T*he Journal of nervous and mental disease* 199, no. 5 (2011): 309-312.

[14] Sareen, Jitender, Murray B. Stein, Siri Thoresen, Shay-Lee Belik, Mark Zamorski, and Gordon JG Asmundson. "Is peacekeeping peaceful? A systematic review." The Canadian Journal of Psychiatry 55, no. 7 (2010): 464-472.

[15] Souza, Op Cit, 310.

[16] Sareen, Op Cit, 468.

combat. Importantly, the same authors noted that: "Perceived meaningfulness of the mission, post-deployment social supports, and positive perception of homecoming were associated with lower likelihood of distress (p.464)" and may therefore be regarded as protective factors.

In the Irish military context, the relevance of a timely and effectively supportive response from the DF's Medical Corps and PSS are of clear and likely value in relation to such findings. In a more recent example of mental health morbidity among Australian peace-keepers[17], 12-month prevalence of numerous mental disorders among personnel were of particular note, namely: PTSD (16.8%), depression (7%), generalised anxiety disorder (4.7%), alcohol misuse (12%), alcohol dependence (11.3%) and suicidal ideation (10.7%). Such findings reflect a higher prevalence than that found among civilians and the presence of these mental health conditions was most strongly and consistently associated with exposure to potentially traumatic experiences (PTEs). These issues are primarily addressed in the Irish DF via the operational resources delivered by the Medical Corps and the Personnel Support Service (PSS).

Mental Health Services in the Defence Forces

The provision of mental health services in the DF lies within the remits of both the Medical Corps and the PSS. Such provision includes primary and secondary healthcare in the context of an occupational health framework. It is delivered by mental health clinicians and additional trained personnel throughout the organisation.

The provision of mental healthcare within the Medical Corps operates via a multi-disciplinary team context. The clinical team consists of one Military Psychiatrist (currently a vacant post), a PDF Military Clinical Psychologist and a full-time Department of Defence (DOD) Clinical Psychologist, along with one RDF Military Clinical Psychologist. This clinical team is responsible for delivering occupational mental healthcare to all serving members of the DF. As outlined by two such psychologists[18], such professionals provide a full spectrum of clinical services that balance the needs of the patient with those of the organisation in achieving the DF's operational objectives. The Medical Corps' mental health personnel retain a focus on promoting mental health, preventing mental ill-health, detecting healthcare problems that may arise, and delivering direct clinical services. They support command at home and overseas, whilst functioning as subject matter experts and consultants to DF leadership across the organisation. Such priorities are mirrored in the military mental health systems of other nations.[19] [20]

The PSS services are delivered by a combination of professional social workers, as well as trained NCOs based at various barracks who function as Personnel Support Officers (PSOs). They provide preventative critical incident responses, peer support programmes, pastoral counselling, training of personnel tasked with the care and welfare of others, and informational talks/workshops on subjects such as suicide awareness and stress. In both online and in-person

[17] Forbes, David, Meaghan O'Donnell, Rachel M. Brand, Sam Korn, Mark Creamer, Alexander C. McFarlane, Malcolm R. Sim, Andrew B. Forbes, and Graeme Hawthorne. "The long-term mental health impact of peacekeeping: prevalence and predictors of psychiatric disorder." *BJPsych open* 2, no. 1 (2016): 32-37.
[18] McCauley, M., and D. O'Brien. "Military clinical psychology in the Irish defence forces." *The Irish Psychologist* 44 (2017): 10-15.
[19] Greenberg, Neil, and Norman Jones. "Optimizing mental health support in the military: The role of peers and leaders." (2011).
[20] McCauley, Mathew and Johno Breeze. "Dispatches from the editor: military psychology, a force multiplier." *Journal of the Royal Army Medical Corps* 165, no. 2 (2019): 63-64.

formats, personnel accessing these services can avail of signposting and referral to resources of relevance concerning matters such as bereavement, substance misuse, family issues, and relationships. A strong focus of the service is the support of families both during deployments and beyond. The PSS also has links with, and provides supports for, veterans.

Tele-Mental Health

A significant body of research now exists concerning the use of distance technologies for various forms of mental health and wellbeing-related information, assessment, and intervention. For example, in a large-scale review[21] of TMH trials, the authors conclude that research conducted up until 2003 suggests strong evidence for patient and provider satisfaction with a range of TMH services as well as evidence for the reliability of clinical assessments relative to face-to-face versions. They also noted more minimal evidence supporting its use in treating specific mental health disorders, limited additional benefits for specific populations, or comparable effectiveness for populations such as older adults, children, or those living in rural areas with lesser healthcare access. Encouragingly, research undertaken since then has utilised both better technology, as well as more sophisticated research designs, most notably a growing number of Randomised Controlled Trials (RCTs). According to one of the most recent RCTs conducted to date, "tele-mental health has demonstrated equivalent efficacy compared to face-to-face care in a variety of clinical settings and with specific patient populations". An updated review[22] is similarly positive, suggesting:

> *Telemental health is effective for diagnosis and assessment across many populations … and for disorders in many settings (e.g. emergency, home health) and appears to be comparable to in-person care. In addition, this review has identified new models of care (i.e., collaborative care, asynchronous, mobile) with equally positive outcomes… Telemental health is effective and increases access to care.*

Much of the reviewed research outlined above pertains to video-conferencing interaction, a format thought to maximise the amount of multi-sensory information otherwise lost to both clinician and patient during interaction. However, a large meta-analytic study[23] examined a comprehensive variety of different types of online formats (e.g. email, video-conferencing, psychoeducational materials, etc). The authors similarly conclude that: "A comparison between face-to-face and Internet intervention … revealed no differences in effectiveness. The findings of this meta-analysis… provide strong support for the adoption of online psychological interventions as a legitimate therapeutic activity" (p.109). Furthermore, a distinction seems to occur between a client's initial perception of, and confidence in, the acceptability of online versus in-person interaction once the client has actually experienced online service provision.[24] Findings concerning patient satisfaction, as well as therapeutic alliance, compare equivalently between both modalities.[25]

[21] Richardson, Lisa K., B. Christopher Frueh, Anouk L. Grubaugh, Leonard Egede, and Jon D. Elhai. "Current directions in videoconferencing telemental health research." *Clinical Psychology: Science and Practice* 16, no. 3 (2009): 323-338.

[22] Hilty, Donald M., Daphne C. Ferrer, Michelle Burke Parish, Barb Johnston, Edward J. Callahan, and Peter M. Yellowlees. "The effectiveness of telemental health: a 2013 review." *Telemedicine and e-Health* 19, no. 6 (2013): 444.

[23] Barak *et al.*, Op Cit 109.

[24] Gros, Daniel F, Cynthia Luethcke Lancaster, Cristina M López, and Ron Acierno. "Treatment Satisfaction of Home-Based Telehealth versus in-Person Delivery of Prolonged Exposure for Combat-Related PTSD in Veterans." *Journal of Telemedicine and Telecare* 24, no. 1 (January 2018): 51-55.

[25] Jenkins-Guarnieri, Michael A., Larry D. Pruitt, David D. Luxton, and Kristine Johnson. "Patient perceptions of telemental health: Systematic review of direct comparisons to in-person psychotherapeutic treatments." *Telemedicine and e-Health* 21, no. 8 (2015): 652-660.

Military Applications of Tele-Mental Health

Broadly speaking, findings to date concerning the use of TMH with military populations seem promising. Recent studies suggest positive comparisons with in-person interventions relating to both currently serving personnel,[26] as well as military veterans.[27] [28]

RCTs used to explore such comparisons have yielded positive results across multiple mental health disorders, including PTSD,[29] [30] depression,[31] and substance misuse.[32] Some studies have replicated such findings in group- and individually-based interventions, providing potential cost effectiveness improvements, as well as utilising group processes in therapy.[33] [34] At least one study[35] has demonstrated the effectiveness of TMH treatment 'in theatre' for Acute Stress Disorder (i.e. a clinical disorder diagnosed in the more immediate aftermath of a traumatic event).

Possible military-cultural treatment challenges, as well as strategies to address same, have been discussed elsewhere in detail[36] and may include personnel attitudes to mental health issues, unsupportive leadership, concerns about impacts on career (e.g. security clearances), and long-duty hours impeding consistent engagement in treatment. Decisions regarding the use of TMH should also be based on sound clinical judgment and characteristics of an individual's clinical presentation. For example, a study[37] has demonstrated that factors such as baseline severity of disorder, high anxiety and loneliness scores, and older age predicted less symptom improvement. The evidence reviewed above suggests a broad comparability between TMH for various disorders compared with in-person engagement. TMH may be effective for those in rural/remote settings, even for conditions as clinically severe as PTSD,[38] along with those experiencing mobility issues[39] and family members of personnel,[40] whilst such options for intervention may represent a more cost-effective method of service delivery under certain

[26] Pelton, Dan, Bethany Wangelin, and Peter Tuerk. "Utilizing telehealth to support treatment of acute stress disorder in a theater of war: Prolonged exposure via clinical videoconferencing." *Telemedicine and e-Health* 21, no. 5 (2015): 382-387.

[27] Gros, Daniel F., Matthew Yoder, Peter W. Tuerk, Brian E. Lozano, and Ron Acierno. "Exposure therapy for PTSD delivered to veterans via telehealth: Predictors of treatment completion and outcome and comparison to treatment delivered in person." *Behavior Therapy* 42, no. 2 (2011): 276-283.

[28] Turgoose, David, Rachel Ashwick, and Dominic Murphy. "Systematic review of lessons learned from delivering tele-therapy to veterans with post-traumatic stress disorder." *Journal of telemedicine and telecare* 24, no. 9 (2018): 575-585.

[29] Resick, Patricia A., Jennifer Schuster Wachen, Katherine A. Dondanville, Kristi E. Pruiksma, Jeffrey S. Yarvis, Alan L. Peterson, Jim Mintz et al. "Effect of group vs individual cognitive processing therapy in active-duty military seeking treatment for posttraumatic stress disorder: A randomized clinical trial." *JAMA psychiatry* 74, no. 1 (2017): 28-36.

[30] Gros *et al.*, Op Cit, 53.

[31] Luxton *et al.*, Op Cit, 923.

[32] Neighbors, Clayton, Melissa A. Lewis, David C. Atkins, Megan M. Jensen, Theresa Walter, Nicole Fossos, Christine M. Lee, and Mary E. Larimer. "Efficacy of web-based personalized normative feedback: a two-year randomized controlled trial." *Journal of consulting and clinical psychology* 78, no. 6 (2010): 898.

[33] Resick, Patricia A., Jennifer Schuster Wachen, Jim Mintz, Stacey Young-McCaughan, John D. Roache, Adam M. Borah, Elisa V. Borah et al. "A randomized clinical trial of group cognitive processing therapy compared with group present-centered therapy for PTSD among active duty military personnel." *Journal of Consulting and Clinical Psychology* 83, no. 6 (2015): 1058-1068.

[34] Steenkamp, Maria M., Brett T. Litz, Charles W. Hoge, and Charles R. Marmar. "Psychotherapy for military-related PTSD: a review of randomized clinical trials." *Jama* 314, no. 5 (2015): 489-500.

[35] Pelton *et al.*, Op Cit, 384.

[36] Hall-Clark, Brittany N., Edward C. Wright, Brooke A. Fina, Tabatha H. Blount, Wyatt R. Evans, Patricia K. Carreño, Alan L. Peterson, Edna B. Foa, and STRONG STAR Consortium. "Military culture considerations in Prolonged Exposure Therapy with active-duty military service members." *Cognitive and Behavioral Practice* 26, no. 2 (2019): 335-350.

[37] Smolenski, Derek J., Larry D. Pruitt, Simona Vuletic, David D. Luxton, and Gregory Gahm. "Unobserved heterogeneity in response to treatment for depression through videoconference." *Psychiatric rehabilitation journal* 40, no. 3 (2017): 303.

[38] Rosen, Craig S., Kathleen M. Chard, Patricia Resick, and B. Christopher Frueh. "Cognitive processing therapy for posttraumatic stress disorder delivered to rural veterans via telemental health: a randomized noninferiority clinical trial." J Clin Psychiatry 75, no. 5 (2014): 470-476.

[39] Price, Laura E., Paraskevi Noulas, Irina Wen, and Amanda Spray. "A portal to healing: Treating military families and veterans through telehealth." *Journal of clinical psychology* 75, no. 2 (2019): 271-281.

[40] Grady, Brian J., and Ted Melcer. "A retrospective evaluation of TeleMental Healthcare services for remote military populations." *Telemedicine Journal & E-Health* 11, no. 5 (2005): 551-558.

circumstances.[41] Furthermore, alterations in the process of communication may have some positive implications in the military sector, with at least one study suggesting superior outcomes for personnel and their families assigned to remote military locations.[42]

Future Developments

More research is required on the utility and efficacy of TMH for military personnel. Additional investigations are also necessary, prior to any implementation of TMH within the Irish DF. However, research reviewed in this paper suggests the potential utility of TMH and wellbeing supports through both the Medical Corps as well as PSS. Examples are provided hereafter and might fall under three broad categories, namely: (1) Broad informational and psychoeducational support; (2) 'In-theatre' specialist assessment and intervention; and (3) 'Home-based' treatment and care. Specific research examples concerning a range of potential applications are thereafter provided in Appendix A. These include studies of TMH applied to the treatment of PTSD[43] and other traumatic disorders[44], more common mental health difficulties[45], mental health screening[46], psychoeducation[47], and the support of military families[48].

Firstly, it seems entirely feasible to use distance-technologies to provide effective informational support[49] to a broad range of individuals in the context of the DF. In addition to information already provided by the PSS in this regard, further options could include more comprehensive psychoeducational and wellbeing-related information; these might be developed not only for currently serving personnel, but also families and veterans, as per the stated remit of the PSS. Brief online questionnaires, completely anonymised to ensure confidentiality and GDPR adherence, could be utilised in actively bringing to the attention of personnel a variety of services (both internal and external) of potential relevance, based on answers to specific questionnaire items. The same process could be used to export, possibly in the form of a 'personalised' report, psychoeducational, and other health-related materials concerning a broad range of subjects including stress management, diet, physical fitness, and relational/family support whilst serving overseas.

Secondly, existing Medical Corps mental health expertise could be utilised more promptly when required for personnel serving overseas. Psychological assessment, medication review, second opinion evaluations, direct therapeutic intervention, as well as consultation with an individual or unit's Chain of Command whilst overseas could be expedited through the use

[41] Bounthavong *et al.*, Op Cit, 86.
[42] Grady & Mercer, Op Cit, 555.
[43] Morland, Leslie A., Anna K. Hynes, Margaret- Anne Mackintosh, Patricia A. Resick, and Kathleen M. Chard. "Group cognitive processing therapy delivered to veterans via telehealth: A pilot cohort." *Journal of Traumatic Stress* 24, no. 4 (2011): 465-469.
[44] Pelton, Dan, Bethany Wangelin, and Peter Tuerk. "Utilizing telehealth to support treatment of acute stress disorder in a theater of war: Prolonged exposure via clinical videoconferencing." *Telemedicine and e-Health* 21, no. 5 (2015): 382-387.
[45] Luxton, David D., Larry D. Pruitt, Amy Wagner, Derek J. Smolenski, Michael A. Jenkins-Guarnieri, and Gregory Gahm. "Home-based telebehavioral health for US military personnel and veterans with depression: A randomized controlled trial." *Journal of consulting and clinical psychology* 84, no. 11 (2016): 923.
[46] Sadler, Anne G., Michelle A. Mengeling, James C. Torner, Jeffrey L. Smith, Carrie L. Franciscus, Holly J. Erschens, and Brenda M. Booth. "Feasibility and desirability of web- based mental health screening and individualized education for female OEF/OIF Reserve and National Guard war veterans." *Journal of traumatic stress* 26, no. 3 (2013): 401-404.
[47] Bush, Nigel E., Charles P. Bosmajian, Jonathan M. Fairall, Russell A. McCann, and Robert P. Ciulla. "afterdeployment. org: A web-based multimedia wellness resource for the postdeployment military community." *Professional Psychology: Research and Practice* 42, no. 6 (2011): 455.
[48] Gewirtz, Abigail H., Keri LM Pinna, Sheila K. Hanson, and Dustin Brockberg. "Promoting parenting to support reintegrating military families: After deployment, adaptive parenting tools." *Psychological services* 11, no. 1 (2014): 31.
[49] Barak *et al.*, Op Cit, 1.

of audio-visual technologies. In some research,[50] even conditions such as Acute Stress Disorder have successfully been treated in-theatre, and remotely. Similarly, this could facilitate mental health specialists to make decisions about the necessity of an individual returning to Ireland due to mental health concerns. Such a capability could help forego costly, disruptive, and potentially unnecessary removal of personnel from operational duties.

Finally, both the Medical Corps and PSS could provide their respective supports to personnel remotely in Ireland. In support terms, there is a Barrack Personnel Support Service Officer and 16 chaplains available to personnel across every DF barracks. However, resources involving in-person provision of clinical psychological assessment and evidence-supported treatment by the Medical Corps, as well as personal counselling and pastoral support (PSS), are limited to only a few locations across the country. Therefore, the increased use, and evaluation of, TMH through both the Medical Corps and PSS seems worthy of further investigation. Through judicious ethical and professional considerations[51] [52], coupled with a minimal investment in the technological and practical resources required, numerous mental wellbeing supports could be offered to personnel based at smaller military installations; or even in their own homes under certain circumstances. Finally, the PSS support provided to families of currently serving personnel, as well as veterans, could likely be enhanced through such means.

Conclusion

This paper has sought to review evidence concerning relevant studies of military mental health, the effectiveness of TMH generally, and its use with military populations to date. The authors have concluded with a brief description of a variety of ways in which TMH might benefit the mental health and wellbeing of DF personnel, citing specific examples of research supporting same. Though the current paper addresses such possibilities largely in relation to currently serving personnel, similar applications may prove just as feasible for both families and our country's veterans. Based on such evidence, it is proposed that TMH supports be further researched for future use by the DF, with due regard afforded to important issues concerning safe implementation, technological requirements and the feasibility, confidentiality, and user experience of the technologies involved.

[50] Pelton *et al.*, Op Cit, 386.

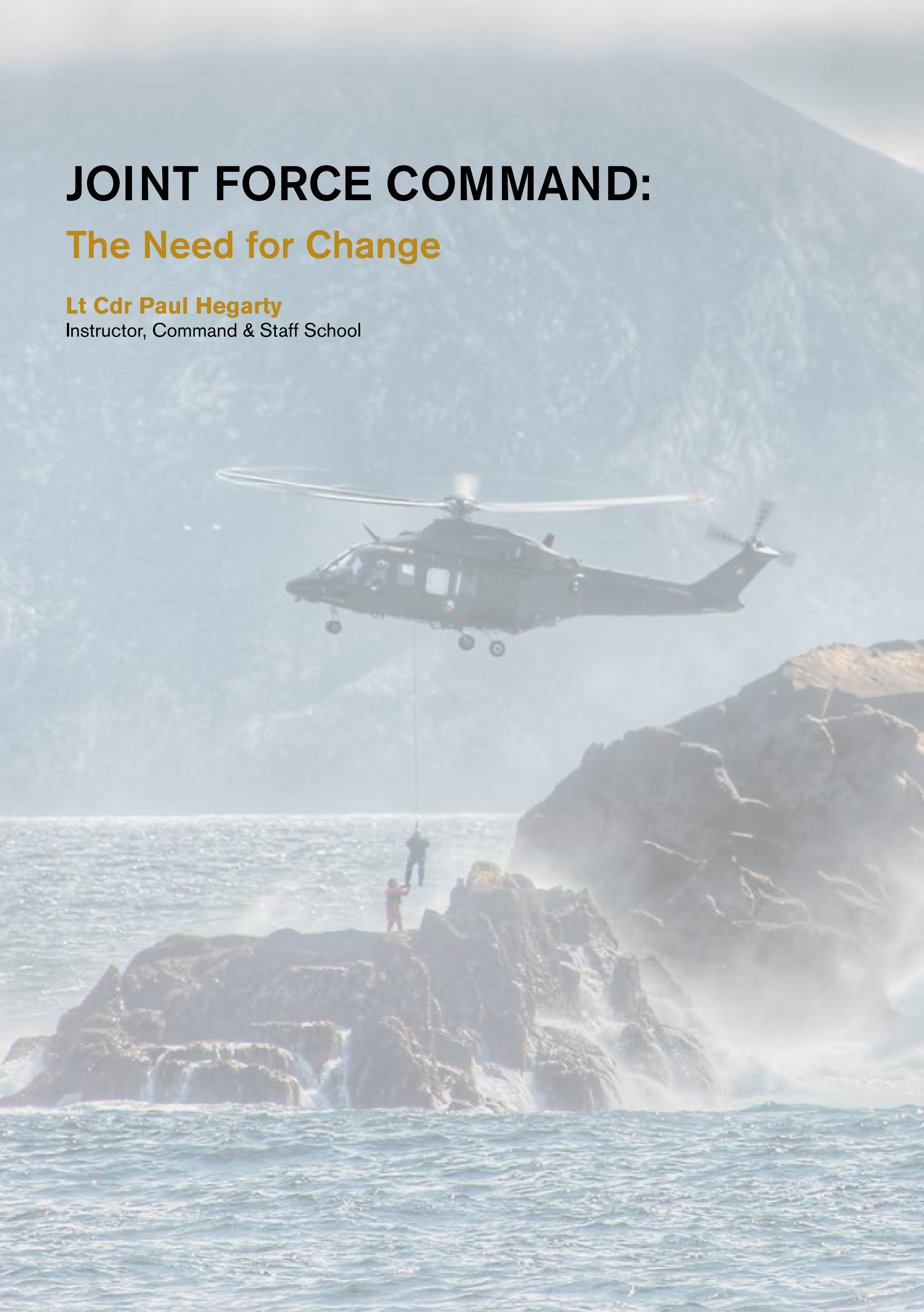
[51] Anthony, Kate, DeeAnna Merz Nagel, and Stephen Goss, eds. T*he use of technology in mental health: Applications, ethics and practice.* Springfield, IL: Charles C. Thomas Publishers, 2010.

[52] Luxton, David D., Anton P. Sirotin, and Matthew C. Mishkind. "Safety of telemental healthcare delivered to clinically unsupervised settings: A systematic review." *Telemedicine and e-Health* 16, no. 6 (2010): 705-711.

JOINT FORCE COMMAND:

The Need for Change

Lt Cdr Paul Hegarty
Instructor, Command & Staff School



Abstract

This paper examines the current structure of the Irish Defence Forces and seeks to establish if its structure remains suitable in today's operating environment. The paper uses a combination of previous international experience and associated transformations as a means of exploring if the application of a joint force command structure would benefit the Irish Defence Forces. By presenting both historic and current experiences through the use of literature and previous research, the paper seeks to evaluate the benefits associated with moving away from a single Service orientated construct and adopting a joint force command structure. In this regard, it must be remembered that unlike other international militaries, the Defence Forces has not evolved from its historic land-centric structure.

The paper additionally explains the need for a future joint force concept that looks out to 2035-2040 and examines its relevance for the Defence Forces. An objective of this concept is the idea that joint action, and therefore influence can be enhanced through exploiting information, being more integrated as a force and being more adaptable. The joint approach is in operation elsewhere and the consensus there is that this approach is both inevitable and necessary. In no case where it has been applied, particularly in the last 10 years, have there been moves to reverse course. The paper concludes by presenting the argument for the necessary paradigm shift towards a Defence Forces joint force command structure.

Introduction

> *"Separate ground, sea and air warfare is gone forever. If we ever again should be involved in war, we will fight with all elements, with all Services, as one single concentrated effort".*[1]

Reflecting on General Eisenhower's observations, particularly as Europe celebrates the 75th anniversary of D-Day, this paper contends that the lessons of World War 2 and subsequent developments in military force structure have not been absorbed by the Irish Defence Forces (DF) and further posits that the DF is in urgent need of a modernisation process in order to prepare it for both current and future operations, both at home and overseas.

The concept of 'jointery' has been developed within the literature on modern military organisations over the last number of decades.[2] While its role has traditionally focussed on the three domains of land, air and sea, and their associated military connotations, contemporary military operations have demonstrated that jointery should additionally include the 'integrated approach'.[3] Figure 1 highlights the five domains, which now exist within contemporary military operations and additionally emphasises the need for military organisations to have the capability to achieve and maintain influence in all domains.

[1] General Dwight D Eisenhower, 'memorandum to Admiral Chester W Nimitz', 17 April 1946. Quoted in Griffin, Stuart. Joint Operations: a short History, Produced by Training Specialist Services, HQ, p.7.

[2] Sullivan, Brian R. "The future nature of conflict: A critique of "the American revolution in military affairs" in the era of jointery." Defense Analysis 14, no. 2 (1998): 91-100.

[3] Military and civilian organisations working together as on unified organisation.

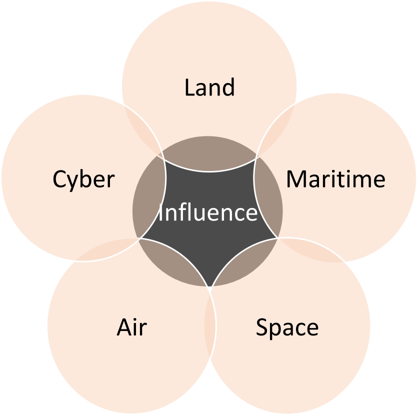


Figure 1 –Joint Operations and Influence[4]

Implicit within this acknowledgement is the necessity for commanders and their staffs to conceive and prepare operations with regard to the "strengths, weaknesses, capabilities and limitations of all Services" involved, and this is primarily the essence of joint operations.[5] Moreover, contemporary military operations are conducted in an expeditionary context due to the strategic requirement to 'project power', therefore, jointery becomes more of a necessity in order to achieve this objective.[6] It is therefore, inferred that a military organisation must be structured to reflect the way in which it fights and this requires a joint approach, both structurally and culturally.

In 2015, the Irish Department of Defence published its second White Paper on Defence, (WP2015), and sought to encapsulate a modernisation programme that would ensure the DF was capable of providing "an organisation that would be prepared to deliver a flexible and adaptive response to any adverse changes in a dynamic security environment".[7] Within WP2015, there was an acknowledgement that the DF would need to be capable of working jointly in order to achieve this government policy objective[8], however, the ability to operate jointly has historically never been pursued by the DF.

Internationally, jointery is considered a routine modus operandi and is progressively replacing single service methodologies towards joint military operations. It can, therefore, be proposed that jointery has become "as much a state of mind as a method of prosecuting war".[9] Modern operations will be complex and unconventional, and flexibility will be key to coming to terms with this vague future and joint capabilities are universally accepted as being central to this.[10]

[4] Development, Concepts and Doctrine Centre. JCN 1/17 – Future Force Concept. Shrivenham: Forms and Publications Centre, 2017, 19.
[5] B.A. Wood, "Joint Operations: An Essential Aspect of Today's Armed Forces." *Australian Defence Journal* (1999): 19-24.
[6] Andrew Dorman, Dr Mike Smith and Dr Matthew Uttley, "Jointery and Combined Operations in an Expeditionary Era: Defining the Issues", Defence Analysis, 14, no. 1 (1998): 5. Doi: 1080/07430179808405745.
[7] Department of Defence, White Paper on Defence 2015 (Dublin, 2015) 5.
[8] Ibid., 62.
[9] Griffin, Joint operations, 7.
[10] Ibid., 23.

Why Joint, why now?

Prior to critically examining the model of joint forces command and the DF's current position with respect to this concept, it is important to define the term 'jointery".[11] There are many different definitions of jointery and the NATO definition of joint is "an operation carried out by forces of two or more NATO nations, in which elements of more than one Service participate"[12]. The DF define joint as 'the ability to operate jointly – that is to bring elements of the army, air corps and naval service together to deliver effects in operations in a coordinated and cohesive manner"[13]. Research of DF operations demonstrates, that while the DF do complete joint exercises at the tactical level (Air Corps providing support to Army units during MRET[14] periods, etc.), at the operational and strategic level, there is limited understanding as to how this is to be achieved, as tri-service joint operations are not supported doctrinally or routinely exercised, particularly at the component or strategic levels.

For the purpose of this paper, the following discussions regarding 'jointery' will focus on the permanent physical constructs such as force structures, rather than those joint task force elements that are created temporarily for the purpose of single operations. To ensure a common definition is established for this permanent force construct, this paper will additionally focus on the Joint Force Command concept, which is defined as "a general term applied to a commander authorised to exercise operational command or control over a Joint force structure"[15].

The concept of jointery and the Joint Force Command is seen by many as a threat to the culture and identity of the single Service entities. The application of increased jointery has the potential to create heightened levels of apprehension within the various single Services, as the initial default position is to protect the single Services unique culture, ethos, values and traditions.[16] Whilst this protectionism is natural, there must be cognisance that tradition, habit and jealousies will always remain between military organisations, irrespective of whether it is Service versus joint structure, Service versus Service or joint structure versus joint structure.[17] The obstacles to change and transformation will innately remain, and failure to accept this will inevitably lead to additional issues being created. The critical requirement is that each Service has the ability to specialise within its own domain and in addition, has the competence and capability to deliver an effective presence within the other domains.[18]

Since World War II, the addition of sea power and air power has had a consequential impact on the faith of jointery and its application. Irrespective of how compelling the integration of forces may be, joint operations compounds the problems of assembling the forces for today and transforming them for the challenges of tomorrow.[19] It is necessary, therefore, to acknowledge, "no one service bears sole responsibility for military operations in any one domain."[20] Colin Gray further supports this observation and highlights that an exclusive strategic orientation,

[11] For the purposes of this paper, jointery and jointness are taken to have the same meaning.

[12] NATO, APP-6 (2015). NATO Glossary of terms in English and French, 2-A-12.

[13] Defence Forces, *Defence Forces Capstone Document* (Dublin, 2016) unpublished, 6-10.

[14] MRET refers to Mission Readiness and Evaluation Training and is carried out by units prior to deploying overseas.

[15] Development, Concepts and Doctrine Centre. *UK Joint Operations Doctrine*, 5th ed. Shrivenham: Forms and Publications Centre, 2014, 123.

[16] Michael Codner, The Strategic defence review: How much? How Far? How joint is Enough?" p.6.

[17] David C. Gompert, "Preparing Military Forces for Integrated Operations in the Face of Uncertainty" Santa Monica, CA: RAND Corporation, 2003. 1. Access 10 March 2018. https://www.rand.org/pubs/issue_papers/IP250.html.

[18] James Jay Carafano "America's Joint Force and the Domains of Warfare" The Heritage Foundation. p.23, accessed 21 April 2018, https://www.heritage.org/military-strength/americas-joint-force-and-the-domains-warfare.

[19] Gompert, "Preparing Military Forces for Integrated Operations in the Face of Uncertainty," 2.

[20] Carafano, "America's Joint Force and the Domains of Warfare," 24.

which places too much emphasis on military strength, geared for a specific geography, be it land, sea or air, can prove woefully vulnerable if strategic history takes an unanticipated course.[21] To prepare for the operations of the future there is a need to modernise and transform towards the long-term future and not just the near-term. Military forces continuously deal with uncertainty and this permeates the current security environment and the 'fog of war' will inevitably transcend our view of how the operational environment will evolve both in the medium to long- term.[22]

In an attempt to provide context to the application of Joint Forces Command (JFC), the following section will introduce two international experiences of transformation towards a JFC and presents a synopsis of research already conducted by the author.[23] The first review will be that of the Royal New Zealand Defence Forces (NZDF) and the second will be of the Royal Canadian Armed Forces (CAF). The NZDF was selected as it is comparable in size to the DF, shares a similar mind-set and has a similar operating profile. The Canadian experience of JFC is perceived internationally as an example of how not to implement a joint approach and remains viewed as a "bold move, one that none of Canada's allies has yet replicated."[24]

International Experience of the JFC Concept

In 1989, the NZDF conducted and implemented an initial Defence Resource Management Review and the changes wrought by this review resulted in the "abolition of the Security Council, the separation of policy from operations, and to have the Ministry of Defence responsible for the former, and the NZDF responsible for the latter."[25] This review was not a success and the inadequacies of the implemented structure was exposed by Jane's Defence Weekly:

> *"The resulting structure rather than separating operations from policy, as was the intention, has left both institutions without the resources to fully carry out their respective functions, while at the same time providing two conflicting streams to the government."*[26]

The contagion of the internal issues, which hindered command and control through the existence of silo's and inefficiencies, lead to the NZ Government to seek a new review that was tasked with reviewing the accountabilities and structural arrangements between the NZ MoD, the NZDF and each of the three single Services.[27] The Hunn Report was published in 2002 and recommended widespread changes for the NZDF, and based much of its recommendations on the central argument that the "two arms be re-established as a single organisation, as neither of these organisations had been functioning effectively and that the NZDF had been riven with internal dissention."[28]

The NZDF established its Joint Forces Headquarters in 2002 and the NZ Government sought to institutionalize a greater degree of 'jointness' not only "within the NZDF but also between

[21] Colin S. Gray, *The Future of Strategy* (Cambridge: Polity Press, 2017): 95.
[22] Gompert, "Preparing Military Forces for Integrated Operations in the Face of Uncertainty," 4.
[23] P Hegarty, "Joint Forces Command: The Irish Defence Forces 'horse and tank' moment?" *Defence Research Paper.* Joint Services Command and Staff College, Shrivenham, UK. (2018)
[24] Geoffrey Shaw, "The Canadian Armed Forces and Unification" *Defense Analysis*, Vol 17, no. 2, (2001): 161. doi: 10.1080/0743017012420.
[25] Hon. D.F. Quigley, New Zealand Defence, Resource Management Review 1988, (Strategic Consulting Limited, 1991). 12.
[26] Philip McKinnon, "New Zealand reviews Defence Structure", *Jane's Defence Weekly*, 26 September 2001, p.10.
[27] Greener, Peter. *Timing is Everything: the Politics and Processes of New Zealand Defence Acquisition Decision Making,* (Canberra: ANU E Press, 2009), 73.
[28] Hunn, Don, K. *Review of Accountabilities and Structural Arrangements between the Ministry of Defence and the New Zealand Defence Force*, Wellington, 30 September 2002, p.vi.

the NZDF and the NZ Ministry of Defence."[29] A variety of measures were introduced to give effect to this, including a public statement of intent by the NZ Government that set out a joint approach as the new standard to be used in the NZDF.[30] The primary command and control and structural arrangements as outlined in the Hunn Report were adopted and the Commander of Joint Forces New Zealand (COMJFNZ) leads JFC and this includes all "deployable NZDF Force Elements."[31] In addition COMJFNZ is responsible for the command and control of all joint and/or combined (international) operations and exercises. This includes the requirement of the three single Service chiefs to maintain the capability of "raising, training and maintaining their own Services and bringing assigned forces to their Directed Level of Capability (DLOC)."[32]

In order to ensure that the Single Services were capable of operating and delivering at the joint operational level, internal changes were also initiated in many of the various command and control and training functions. These changes included: "the Joint Forces Headquarters; a joint staff college; a joint appointment process for senior staff requiring clearances by all three Service chiefs; information technology centralisation and standardisation; and development of a joint non-operational logistic and support organisation."[33]

Furthermore, to achieve greater jointness and cooperation at the civilian-military level, a new approach to allocating responsibility and accountability was implemented. The result of these measures ensured that greater clarity was provided as to who was responsible for advising Government on military matters, thus serving to underpin the Government's defence outcomes. Finally, all command and control accountability was assigned to the Chief of Defence Staff (CDS)[34] and the Secretary of Defence on a similar but shared basis.[35]

The NZDF White Paper on Defence 2016 elaborated on the successes the previous reforms have obtained and highlighted additional areas of organisational change that will occur as the NZDF progresses towards an Integrated Defence Force by 2035.[36] A revised corporate structure now exists and additional joint functions have been added: Chief of Defence Strategy and Governance, Chief Joint Defence Services and Chief People Officer, to ensure that a more holistic view is being taken towards defence, as demonstrated in Figure 2.

[29] NZMOD, *Improving Joint Effectiveness in Defence,* (Wellington, 2002), 1.

[30] A Modern, Sustainable Defence Force Matched to New Zealand's Needs', 2001

[31] NZDF, Headquarters NZDF, (accessed 05 March 2018), http://www.nzdf.mil.nz/about-us/hqjfnz/default.htm.

[32] NZMOD, *Improving Joint Effectiveness in Defence*, 2.

[33] Ibid., 2.

[34] Chief of Defence Staff (CDS) and Chief of Defence (CHOD) both refer to the individual in command of their respective organisation. Each country uses its own version of the term.

[35] NZDF, *White Paper on Defence 2010*, (Wellington, 2010), 13.

[36] NZDF Future35, Our Strategy to 2035, (Wellington, 2015), 65.

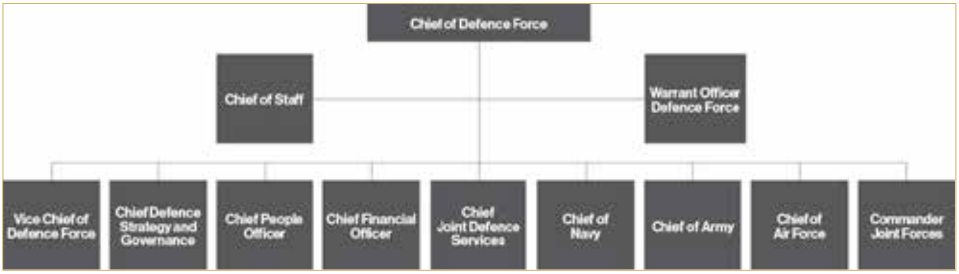


Figure 2 – NZDF Command and Control Organisation

The following section will review the transition of the Royal Canadian Armed Forces (CAF). The Canadian Armed Forces (CAF) initiated a unification process under the Canadian White Paper on Defence in 1964 and sought to unify all three single Services under one single Defence Force.[37] The primary function of the strategy witnessed the loss in the legal status of the single Services and legitimised the new organisation, which was termed the 'Canadian Forces (CF)'. The core objectives for pursuing this amalgamation was to create a force that was more efficient and effective, to reduce operating costs and to create a common identity and encourage a higher level of loyalty than that which is given to a single Service.[38] By creating a new organisational culture it was envisaged that the new force would rescind any previous loyalty to the previous regimental system and that the induction of a new singular uniform, "free of any historical distinguishing markings" would encourage acceptance of the new single Service.[39]

Due to the significant change inflicted on the organisation there was a significant level of opposition against the reorganisation and a high level of high-ranking officers and personnel resigned from the CF and significant amounts of experience and knowledge were lost. Frustration was directed at the perceived "cost saving initiative", many considered the reorganisation to be regressive and it took decades for the Canadian Forces to fully realise and attempt to repair the damage that had been inflicted.[40] To make matters worse, defence policy in Canada over those years seldom originated from a strategic idea, "a notion Hellyer had attempted to introduce in 1964, but, rather, it evolved from the dynamics of the annual federal budget."[41] Without a national defence strategy or a coherent unified defence policy, the maintenance of defence revolved around the maintenance of a balanced force, however this focussed on maintaining certain minimal operational capabilities within each Service, a system that sustained the Service orientated approach to defence planning and force development.[42] The arrival of General Rick Hillier as CDS in 2005 provided a much-needed catalyst:

[37] Paul Hellyer and Lucien Cardin. "White Paper on Defence." (Canadian Government paper on the restructuring of Defence, (March 1964), 158.
[38] Paul Hellyer and Lucien Cardin. "White Paper on Defence.", 164.
[39] Ibid., 160
[40] Ibid., 160.
[41] Bland, Douglas. "Chiefs of defence: Government and the united command of the Canadian armed forces." *Canadian Defence Quarterly* 25, no. 3 (1996): 158.
[42] Ibid., 268-72.

> *"Canadian Forces identity – Our first loyalty is to Canada. Beyond this fundamental imperative, all Service personnel must look past environment, component or unit affiliations to most closely identify with the Canadian Forces. The greater good of Canada and the Canadian Forces will, in every instance, take precedence over considerations of Service, component or unit affiliation."*[43]

In order to regain the initiative, organisational changes were required within the CF and these focussed on three key areas; the CDS assumed control of the force development by establishing a Chief of Force Development to focus on the now CAF transformation; creation of a Military Personnel Command, responsible to the CDS; and, the dismantling of the Deputy Chief of Defence Staff (DCDS) group and the establishment of a strong unified Strategic Joint Staff (SJS) which reported to the CDS.[44] The impact of the Strategic Joint Staff (SJS) was positive and improved the organisation's ability to make decisions at the operational level, thus improving military influence.

In 2009, there was recognition of the complexity facing Canada as the importance of its geostrategic location had created cumbersome solutions and the organisational structure had to be reformed.[45] The new structure comprises of four components, army, air force, navy and Special Forces that generate highly specialised capabilities and combat forces. From a command perspective; "CAF has one functional command that groups common national support functions and capabilities (CANOSCOM), two operational commands that employ CAF assets for the conduct of operations (Canada Command and CEFCOM), and a unified chain of command with a dedicated unified joint staff at the military strategic-political-diplomatic interface that helps the CDS to command the CAF, to carry out his national command responsibilities, and to advise the government."[46] Finally, in 2012 the CAF conducted a further modernisation programme and established the Canadian Joint Operations Command (CJOC) and merged the Canada Command, the Canadian Expeditionary Force Command and the Canadian Operational Support Command. CJOC's role is to "anticipate and conduct Canadian Forces operations, and develop, generate and integrate joint force capabilities for operations."[47] In addition Canada also created a Directorate for Cybernetics, and that works with Commander CJOC and Figure 3 presents a holistic overview of this new structure, based on all changes that have taken place in the previous decade.

[43] CDS Transformation Principle One, General Rick Hillier, CDS, *The Maple Leaf*, "CF Transformation: From Mission to Vision," Vol. 8, No. 36, (2005) p. 7.

[44] Major-General Daniel Gosselin Hellyer's Ghosts: Unification of the Canadian Forces is 40 years old – Part 1. (accessed on 20 April 2018) http://www.journal.forces.gc.ca/vo9/no2/03-gosselin-eng.asp.

[45] Jeff Tasseron, "Facts and Invariants: The Changing Context of Canadian Defence Policy," *Canadian Military Journal*, Vol. 4, No. 2, (2003), 23.

[46] Major-General Daniel Gosselin Hellyer's Ghosts: Unification of the Canadian Forces is 40 years old – Part 2. (accessed on 20 April 2018) http://www.journal.forces.gc.ca/vo9/no2/03-gosselin-eng.asp.

[47] National Defence and the Canadian Armed Forces, CJOC, (accessed on 01 May 2018), http://www.forces.gc.ca/en/about-org-structure/canadian-joint-operations-command.page.

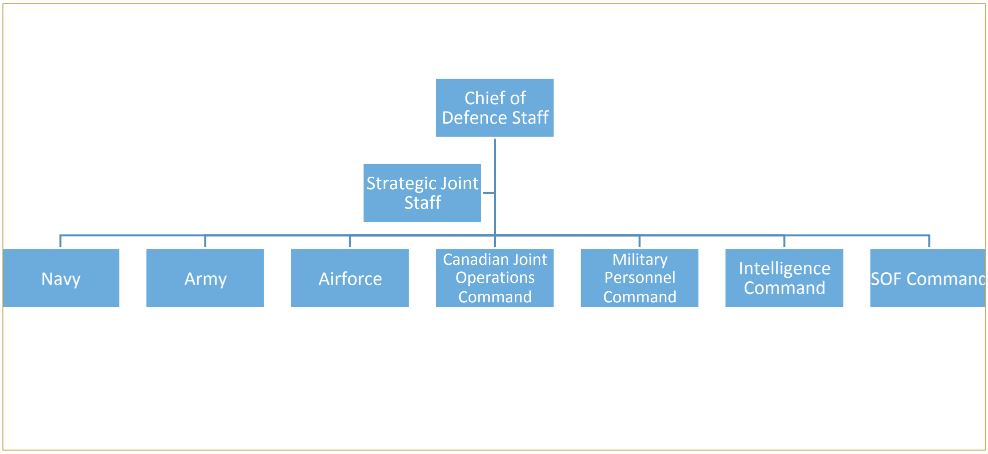


Figure 3 – Canadian Armed Forces Structure

The following summary will reflect on the two JFC concepts that have been presented and will reflect on common themes that were identified. The identification of four key themes were used as a basis for discussing the core command and control issues discussed below.

Jointery & JFC Concept:

The rationale for the creation of a Joint Forces Command were very similar and inadvertently adhered to a similar process that sought to implement a JFC and enhance jointness within their organisations. The 'Canadian Forces' unified model was initially flawed and ultimately failed as a concept and the efforts over the last five years have allowed the CAF to evolve towards and implement a contemporary JFC construct. The role of NATO standards in assisting the development of standardised command structures is notable, but the evidence suggests that the two countries have developed structures that are aligned to their respective national and international objectives. In essence, each country has customised the JFC concept to their innate operational and training requirements.

The individual JFC's are broadly similar, in that they have 4-Star or 3-Star commanders, are at the same level as the various Chiefs (army, navy, air) at the strategic level, hold responsibility for certain joint enablers (Special Forces and Communications and Information Systems) and have subsumed certain elements that were previously held by the single Services (medical).

Lessons Learned:

As posited previously, the initial model used by the Canadian Armed Forces continues to be observed internationally as an approach not to be used and its evolution over the last five years demonstrates what can be achieved when adhering to the contemporary model of a JFC construct. Evidence does acknowledge that both countries learned lessons from previous efforts to implement jointery and emphasis was put on the need to get individuals trained and familiar with the JFC concept before creating and implementing a structure. This was certainly the case with the NZDF and the CAF, particularly as they modernised their JFC over the recent years. Capability planning is also something that is now completed at a joint level for the two militaries analysed and the NZDF uses a 'future force concept' to design and identify their future capability requirements. Figure 4 provides a graphical representation of what a future force concept resembles.

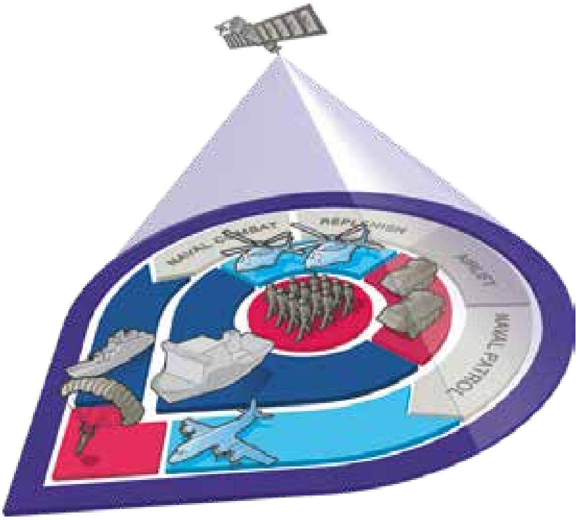


Figure 4 – NZDF Future Force Concept 2035[48]

External Reviews:

Both nations have had external reviews forced upon them politically when there was a national realisation that their previous existing structures were not fit for purpose. While the countries did previously exhibit elements of jointery, there was a significant bias towards their respective single Services, frequently to the detriment of their overall efficiency and effectiveness at the operational level. A significant observation that was elucidated from the analysis is that on completion of all of the external reviews, further enhanced levels of jointery was always recommended and at no stage did any report call for the Services to become less joint.

Challenges:

The analysis has shown that each of the militaries reviewed have had similar challenges with promoting the jointery mind-set and implementing the JFC concept. The development of a suitable command and control system was pivotal in allowing both nations the ability to design a system that was reflective of a contemporary military organisation. Each nation has command invested in their CDS and this allows for the reporting lines to be clear and concise, with one individual in charge. In all cases, the CDS is subordinate to their respective Defence Ministers, as militaries should be, but on level par with the civilian elements of the Defence Ministries (civilian staff). All individual services are subordinate to the CDS but have equal standing at the management level. This issue is pertinent as it was raised during the recent Canadian modernisation due to tension at the civil-military level, and the new SJS ensures that the civil staffs do not assume functions that are within the purview of the military staffs, and that the CDS can effectively command the CAF.

[48] NZDF, FUTURE35, "Our Strategy to 2035", New Zealand Defence Forces White Paper on Defence (2010): 5.

The Irish Defence Forces – Jointery, what's the Problem?

"The only thing harder than getting a new idea into the military mind is getting the old one out"[49]

As outlined at the commencement of this paper, the DF does not currently operate a JFC structure and jointery within the DF is minimal. The DF was established in 1924 and was primarily based around a land centric organisation that was premised on the system the UK military had used prior to the declaration of the Irish Free State.[50] While air and maritime components have been added, the structure has largely remained unchanged including the command and control element.

At present operational command of DF elements is invested in the General Officer Commanding (GOC) Aer Corps, GOC 1 and 2 Brigades and Flag Officer Commanding Naval Service (FOCNS).[51] The Chief of Staff of the DF, therefore, has no command over the force he is in charge of and this has a significant impact on how the DF is organised. Figure 5 represents the current C2 arrangements.

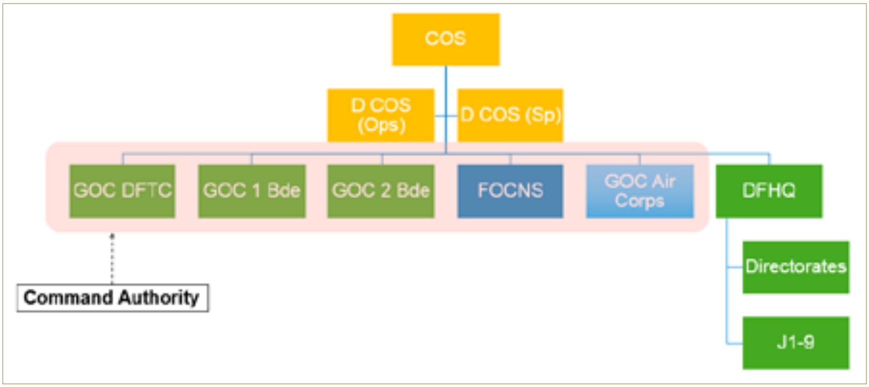


Figure 5 – Current Defence Forces Structure

As a force, the DF has not evolved when compared to other similar modern forces, such as, those reviewed previously in the paper. The resultant impact of the land-centric command and control legacy has had a consequential impact on the DF's ability to promote jointery and a JFC structure. It is noticeable that the staffing functions in DFHQ are aligned to the joint functions 'J1-J9', particularly as no other services can fill these appointments. Figure 6 below provides an alternate joint structure that could be used by the DF for a future JFC. Notable points include; the creation of a Chief of Defence (CHOD) with overall control of the military, a JFC Commander and Commander Joint Operations (CJO), thus allowing for a modern command and control structure to be established, and the amalgamation of joint enablers under the JFC, thus ensuring specialists such as the DF Special Forces have one commander. This model would recognise that each geographically specialised form of military power is vitally important, both in itself as a contributor to strategic effect, and as an enabling factor for other contributing agents.[52]

[49] Basil Liddell Hart, Thoughts on War, 1944.
[50] Defence Forces, *Defence Forces Capstone Document* (Dublin, 2016) unpublished, 1-2.0
[51] Defence Force Regulation A18, *Military Command*, (Dublin, 2015). 1-2.
[52] Gray, *The Future of Strategy*, 95.

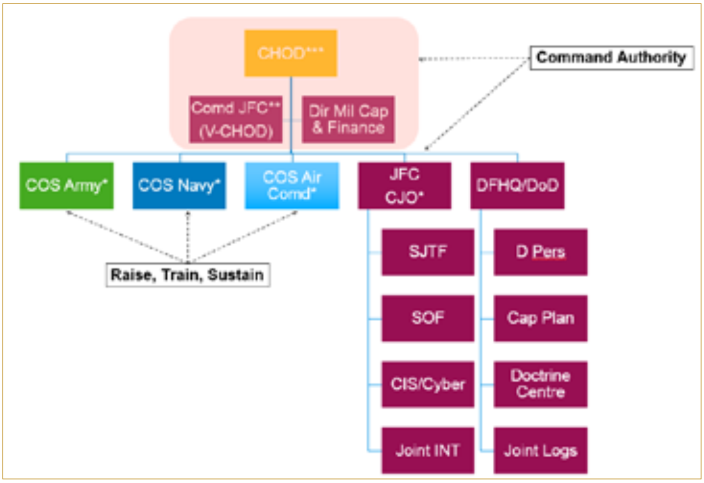


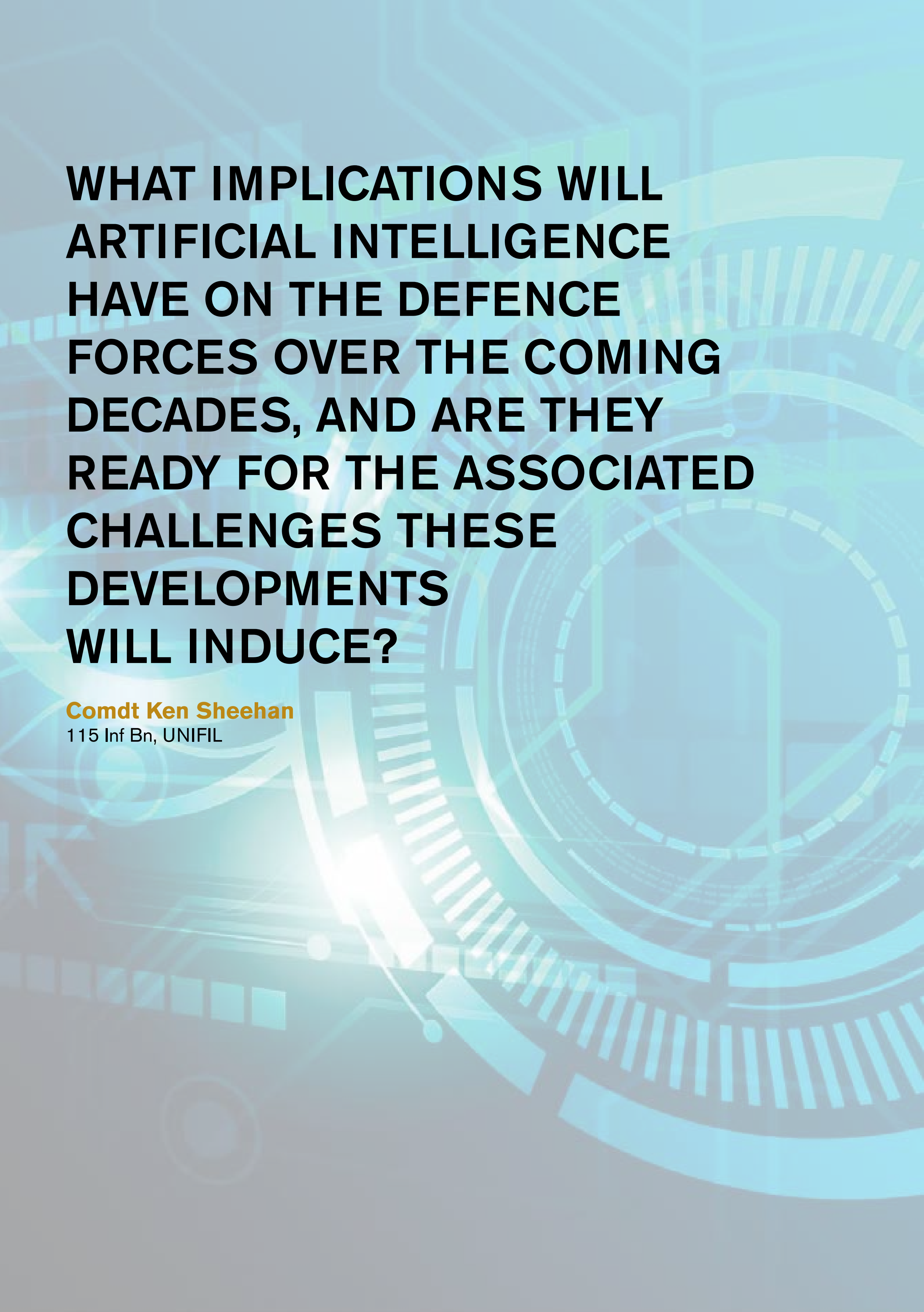
Figure 6 – Alternate Defence Forces Structure for potential JFC

In addition, the proposed new structure would allow the JFC Commander to become primus inter pares and direct all operations through a truly joint system, within which, the function of the single services, would be to raise, train and sustain forces for future DF operations, both at home and overseas. Moreover, the creation of a unified chain of command would replace the current opaque model that has never evolved to reflect best practice, thus aligning the DF to more modern and interoperable structures, similar to its partners. Finally, the lack of a credible and resourced joint cyber command is a notable omission in the current DF structure and the transition to a new modern structure would ensure that the DF could be positioned to meet current and future threats, as analysis has shown that the dogmatic adherence to a 'conventional structure' in an 'unconventional world' is hampering DF capability development.

Conclusion

This research sought to explore and answer the need for change within the DF and the transition towards a Joint Force Command structure. Through the systematic analysis of the concept of joint forces command and the evaluation of international applications of it, this research has determined that the JFC concept is one that should be implemented within the DF. The research has demonstrably shown that the benefits associated with the JFC concept far outweigh the negatives and that the nations examined in this research have promoted the concept is testament to its applicability and pertinence. While each nation faced challenges and experienced difficulties with earlier command and control models, the intervention of external review processes, driven by a political agenda successfully highlighted the deficiencies with previous operating models. The recognition that change had to be introduced was acknowledged and acted upon by each nation examined.

From a DF perspective there has never been an external review of the national command and control structures that are currently in place. Any politically motivated changes that have been implemented have traditionally been cost cutting exercises or personnel reductions and have refused to address the overall command and control elements of the DF. It is both irregular and unprecedented that an organisation that claims to be a modern and innovative military organisation still retains the command and control structure that was established almost one hundred years previous. Furthermore, the inability of the Chief of Staff to have control over the force he must manage is another systemic failure that must be addressed if the DF is to evolve and develop into a more joint organisation. Based on the analysis of this research the modern concept of a JFC does appear to be a much more efficient and contemporary means of successfully managing military operations in an effective manner. In an attempt to provide strategic direction and enable long-term capability planning the development of a 'Future Joint Force Concept' is a strategy that would significantly assist the DF in creating and then implementing a JFC. To fulfil this requirement, it will be necessary for the DF to evolve towards a joint operating model in order to create the synergies and efficiencies required to achieve a force that is affordable, sustainable and efficient. The DF's culture, traditions and history must play a part in creating and developing its future, however, at present its future is being constrained by the hand of history that refuses to allow the organisation to evolve. The solution is evident, the need for change, imminent. Only two options remain, adapt or die.



WHAT IMPLICATIONS WILL ARTIFICIAL INTELLIGENCE HAVE ON THE DEFENCE FORCES OVER THE COMING DECADES, AND ARE THEY READY FOR THE ASSOCIATED CHALLENGES THESE DEVELOPMENTS WILL INDUCE?

Comdt Ken Sheehan
115 Inf Bn, UNIFIL

Introduction

To people of a certain age, Artificial Intelligence (AI) will always be synonymous with the attempts of Arnold Schwarzenegger's T-800 to kill or save John Connor. The generation that watched these attempts in the Terminator series are now in senior leadership positions within the Irish Defence Forces, and it is possible that their perception of AI may be more driven by these cultural references, rather than any knowledge of Boolean logic or neural networks.

AI is an incredibly complex sphere of science, and it is easy to get bogged down in terms and concepts. A useful broad definition is the concept of machines using a "perception-cognition-action (or decision making)" sequence to acquire human-like intelligence.[1] For brevities sake, developments can be thought of in three separate ways:

Artificial Narrow Intelligence (ANI) is task-specific and already exists. Examples include image recognition, and voice assistants like Alexa.

Artificial General Intelligence (AGI) is considerably more complex, and does not exist. This AGI describes human-level intelligence across a number of different tasks.

Artificial Super Intelligence (ASI) is a theoretical concept that describes super human level intelligence across a number of different tasks. [2]

Despite the potential of AGI and ASI, it is expected that ANI applications will dominate over the next ten years, generating 99.5% of total AI revenue.[3] How quickly technology will advance and impact on society is unclear, with some estimates predicting that it will take between 20 and 40 years before the impacts on employment patterns are completely felt. [4]

This paper will examine the potential impact of AI on the Defence Forces by firstly examining the potential developments in the next ten years, focusing on larger militaries and their potential use of AI. It is likely that the Defence Forces will continue to deploy overseas in support of Peacekeeping operations, so it is important to consider how these new technologies are going to influence our partners in other, larger militaries.

Secondly, as a small military with a limited budget, the potential areas where AI could assist the Defence Forces will be considered. Computers excel at assisting in routine, predictable tasks. These attributes may impact on AI's potential contribution to Human Resources and logistical processes, and the potential for use in the Defence Forces will be examined.

Finally, the readiness or otherwise, of the Defence Forces to adapt to the changes that AI will bring as part of the Fourth Industrial Revolution will be examined. The Defence Forces prioritisation of Information Technology will be considered through a People, Process, Technology lens. It will be argued that the Defence Forces may struggle to adapt, and use AI appropriately for an organisation of its size and goals.

[1] Pant, A. (2018) 'Future Warfare and Artificial Intelligence', Institute for Defence Studies & Analyses, Occasional Paper 49, p. 4.

[2] Price, M., Walker, S., & Wiley, W. (2018) 'The Machine Beneath: Implications of Artificial Intelligence in Strategic Decision Making', PRISM The Journal of Complex Operations, Vol. 7(4), pp. 92-105, p. 96.

[3] AI Forum New Zealand (2018) 'AI Shaping a Future New Zealand', AI Forum New Zealand, available: https://aiforum.org.nz/wp-content/uploads/2018/07/AI-Report-2018_web-version.pdf [accessed 01 Jul 19], p. 35

[4] AI Forum New Zealand (2018), Op Cit, 51.

Potential Military Developments In Next Ten Years

The major military powers have recognised the potential of AI, and have committed to its development. The US National Defence Strategy pledges to invest broadly in AI to gain competitive military advantages.[5] China's 2017 New Generation AI Development Plan envisages the country being the world leader by 2030, with an AI sector worth $150 billion. [6] Russian President Putin recently stated "Artificial Intelligence is the future not only of Russia, but of all of mankind."[7]

While AI has been prioritised, and resources have been given to its development, technical, ethical, and legal challenges mean that the advance from ANI to AGI will not be linear. Considering the challenges that lie ahead, there may be three areas where the Defence Forces may encounter AI being used by our partners in larger militaries in overseas deployments: detection, preparation and protection.[8]

Unmanned Vehicles on land, air and sea have the potential to improve situational awareness and increase the likelihood of detection of a threat. ANI is already used in a number of Unmanned Aerial Vehicles (UAV), and the technology is likely to lead to countries deploying UAVs in swarms. Russia is also reportedly developing swarm technology using AI[9], and the US has carried out tests with over 100 drones being deployed from a F/A-18.[10] In the cyber domain, Project Maven, is reportedly already in use by US Africa and Central Commands. This project is developing AI algorithms to intercept satellite and drone surveillance feeds.[11]

Intelligent Decision Support Systems (IDSS) may support commanders in preparations for operations "by collecting and analysing evidence, detecting familiar patterns in the data, checking hypotheses, suggesting possible courses of action, and evaluating the appropriateness of proposed actions." [12] The three block war concept has evolved into a multi-domain hybrid conflict. The US Army has developed an Automated Planning Framework prototype to analyse the Military Decision Making Process (MDMP) with the goal of assisting the army in understanding, planning and fighting in a multi-domain battle.[13] An IDSS could help to "deal with complexity better"[14] as increasing amounts of information are provided to commanders by AI enabled sensors. This could lead to better, quicker decisions, which may drive demand for further AI innovation in the MDMP process. The practical, ethical and training considerations that these systems could have on Peace Support Operations may become significant, as militaries who use AI enhanced MDMP will change their tactics, techniques and procedures to maximise their leverage from this advantage.

There are several weapon systems in service which use ANI to protect against a threat, such as Israel's Harpy (anti-radar) and Iron Dome (anti-missile); and the US's Phalanx close in weapons

[5] Price, Walke & Wiley, Op Cit,97.
[6] AI Forum New Zealand, Op Cit, 16.
[7] Price, Walke & Wiley, Op Cit, 97.
[8] Fiott, D. & Lindstrom, G. (2018) 'Artificial Intelligence What Implications for EU Security and Defence?' EU Institute for Security Studies Briefs, Nov, pp 1-8, p. 4.
[9] Pant, Op Cit, 39.
[10] Madrigal, A. (2018) ' Drone Swarms Are Going to be Terrifying and Hard to Stop', The Atlantic, available: https://www.theatlantic.com/technology/archive/2018/03/drone-swarms-are-going-to-be-terrifying/555005/ [accessed 01 Jul 19]
[11] Fiott, D. & Lindstrom, G., Op Cit, 2.
[12] Van den Bosch, K. & Bronkhorsy, A. (2018) 'Human-AI Cooperation to Benefit Military Decision Making', NATO Science & Technology Organisation, available: https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-IST-160/MP-IST-160-S3-1.pdf [accessed 01 Jul 19], pp. 1-13, p. 4.
[13] Price, Walke & Wiley, Op Cit, 99.
[14] Roke (2019) 'STARTLE', Roke, available: https://www.roke.co.uk/what-we-do/intelligent-sensors-and-unmanned-systems/startle [accessed 01 Jul 19]

system and Patriot anti-missile system. South Korea has deployed the Samsung Techwin SGR-A1 autonomous gun, which includes surveillance, tracking and firing technologies as part of its border defences.[15] The potential for these types of weapon systems to assist in the detection of threats around a camp or a Forward Operating Base in a Peace Support Operation are clear.

Where Can AI Help The Defence Forces

Considering the limited size and budget of the Irish Defence Forces (2019 non-pay expenditure is estimated to be €229 million[16]), it is unlikely that any of the bespoke military AI systems will be purchased in the short term. However, rather than military systems, AI Research and Development (an estimated $5 billion in 2020[17]) is likely to be focused on dull, repetitive tasks that are currently carried out by humans across a number of different industries.[18] AI does have the potential to substitute humans in a range of manual or repetitive tasks, allowing the same people to be redeployed into higher value tasks. A New Zealand study found that this process alone had the potential to increase its GDP by up to $36 billion by 2035.[19]

An obvious area where the Defence Forces could employ AI is in logistical management. Logistical management is a labour intensive task, requiring expertise, but with significant amount of repetition, and patterns. The practice of militaries using AI to assist in logistical management started almost 30 years ago when, when the US military used the Dynamic Analysis and Replanning Tool (DART) in the First Gulf War. [20] Since then, the use of AI to assist with logistics has become more and more widespread. There are a number of logistical companies using AI technology like Microsoft Cortana Intelligence to manage transportation, and increase the accuracy of their forecasting. [21]

There are several Human Resources (HR) applications that utilise the ability of machine learning algorithms to infer a wide array of things about people.[22] One potential use of AI in the HR sphere for the Defence Forces is to better identify those that are at risk of leaving the organisation. Recruit Holdings (a Japanese staff servicing group) uses a wide array of data to compare employees to those who previously resigned. These employees are then interviewed by managers to resolve potential issues.[23] This is an obvious way in which retention could be improved, if technology assisted to identify dissatisfied members in advance. There are also likely to be cultural barriers that may prevent the use of AI in certain processes like promotion. There are some studies showing the potential of techniques like "vocal analysis" and micro expression analysis to identify traits which match those of existing high-performing employees. [24] This is a possible area where the Defence Forces values could come into conflict with technology.

[15] Pant, Op Cit, 42.
[16] Kehoe, P. (2019) 'Select Committee on Foreign Affairs, Trade and Defence' Dail Eireann Debate, available: https://data.oireachtas.ie/ie/oireachtas/committee/dail/32/select_committee_on_foreign_affairs_and_trade_and_defence/submissions/2019/2019-03-05_opening-statement-paul-kehoe-minister-for-defence_en.pdf [Accessed: 01 Jul 19]
[17] Pant, Op Cit, 18.
[18] Ibid, 35.
[19] AI Forum New Zealand, Op Cit, 19.
[20] Pant, Op Cit, 15.
[21] AI Forum New Zealand, Op Cit, 76.
[22] Tufekci, Z (2019) 'Think You're Discreet Online? Think Again.' New York Times, available: https://www.nytimes.com/2019/04/21/opinion/computational-inference.html [Accessed: 01 Jul 19]
[23] Nikkei (2018) 'Japan's Recruit Employs AI to Stop Workers From Quitting', Nikkei Asian Review, available: https://asia.nikkei.com/Business/Companies/Japan-s-Recruit-employsAI-to-stop-workers-from-quitting [Accessed: 01 Jul 19]
[24] Buranyi, S (2018) 'Dehumanising, Impenetrable, Frustrating": The Grim Reality of Job Hunting in the Age of AI', The Guardian, available: https://www.theguardian.com/inequality/2018/mar/04/dehumanising-impenetrable-frustratingthe-grim-reality-of-job-hunting-in-the-age-of-ai [accessed: 01 Jul 19]

Defence Forces values are explicitly linked with the way the organisation thinks about and understands both leadership and promotion.[25] Culturally, no matter how good the science is, it is impossible to see how the Defence Forces could move towards an assessment method that is not open and easily understandable. The idea that a leader is in anyway evaluated by something that is not detectable to the human eye is likely not to be accepted within the organisations culture, at least in the short term.

A third area where AI could be used in the Defence Forces within the next ten years is to assist with anomaly detection in communications networks. Currently, analysis of network traffic is generally carried out by specialists. Intrusion Detection Systems (IDS) could reduce the Communications and Information Services (CIS) Corps specialists required to defend the network, utilising the ability of ANI to recognise patterns.[26] This could allow the CIS Corps to redeploy personnel away from repetitive, but important tasks, to be better used elsewhere. There are also other areas where the ability to detect change in patterns could improve our personnel and processes in the short term. UK Police forces are already using predictive policing models in an attempt to offset financial cuts.[27] This type of technology may improve the Defence Forces ability to detect changes in patterns across different domains.

Readiness Of The Defence Forces To Adapt

Past performance is usually the best indicator of future behaviour. While assessing the likelihood of the Defence Forces being ready to adapt, it is appropriate to consider briefly how the organisation has adapted to technology over the last ten years through a people, process and technology lens.

The Defence Forces has made a considerable investment in its personnel over the last ten years to keep up with technology, with the Trainee Technician Scheme which awards trainees level seven degrees in conjunction with IT Carlow[28] and the CIS Young Officers Course awarding a Masters level qualification. [29] However, the number of personnel that are in the Defence Forces with these qualifications is arguably not sufficient considering the wide array of tasks that they have. The CIS Corps currently has 22 technical officer appointments, and 202 technician appointments. There are 66 technician appointments not filled. [30] These figures do not include non-technical CIS appointments and those in training, however it is difficult to envisage how the Defence Forces can meaningfully and consistently engage with emerging technologies with very limited personnel. The AI expert shortage worldwide[31] is also likely to create issues for the Defence Forces, as any personnel that gain experience are likely to be very attractive to the private sector. Other militaries, such as the New Zealand Defence Forces (NZDF), have assessed

[25] Irish Defence Forces (2016) 'Defence Forces Leadership Doctrine', Irish Defence Forces, available: https://www.military.ie/en/public-information/publications/df_leadership_doctrine.pdf [accessed: 01 Jul 19]

[26] Svenmarck, P., Luotsinen, L., Nilsson, M., & Schubert, J. (2018) 'Possibilities and Challenges for Artificial Intelligence in Military Applications', NATO Science & Technology Organisation, available: https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-IST-160/MP-IST-160-S1-5.pdf [accessed 01 Jul 19], pp. 1-15, p. 4.

[27] Marsh, S. (2019) 'Ethics Committee Raises Alarm Over ' Predictive Policing' Tool', The Guardian, available: https://amp.theguardian.com/uk-news/2019/apr/20/predictive-policing-tool-could-entrench-bias-ethics-committee-warns [accessed 01 Jul 19]

[28] Irish Defence Forces (2019) 'Communications & Information Services School', Irish Defence Forces, available: https://www.military.ie/en/who-we-are/army/defence-forces-training-centre/schools-of-the-dftc/cis-school/ [accessed 01 Jul 19]

[29] Irish Defence Forces (2019) 'Defence Studies', Irish Defence Forces, available: https://www.military.ie/en/who-we-are/army/defence-forces-training-centre/the-military-college/defence-studies-programme/ [accessed 01 Jul 19]

[30] Kehoe, P. (2019) 'Defence Forces Personnel Data', Dail Eireann Debate, available: https://www.oireachtas.ie/en/debates/question/2019-03-27/99/ [accessed 01 Jul 19]

[31] Horowitz, M., Allen, G., Kania, E. & Scharre, P. (2018) 'Strategic Competition in Era of AI', New American Security, available: https://www.cnas.org/publications/reports/strategic-competition-in-an-era-of-artificial-intelligence [accessed 01 Jul 19], pp. 1-26, p. 5.

how technology can be used as a force multiplier. The NZDF have committed significant resources and time (€60.7 million over the next four years[32]) to the Network Enabled Army programme. This programme is expected to last 15 years, and it intends to exploit advances in information systems to drive change, including mitigating the NZ Army's lack of numerical strength.[33] The Defence Forces, despite investing in technology such as the Virtual Desktop Architecture system and the Software Defined Radio project, do not currently have a long term strategy to ensure that the organisation can adapt its personnel, its processes and its regulations to use technology appropriately.

From a process lens, the 2015 White Paper of Defence referred to responsibilities in cyber for the first time. A Cyber event is assessed as having a very high impact and a moderate likelihood on the National Risk Matrix. [34] While the Defence Organisation is "committed to participating in the delivery of measures to improve the cyber security of the state" [35] it is difficult to see how the Defence Forces is in a position to assist significantly in the cyber security of the state, considering the current number of personnel, what the CIS Corps is tasked with supporting, and the level of spending (CIS capital spending was €11.1 million[36] in 2017). As technology expands further, it is hard to envisage how the Defence Forces will keep up unless there is some process change. The example of the Cyber Defence Unit of the Estonian Defence League shows what is possible if an innovative approach is taken to how defence organisations mitigate against the challenges posed by technology.[37]

Technically, there have been some real advances over the last ten years. Recent rollouts of Sharepoint, [38] data centre innovation, [39] the Virtual Desktop Architecture Project [40] and SITAWARE[41] have shown that the Defence Forces currently retains the capability of delivering technical solutions. There have also been attempts to ensure that Defence Forces is getting value for money from these technical solutions, like the Chief of Staff's innovation awards. However, these technical advances have not been matched by changes in our structures to provide support to these new technologies. As well as the personnel issues already outlined, it could be argued the Defence Forces regulations have not kept pace with the changes in technology, to, for example, ensure that routine administrative processes, are using technology to its full potential.

AI is unique in a number of ways that will cause difficulties. As with most technical advances, senior leadership within organisations will need to adapt, understand and prioritise AI before

[32] Mark, R. (2019) 'Next Stage of Network Enabled Army Programme to Begin', Beehive, available: https://www.beehive.govt.nz/release/next-stage-network-enabled-army-programme-begin [accessed 01 Jul 19]

[33] New Zealand Defence Forces (2017) 'Future Land Operating Concept 2035', New Zealand Government, available: http://www.army.mil.nz/downloads/pdf/public-docs/2017/20170626-future-land-operating-concept-2035.pdf [accessed 01 Jul 19], p. 34.

[34] Department of Defence (2017) 'National Risk Assessment 2017', Department of Defence, available: https://www.defence.ie/system/files/media/file-uploads/2018-07/national-risk-assessment-ireland-2017.pdf [accessed 01 Jul 19]

[35] Department of Defence (2017) 'DoD and DF Strategy Statement 2017-2020', Department of Defence, available: https://www.defence.ie/system/files/media/file-uploads/2018-06/ss2017_0.pdf [accessed 01 Jul 19]

[36] McCarthy, S (2018) 'Vote 36', Comptroller and Auditor General, available: https://www.audit.gov.ie/en/Find-Report/Publications/2018/vote-36.pdf [accessed 01 Jul 19]

[37] Kaska, K., Osula, A. & Stinissen, J. (2013) 'The Cyber Defence Unit of the Estonian Defence League', NATO Cooperative Cyber Defence Centre of Excellence, available: https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf [accessed 01 Jul 19]

[38] Spanish Point (2015) 'Defence Forces and Spanish Point are awarded IT Professional Team of the Year', Spanish Point, available: https://www.spanishpoint.ie/news-blog/defence-forces-and-spanish-point-are-awarded-it-professional-team-of-the-year/ [accessed 01 Jul 19]

[39] Tech Awards (2019) 'Tech Excellence Awards 2019', available: https://techawards.techcentral.ie/winners-2019/ [accessed 01 Jul 19]

[40] Kehoe, P. (2018) 'National Development Plan Funding', Dail Eireann Debate, available: https://www.oireachtas.ie/en/debates/question/2018-10-23/section/135/ [accessed 01 Jul 19]

[41] Systematic (2019) 'Ireland Conncets All Forces Through Sitaware', Systematic, available: https://systematic.com/defence/cases/ireland-connects-all-forces-through-sitaware/ [accessed 01 Jul 19]

it could reach its potential. This process will not take place in a bubble, and it is likely to be influenced by AI use in the wider society, with autonomous drones being one of the most likely widespread, noticeable uses of the technology in the next ten years.[42] How humans interact and "trust" AI enabled systems is recognised as being a significant challenge and studies are underway to investigate how these systems can "build trust" with humans. One concept being developed is "explainable AI", where the AI would "explain" the reasoning used to make a choice.[43]

Conclusion

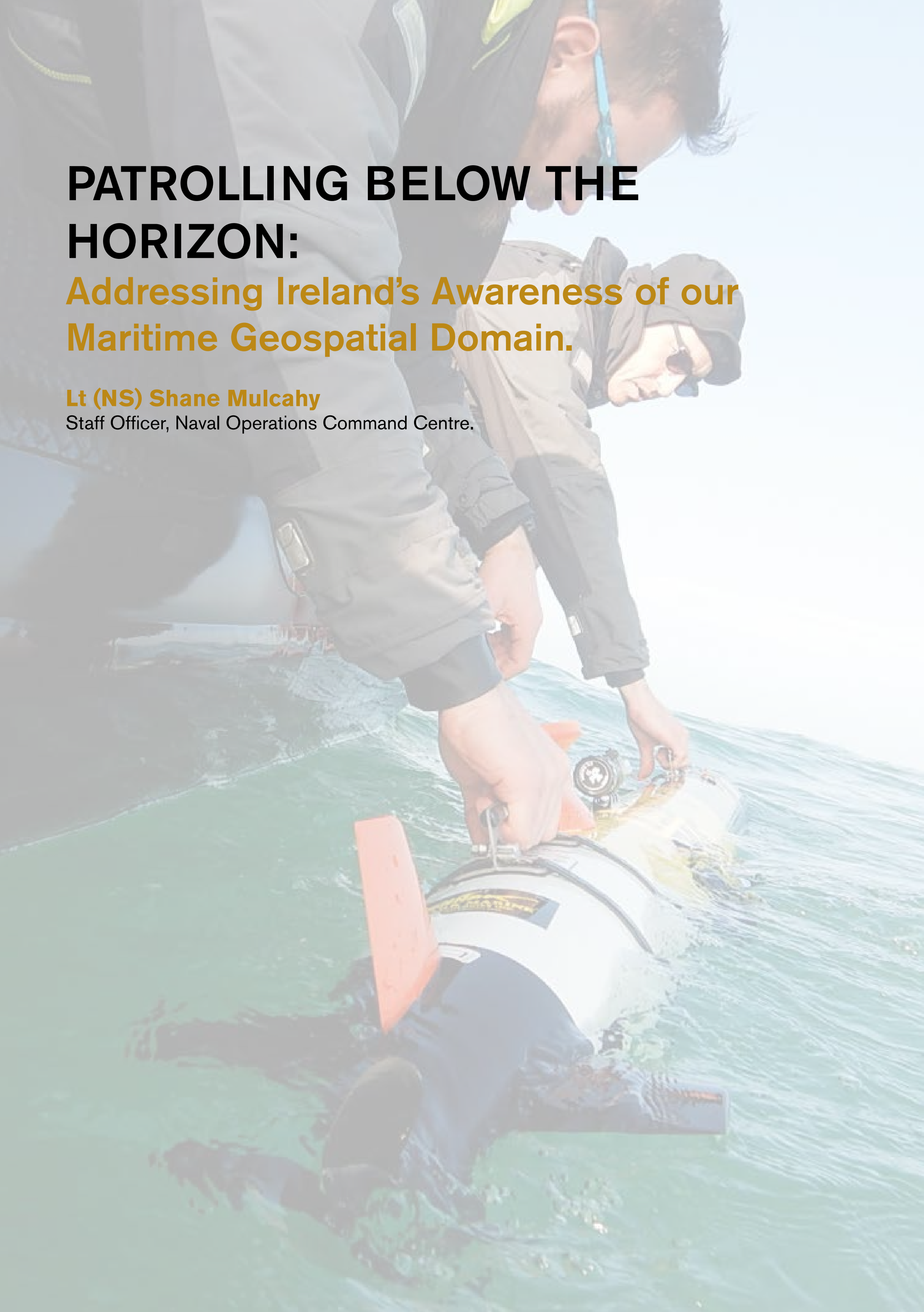
In 2017, Ireland was one of 25 European countries signing a declaration of cooperation on AI.[44] However, Ireland does not have a National AI strategy. This is essential if Ireland Inc. and the Defence Forces are to consider how and why AI will be used. A recent New Zealand report describes the risks of non-engagement with AI starkly – "shape or be shaped".[45]

The Defence Forces is likely to encounter AI enabled systems within the next ten years on Peace Support Operations and also in other limited areas to assist with repetitive tasks. The ability of the Defence Forces to adapt is uncertain given the limited amount of CIS specialists to implement, maintain and operate these systems.

AI has the potential to change warfare by delivering "violence at a greater volume and higher velocity than ever before."[46] It does not take too much imagination to look at the 2018 Winter Olympics Opening Ceremony, which was performed with the assistance of 1,218 autonomous drones,[47] and imagine changes to come. This paper has concentrated on how the Irish Defence Forces and its partners in multi-national operations could use AI, however it has not considered how non-friendly actors could use this technology. The "cost of entry" for simple applications could be low, as large tech companies are making their machine-learning tools freely available.[48] Militaries could be vulnerable if non-friendly actors combined AI with social media to perform large disinformation campaigns.[49] It is not hard to imagine how difficult this type of a scenario would be to deal with if an overseas unit were targeted.

There are challenges ahead, but technology will continue to drive changes within our society and our Defence Forces. Considering the responsibilities that the Defence Forces has to state security, the nature of Ireland's economy, and its foreign policy goals, if there is not a considered engagement with the constant process of catching up with technology, not only is there a risk of missing out on the benefits of technology, but also of becoming that little bit less relevant.

[42] Cummings, Op Cit, 12.
[43] Pant, Op Cit, 31.
[44] Fiott, D. & Lindstrom, G. Op Cit, 2.
[45] AI Forum New Zealand, Op Cit, 17.
[46] Brose, Op Cit, 127.
[47] Ibid., 127.
[48] Ramamoorthy & Yampolskiy, Op Cit, 3.
[49] Svenmarck, P., Luotsinen, L., Nilsson, M., & Schubert, J, Op Cit, 9.



PATROLLING BELOW THE HORIZON:

Addressing Ireland's Awareness of our Maritime Geospatial Domain.

Lt (NS) Shane Mulcahy
Staff Officer, Naval Operations Command Centre.

Abstract

In January 2008 off Alexandria Egypt, two merchant vessels anchored in order to wait out an approaching weather front moving through the Mediterranean. Heavy wind and swell conditions caused the ship's anchors to drag along the seabed; a common occurrence at sea. On this occasion however, the anchors severed five submarine communication cables in the process, crippling communications systems connecting Europe, North Africa, and the Middle East. The sole remaining telecom link buckled under the transferred stress, disrupting the internet connectivity of more than 80 million people, including governments and businesses in the Middle East and Asia.[1] Notwithstanding substantial costs of repair, the economic effect of this accidental and relatively short-lived interruption was felt internationally, with the event linked to global oil prices and US dollar fluctuations at the time.[2] Eleven years on, what has been learned about protecting these vital subsea communication links?

How important are Undersea Cables?

Ireland's central role in global communications far outdates the arrival of tech industry giants like Apple or Microsoft to our shores. On August 16th, 1858, the world's first trans-Atlantic telegraph was sent along a copper cable wrapped in tree-sap, which stretched over 2,000 miles from Newfoundland, Canada to Valentia Island off the Kerry coast. The message sent; a letter of congratulations from Queen Victoria to US President James Buchanan. Comprising of less than 100 words, it took almost 18 hours to transmit.[3]

Thankfully, transmission speeds have improved over time. Modern cables have replaced copper with glass strands, allowing data to be transmitted down optical fibres as wavelengths of light, travelling at about 180,000 miles per second. One such strand has the capacity to transmit data at up to 400GB per second, the equivalent to around 375 million phone calls, or transfer every single episode of Game of Thrones in high definition, per second. With a single undersea cable (slightly thicker than a garden hose) containing upwards of 200 fibres, the scale of information transfer occurring unnoticed along the seabed is staggering.

It was once assumed that modern satellite communication systems would replace the need for these dated landlines. However, satellites continue to account for less than 3% of global data transmission, with over 97% of all data passing along the ocean floor.[4] The interest in satellite data traffic of the 1980s was quickly replaced by the dawn of fibre-optic technology, which could transfer data over five times faster than by satellite, and do so at a fraction of the cost; on reflection, it is far cheaper to dispatch a repairman to the English Channel than into space.[5] Today's network of submarine cables comprises of over 200 separate systems, made up of over 500,000 miles of fibre, enough to wrap around the equator over twenty times.[6]

[1] Rishi Sunak and James Stavridis, Undersea Cables: *Indispensable, Insecure* (Policy Exchange, 2017), 37.

[2] John C. Dvorak, "Using the Internet as a Weapon," (MarketWatch, 2008), 8.

[3] Glover, B, *History of the Atlantic Cable & Undersea Communication from the First Submarine Cable of 1850 to the Worldwide Fiber Optic Network: Atlantic Cable Broadsides and Lithographs.* (Canada, FTL Design, 2010).

[4] Sechrist and Belfer, New Threats, Old Technology: Vulnerabilities in *Undersea Communications Cable Network Management Systems*, (Center for Science and International Affairs 2012).

[5] Caroline Elliott et al., "An Economic and Social Evaluation of the UK Subsea Cables Industry," Monograph, 2016.

[6] Sunak and Stavridis, Op Cit, 38.

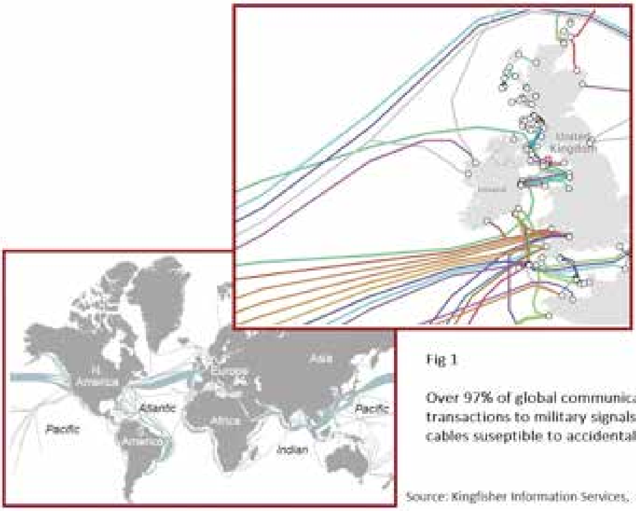


Fig 1

Over 97% of global communications, from financial transactions to military signals, are carried by undersea cables suseptible to accidental or deliberate damage.

Source: Kingfisher Information Services, http://www.kis-orca.eu/map.

What makes these cables so important? Within the 2.5 billion gigabytes of data produced globally every day are on average, 500 million tweets, 294 billion emails, and 2.7 billion Facebook likes. It also includes the 15 million daily financial transactions which keep the global economy afloat, valued at over US$10 trillion, every 24 hours.[7] The steady increase in our data dependence has caused undersea cables to silently become the bedrock of a modern, globally interdependent society. Considering Ireland's geostrategic location, the lattice of submarine cables surrounding our Ireland has been well described as the 'corporate and physical backbone layers of the Internet'.[8]

What is the risk?

Around three quarters of all transatlantic cables in the northern hemisphere pass through or near Irish waters.[9] The risk posed to these cables ranges from curious sea-life, natural disasters, accidental or deliberate human interaction, or from the sheer harshness of the marine environment in which they reside. Our role in protecting this global network is becoming increasingly evident. For example, in the unlikely event that the undersea network between Europe and America were to fail, the entire capacity of every satellite orbiting the earth could handle less than 10% of the communications sent from the United States alone.[10] From an accidental point of view, this risk is usually remote; today's undersea cables are constructed to extraordinarily high standards of reliability, on par with those seen in nuclear weapons and on space shuttles.[11] In terms of dependability, the average downtime of modern cables is measured in seconds per year, with the global undersea network suffering an average of around 100 cable outages per annum. Network redundancy often allows such breakages to go relatively unnoticed, however this is not always the case.

[7] John Filitz, "UNDERSEA FIBER-OPTIC CABLE CRITICALITY," n.d., 4.

[8] Paul O'Neill, "Underwater Cables Leave Ireland Tangled – and Implicated – in the Internet," *Dublin Inquirer*, February 20, 2019.

[9] Kingfisher Information Services, "Offshore Renewables and Cables Awareness Interactive Map," http://www.kis-orca.eu/map.

[10] US Chamber of Commerce, "Statement of the U.S. Chamber of Commerce on Hearing on the United Nations Law of the Sea Convention," n.d. (2012)

[11] Modern subsea cables are engineered to what is known as the 'five nines' standard. In other words they are reliable 99.999% of the time. Sechrist and Belfer, *New Threats, Old Technology,* (Center for Science and International Affairs).

In December 2006, a 7.0 Mw earthquake triggered massive undersea landslides near the 160-mile-wide Luzon strait, which severed the vast majority of submarine cables linking internet and phone services from North America to China, Hong Kong, Japan, Singapore, South Korea, and Taiwan.[12] Considering the geographic realities which caused multiple systems to be placed in such close proximity, it is worth pointing out that the majority of transatlantic cables transiting past the Irish coast do so through a funnel less than 100 miles wide.[13]

Unfortunately, the most potent risk to our subsea domain may not be a natural or accidental one. If these vital information arteries can be susceptible to a dragging anchor or rogue fishing net, we are left with a far more worrying question to address: What about a deliberate, hostile act?

In terms of strategy, cable cutting is a legitimate and often utilised tactic. Within hours of declaring war in 1914, pre-positioned Royal Navy assets quietly severed all five of Germany's vital trans-Atlantic undersea telegraph cables.[14] A full century later, the annexation of Crimea by Russia in 2014 was aided by 'little green men' who cut all but one of the cable connections linking the Crimean peninsula to the rest of Ukraine (the sole remaining internet exchange point was already under Russian control, being used to control the flow of disinformation to portray the legitimacy of Russia's military action).[15]

Subsea cables are by their very nature a soft military target. They are fragile and geographically concentrated, often in remote and hard to monitor locations. They can be attacked with little risk of loss of life, and any unwitnessed tampering can usually be plausibly denied (important for anyone looking to exploit the grey areas of NATO Article 5 mutual responsibilities). The relative ease of severing a subsea cable means that a threat can easily emanate from non-state actors, and their susceptibility is heightened by the public knowledge of their positions; to avoid accidental damage from fishing activity, charts providing accurate locations of the majority of commercial cables are freely available in the public domain.[16]

Aside from cables being cut – tapping of subsea communication lines has been common practice since the cold war.[17] As evidenced by NSA whistle-blower Edward Snowden in 2013, the practice of undersea cable tapping certainly hasn't been curtailed in any way by advances in cable design. On the surface, a modern fibre optic cable can be tapped in just minutes using a handful of modest tools; at depth, military powerhouses like the United States have ensured that their ability to listen at will has not been compromised.[18] Ireland is most assuredly not immune from the risk of tapping. The widely known but unacknowledged Russian 'Spy ship' YANTAR made headlines in 2015 when it was found loitering over subsea cables off the US coast.[19] Carrying two submersibles capable of working at depths of 6,000 meters, YANTAR is no stranger to European, and even Irish, waters. With global interest in the wealth of information travelling along our seabed, it's not a case of preventing cables from being tapped;

[12] Sunak and Stavridis, Op Cit

[13] Kingfisher Information Services, Op Cit

[14] Martin Gibson, "Britain Cuts German Cable Communications 5 August 1914," War and Security (blog), August 5, 2014.

[15] Keir Giles, "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power," *Chatham House*, 2016.

[16] Kingfisher Information Services, Op Cit

[17] NSA-led US Navy Operation IVY BELLS in 1971 resulted in compromising a Russian subsea cable between two Soviet naval bases in the Sea of Okhotsk in the Pacific Ocean.

[18] The Associated Press, "New Nuclear Sub Is Said to Have Special Eavesdropping Ability," *The New York Times*, February 20, 2005.

[19] "H I Sutton - Covert Shores,", http://www.hisutton.com/Yantar.html.

governments, businesses, and even ordinary citizens should best assume that they are. With the risk laid bare, what, if any, protection can the Defence Forces offer to this vital infrastructure? This question must be considered not only from a capability standpoint, but also from a legal one.

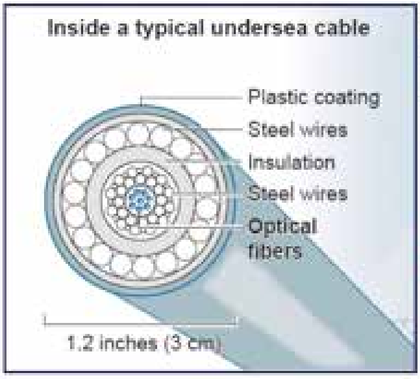


Fig 2
Cables can be damaged by ship's anchors, fishing nets, earthquakes, and other hazards; they are also targets for sabotage. Numerous reports exist of russian surface and submarine assets lingering near North Atlantic cable sites.

First of all, nations have tended not to own the communications cables linking them. Save for a select number of military-focused links,[20] economics dictate that trans-ocean cables are predominantly privately owned and bankrolled by telecoms conglomerates or, more recently, giants such as Facebook and Google.[21] Afterall, subsea cables are expensive. The Southern Cross Cable for example, linking the Australian and North American continents cost upwards of US$1.5 billion.[22] While the entrepreneurial approach to undersea communication has been successful, it has led to a lack of clarity with regard to the international status of cable infrastructure, and little protection at national government level.

Unlike the ship's which lay them, subsea cables do not fly a flag, have no homeport, and bear no legal association with any particular nationality. Numerous attempts have been made to address this complicated status under international law. The 1884 Convention for the Protection of Submarine Telegraph Cables was a first attempt to make interference with subsea cables a punishable offence at a national level,[23] followed by the 1958 Geneva Convention on the High Seas, which protected the creation of undersea cables in international waters.[24] The most recent and comprehensive legal consideration has been the 1982 United Nations Convention on the Law of the Sea (UNCLOS), frequently referred to as a 'constitution of the seas'.[25] This comprehensive convention, on which some 167 nations reached varying levels of agreement, places significant theoretical protection on undersea cables in international waters, but falls short in some vital practical aspects. One critical flaw in the protections offered lies

[20] Thomas Nilsen, "*Russia plans to lay a trans-Arctic fiber cable linking military installations*", The Independent Barents Observer, April 24, 2018.
[21] Sunak and Stavridis, Op Cit.
[22] Tara Davenport, "Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis," *Catholic University Journal of Law and Technology* 24, no. 1 (2015).
[23] Submarine Telegraph Act 1885, Chapter 49.
[24] United Nations Convention on the High Seas 1958.
[25] United Nations Convention on the Law of the Sea, (UNCLOS) 1982. Article 113.

in Article 113, which stops short of giving warships the right to board vessels suspected of intentionally trying to damage undersea cables in international waters.[26] Anything short of this

implicit power makes it almost impossible for naval powers of any nation to effectively deter hostile vessels above or below the surface. While critical of the extent of these 1982 protections, it must be remembered, that the birth of transatlantic fibre optics and our reliance on these cable systems are all pre-dated by the 1982 UNCLOS agreement. Increased mandate for the overt protection of these international networks would appear long overdue.

Some nations, having recognised the gap in international protections, have sought to fill the void with policy solutions at a more local level. Australia and New Zealand, as Island nations with communications-dependant economies, have introduced Cable Protection Zones (CPZs) which provide a range of restrictions to prevent cable damage in sovereign waters.[27] These CPZs deliver the mandate for increased surveillance and intervention, as well as financial deterrents of up to £250,000 for those found to be in breach.

Similarly, private companies have started to look at ways to protect their own investments outside of existing conventions. Seismic sensors originally developed for the oil and gas industry also have the ability to detect the vibrations created by surface or subsea vehicles operating in their vicinity. These relatively low-cost sensors, placed around cable routes and other key subsea infrastructures, can gather valuable information of a pending deliberate or accidental threat.[28]

Closer to home, the absence of assured legal footing makes the role of protection more difficult; and increasingly grey. What mandate and methods remain to defend, protect, and support the integrity of our maritime domain?

An Irish response to a Global Problem.

Some will argue that given the international effort required to secure the vast North Atlantic maritime domain in which we reside, our part as a small, 'neutral' nation, should neither be significant nor central. It is worth remembering however that as an Island that has successfully grown a digital economy on a fragile maritime infrastructure, Ireland may have the most to lose.

Considering western preoccupation with weapons of mass destruction in previous decades, it seems almost comical to find that a ship's anchor could now be described as an 'existential threat' to national security and prosperity.[29] With no alternative to using these undersea cables, Ireland must become proactive towards securing the maritime domain on which our contemporary, digital society depends.

The Irish government's 2015 White Paper on Defence provides limited direction, highlighting the Naval Service's ability to "express state sovereignty and political will at sea in order to further national policy objectives in the maritime domain".[30] This is accompanied by the stated intention to provide an 'enhanced capability' in 'the protection of Ireland's vital sea lanes of communication'.[31] This direction has thus far manifested in limited bottom profiling

[26] Davenport, Op Cit.
[27] NZ Ministry of Transport "Protecting New Zealand's Undersea Cables" Ministry of Transport Publication, 2009.
[28] Sunak and Stavridis, Op Cit.
[29] Sechrist and Belfer, Op Cit.
[30] Department of Defence, "White Paper on Defence 2015," Para. 3.5.5.
[31] Department of Defence, "White Paper on Defence 2015," Para. 6.5.

capabilities from surface assets, and a recent foray into autonomous underwater vehicle sensors. Without systems capable of subsurface detection linked to data analysis systems ashore, the Naval Service remains quite literally, lost in the dark.

But there does appear to be some flexibility in how the Naval Service shapes its own perspective. A tentative tender process has commenced with the aim of equipping Ireland's principal sea-going agency with more versatile and capable platforms, supported by government's white paper vision. Increased mandate for further development in countermine and counter-IED capabilities ensures continued focus on monitoring and intervention on the seabed. The development of a highly deployable multi-role vessel concept provides scope for a platform more suited to ocean governance roles. In this regard, the Naval Service is firmly on the road to employing more capable systems to progress its ability to peer beneath the horizon, slowly building geospatial awareness. However, these limited measures fall well short of achieving a robust level of maritime domain awareness and protection. Further work is needed.

When it comes to delivering cost-effective sovereignty to the seabed, The Royal New Zealand Navy's recent procurement success with HMNZS MANAWANUI provides an example worth following.[32] Instead of looking for a brand-new hull to fill the diving and hydrographic capability gap that had been identified, the New Zealand Defence Force instead examined over 150 existing offshore subsea support vessels to find the most suitable candidate for modification. They identified the 85 metre-long MV Edda Fonn, a Norwegian multi-role support vessel built in 2003; after ten months of refit and a total bill of approx. 103 Million NZ dollars (€60m, equivalent to the cost of Ireland's newest patrol vessel, LÉ GEORGE BERNARD SHAW), New Zealand now have a vessel who's capabilities, according to defence Minister Ron Mark, represent "a domestic game changer for the South Pacific Region".[33]

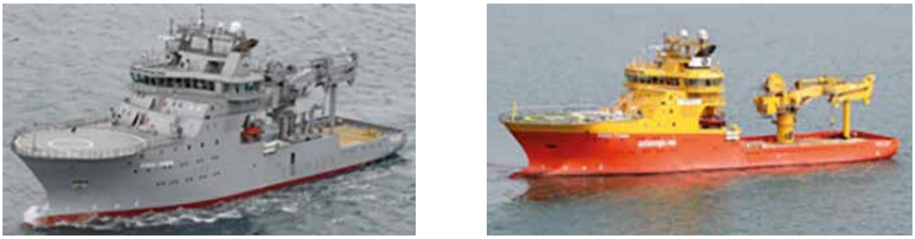


Fig 3 MV Edda Fonn, built in 2003, has been refit and repurposed as HMNZS MANAWANUI, New Zealand's most capable subsea support vessel. Source: marinetraffic.com

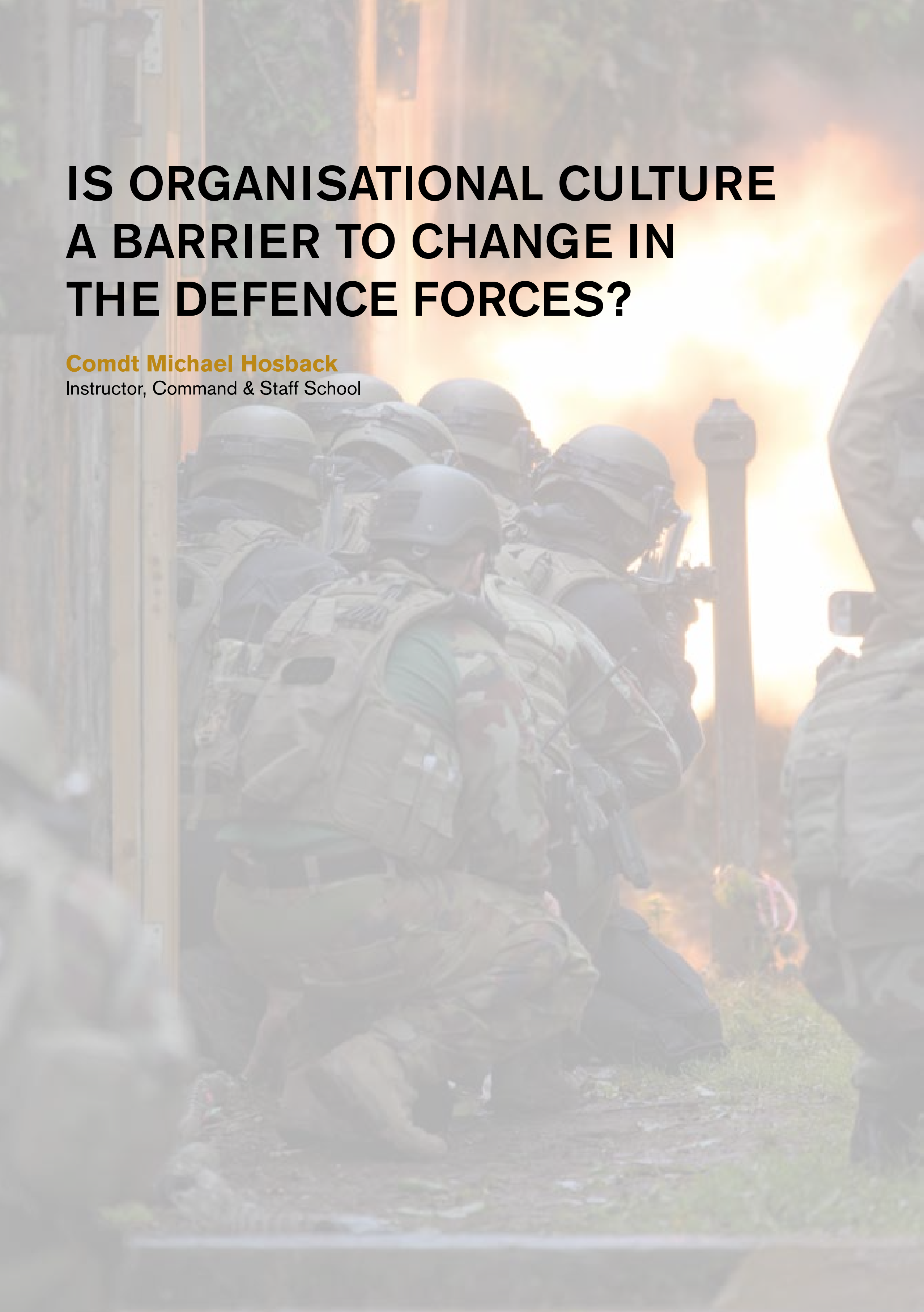
What does the future hold for Ireland's sub-sea domain? In order to support potential future assets like the Manawanui above, reviews of critical national infrastructure will be needed to address the vulnerability of our undersea cable networks and consider the adequacy of our maritime assets to counter this risk. Consideration should be given towards adopting Protection Zones in particularly vulnerable areas with a high density of subsea networks. The introduction of legislation to encourage the provision of sensors and sensor data around undersea infrastructure and along cable routes. Finally, national encouragement towards the

[32] "RNZN - Manawanui,", http://www.navy.mil.nz/mtf/manawanui/default.htm.

[33] Hon Ron Mark, NZ Minister of Defence, "*Commissioning of HMNZS Manawanui*", 07 June 2019.

adoption of modern international treaties which provide more robust protection of subsea assets in sovereign and international waters.

With issues such as Brexit threatening to change regional balances of power, it is worth remembering that the realities which made Ireland a key strategic landmark in the development of global communication technology 150 years ago, still hold true. So long as Ireland remains socially and economically married to the vital but delicate network of glass laying just offshore, it is high time we considered protecting it.



IS ORGANISATIONAL CULTURE A BARRIER TO CHANGE IN THE DEFENCE FORCES?

Comdt Michael Hosback
Instructor, Command & Staff School

Abstract

This paper is an abridged version of a Master's Thesis completed on the subject of Defence Forces (DF) organisational culture, examining whether specific elements of the DF cultural construct may be acting as a barrier to the effective integration of specialised units. Organisational culture is a complex topic, increasingly the subject of attention in terms of discussions of organisational effectiveness. Essentially culture is to the organisation as personality is to the individual. The use of Schein's model of organisational culture, widely utilised in DF Leadership Doctrine, as a framework to understand elements of culture is introduced and a cultural profile of the DF is provided (using a representative sample of 150 personnel). Analysis of the constructed culture profile indicates that there is a significant difference between the espoused values of the DF as outlined in Leadership doctrine and the beliefs held by serving personnel about the nature of DF organisational culture. The impact of this difference between espoused values and unconscious beliefs on organisational effectiveness and organisational ability to manage change and transformation are outlined. Additionally the extent to which personnel's perception of organisational values has changed over time is explored, reflecting on civil military relations and the distinct difference between climate and culture.

Introduction

The recent report of the Policing Authority on "Changing policing in Ireland" identified organisational culture as one of the key enablers of organisational change and renewal.[1] The Report suggested that one barrier to effective modernisation within An Garda Síochána (AGS) results from the impetus to change not being felt by personnel at the front line. The review also referenced the results of a recent AGS cultural audit, which indicated considerable scepticism amongst rank and file personnel towards modernisation. The Defence Forces has not to date completed a comparable cultural audit of personnel to determine their attitudes towards innovation and transformation. This is somewhat surprising given the focus in recent times on workplace climate within the organisation and the understanding that climate is a current manifestation of deeper cultural issues, topics which have been the source of considerable public and political commentary since the publication of the 2015 Climate Survey in particular.

This paper is an abridged version of a thesis completed on the topic of DF organisational culture. This topic is assessed as being particularly relevant given the focus of workplace climate discussions has mainly taken place without consideration of what constitutes DF culture. Prevailing academic opinion indicates that workplace climate change is unlikely to be successful if not informed by an appreciation of underlying culture. This would suggest that the DF, in addressing workplace climate issues, might have developed an incomplete visualisation of its current operating environment.

The paper first outlines an overview of what constitutes organisational culture. The Organisational Culture Assessment Instrument (OCAI) is then introduced and the methodology through which the OCAI was used to complete a cultural profile of the DF outlined. The results of the organisational culture profile and associated analysis are presented.

[1] Policing Authority of Ireland, Monitoring and Assessment of the measures taken by An Garda Siochána to implement the recommendations of the Garda Inspectorate Report on Changing policing in Ireland, 7th Report (Dublin: Government Printing Office, April 2019).

What is Organisational Culture?

Organisational culture describes a framework through which the personnel of an organisation interpret the interactions of their organisation and its members with other actors. Culture essentially represents to the organisation the concept that personality represents to the individual.

Cultural theorists and organisational psychologists provide numerous examples of the ways in which a comprehensive understanding of organisational culture has been used to promote effectiveness. Southwest Airlines, Amazon, Starbucks and Apple are all identified as corporate entities that have parlayed, at various times and with varying degrees of success, a positive organisational culture into a leading market position. Parr, referencing the famous "Culture Eats Strategy for Breakfast" quotation in his writing contends that "culture is a balanced blend of human psychology, attitudes, actions and beliefs that combined can create serious momentum or miserable stagnation".[2] He identifies culture as one of the most important drivers that had to be set or adjusted in order to achieve long-term success. He also outlines five separate and distinct methods through which a positive organisational culture provides significant benefits. These are by providing focus (aligning the entire company towards visions, mission and goals), motivation (building employee loyalty), connection (building cohesiveness), cohesion (encouraging co-ordination) and spirit (shaping employee behaviour at work).[3] Goffee and Jones suggest that without an effective culture a company lacks values, direction and purpose and further contend that organisational culture can be an effective way to hold an organisation together (glue) when more traditional mechanisms for integration such as hierarchies and control systems are ineffective.[4] Military organizations are interested in focus (mission accomplishment) and motivation (building loyalty and esprit de corps). They are concerned with cohesiveness, and spirit (morale) for the same reasons that their civilian counterparts prioritize the creation of a strong sense of cultural identity. The construct of a group dynamic, of a cause bigger than self and the creation of a sense of loyalty and duty are fundamental elements of military training and infuse the military way of life.[5] They are representative of the way military personnel are asked to think about the external world and how these military values and identity relate to the societies they represent. However, for military organizations, the concept of competitive advantage, and the attributes, including culture, which may combine to make the military successful over its competitors, possess a greater degree of finality than can be measured in terms of growth, market share and profitability. Murray suggests a definition of military culture as that which "represents the ethos and professional attributes, both in terms of experience and intellectual study that contribute to a common core understanding of the nature of war within military organizations".[6] He explicitly links military cultural identity to a requirement for militaries to be both introspective and learning organizations. Without these cultural attributes, he suggests that the military understanding of and appreciation of the world in which it operates and of what it is expected to achieve will be lacking.

[2] Shawn Parr, "Culture Eats Strategy for Lunch", Fast Company, Jan 2012, accessed 04 April 2018, https://www.fastcompany.com/1810674/culture-eats-strategy-for-lunch.

[3] Ibid.

[4] Rob Goffee and Gareth Jones, "What Holds the Modern Company Together," Harvard Business Review 1 (Nov-Dec 1996): 8 – 23, Accessed 25 Oct 2018, https://hbr.org/1996/11/what-holds-the-modern-company-together.

[5] Don. M Snider, "An Uninformed Debate About Military Culture", Orbis 43, no.1 (Winter, 1999):14

[6] Williamson Murray, "Does Military Culture Matter", Orbis 43, no. 1 (Winter, 1999): 27.

As the importance of culture, and specifically organisational culture, has come to receive greater recognition, a number of theories and definitions that attempt to encapsulate the concept have been put forward.[7] Schein's theory of organisational culture is utilised in this paper as a theoretical framework as it is heavily influences DF leadership doctrine. Schein defines culture as:

> *A pattern of basic assumptions that a given group has invented, discovered, or developed in learning to cope with its problems of external adaptation and internal integration, and that have worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel as related to those problems.*[8]

Schein posits a model for understanding organisational culture consisting of three cultural levels. The first and easiest discerned level is that of artefacts as they represent a physical manifestation of organisational culture. This can be as simple as the ways in which members of the group dress and speak to one another, their participation in ceremonial events and the myths and stories that members of the culture share with one another. Schein warns that while the artefact level of the cultural model is easy to observe it can be difficult to decipher and it is "especially dangerous to try and infer deeper assumptions from artefacts alone because one's interpretations will be projections of one's own feelings and reactions".[9]

The next level of culture identified by Schein is that of espoused values. Espoused values represent what the organisation says about itself to others or the way in which organisations may represent their goals and summarise their own cultures. Critically Schein contends that cultural difficulties arise when espoused values are contradictory and inconsistent with observed behaviour.

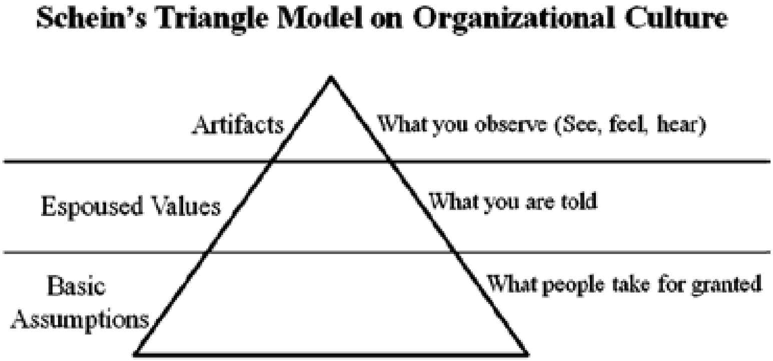

Schein's Triangle Model on Organizational Culture
Artifacts
What you observe (See, feel, hear)
Espoused Values
What you are told
Basic Assumptions
What people take for granted

Figure 1. Schein's Triangle Model on Organisational Culture[10]

The foundation of Schein's model is the presence of underlying basic assumptions. These are the elements of culture that are so ingrained in an organisation that its members take them for granted in the absence of conscious thought. Schein contends that when basic assumptions

[7] Jay M. Shafritz, J. Steven Ott, and Jong Suk Jang, Classics of Organization Theory, 8th Ed. (Boston, MA: Cengage Learning, 2015), 294.
[8] Edgar. H Schein, Organizational Culture and Leadership, 2nd Ed. (San Francisco, CA: Jossey-Bass, Inc.,1992), 12
[9] Ibid., 22.
[10] Source: Schein, On Schein's triangle Model (Research Gate, https://www.researchgate.net/figure/pn=Scheins-Triangle-Model-on-Organisational Culture_fig4_301201939, Oct 10 2018).

are strongly held in a group, members will find behaviour that is based on any other premise inconceivable.[11]

A significant utility of the model developed by Schein is its aid in understanding cultural barriers to adaptation. In organisations where basic assumptions are deep-rooted, deep anxiety can result from the development of mechanisms or viewpoints that contradict those assumptions. In order to pre-empt this, Schein argues that groups will unknowingly distort, deny, project or even falsify what is going on around them to avoid conflict with basic assumptions. This framing of a group viewpoint influenced by an organisation's culture can clearly act as a significant impediment to change and integration.[12]

Methodology

The Organisational Culture Assessment Instrument (OCAI) is a validated research method specifically designed to examine and assess organisational culture developed by Cameron and Quinn. The OCAI utilises a structured questionnaire where participants are requested to rate their organisation in a number of dimensions. These are Dominant Characteristics, Organisational Leadership, Management of Employees, Organisational Glue, Strategic Emphasis and Criteria of Success.

Data analysis enables the creation of a visual representation of the current (now) and desired (+ five years) status of an organisation's culture determining the extent of internal versus external focus and flexibility versus control. The model also use the intersection of these dimensions to group organisational culture into four specific quadrants; the *Clan* (collaborative), *Adhocracy* (creative), *Hierarchy* (controlling) and *Market* (competitive) quadrants. Each quadrant is representative of different elements of organisational culture. If an organisation demonstrates a tendency to be hierarchical in nature for example then clear lines of authority, standardised rules and procedures and control and accountability mechanisms are valued as keys to success. Effective leaders in this type of environment will be good coordinators and organisers who will prioritise a smooth running organisation. Formal rules and policies are valued. Conversely the Adhocracy culture is identified as a dynamic, entrepreneurial and creative workplace. Personnel are risk takers and leadership is visionary, innovative and oriented. Commitment to experimentation and innovation are high. The indications provided by the competing values framework for organisational effectiveness and culture are outlined at Figure 2 below.

[11] Ibid, 25.
[12] Schein, Organizational Culture and Leadership, 22.

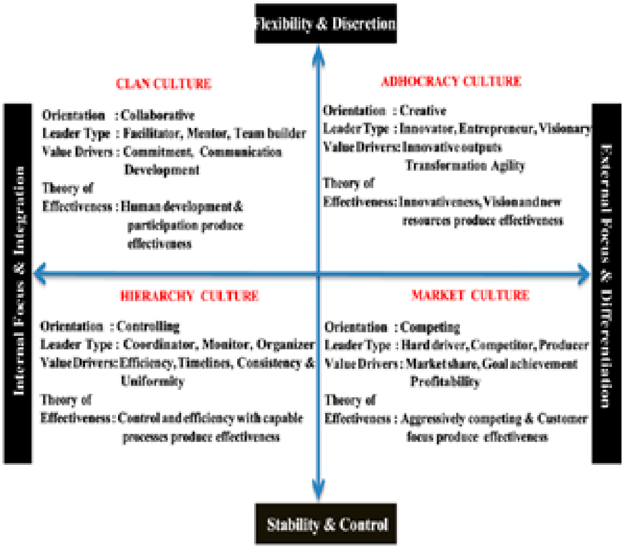

Flexibility & Discretion
CLAN CULTURE
Orientation : Collaborative
Leader Type : Facilitator, Mentor, Team builder
Value Drivers : Commitment, Communication Development
Theory of Effectiveness : Human development & participation produce effectiveness
ADHOCRACY CULTURE
Orientation : Creative
Leader Type : Innovator, Entrepreneur, Visionary
Value Drivers: Innovative outputs Transformation Agility
Theory of Effectiveness: Innovativeness, Vision and new resources produce effectiveness
HIERARCHY CULTURE
Orientation : Controlling
Leader Type : Coordinator, Monitor, Organizer
Value Drivers: Efficiency, Timelines, Consistency & Uniformity
Theory of Effectiveness: Control and efficiency with capable processes produce effectiveness
MARKET CULTURE
Orientation : Competing
Leader Type : Hard driver, Competitor, Producer
Value Drivers : Market share, Goal achievement Profitability
Theory of Effectiveness : Aggressively competing & Customer focus produce effectiveness
Internal Focus & Integration
External Focus & Differentiation
Stability & Control

Figure 2. Competing Values Framework of Organisational Culture[13]

Additionally, an example of a unique organisational culture plot indicated by the OCAI is presented at Fig 3. The representative model demonstrates the responses of US Army personnel during research conducted into possible barriers to effective professional military education resulting from organisational culture.

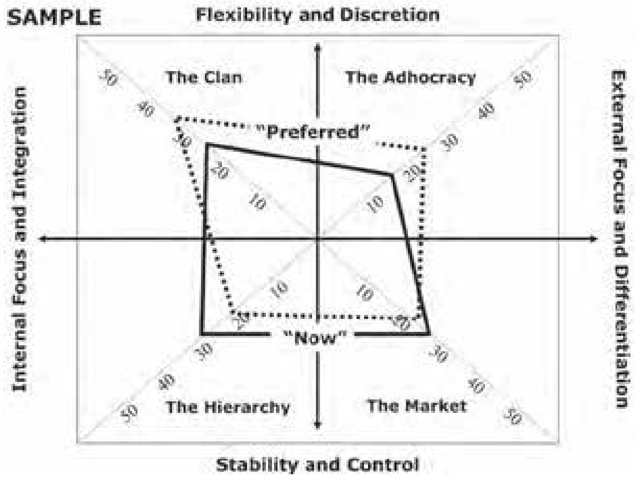


Figure 3. Representative Organisational Culture of the US Army[14]

[13] *Source*: Cameron and Quinn, *Competing Values Framework of Organizational Culture* (Research Gate, https://www.researchgate.net/figure/Competing-Values-Framework-adapted-from-Cameron-Quinn-2011_fig1_317592354, April 4, 2019).

[14] Source: Pierce, *Is the Organizational Culture of the US Army Congruent with the Professional Development of its Senior Level Officer Corps?* (Global Security, https://www.globalsecurity.org/military/library/report/2010/ssi_pierce.pdf, January 15, 2019), page 57.

A culture model of the Irish Defence Forces and its implications

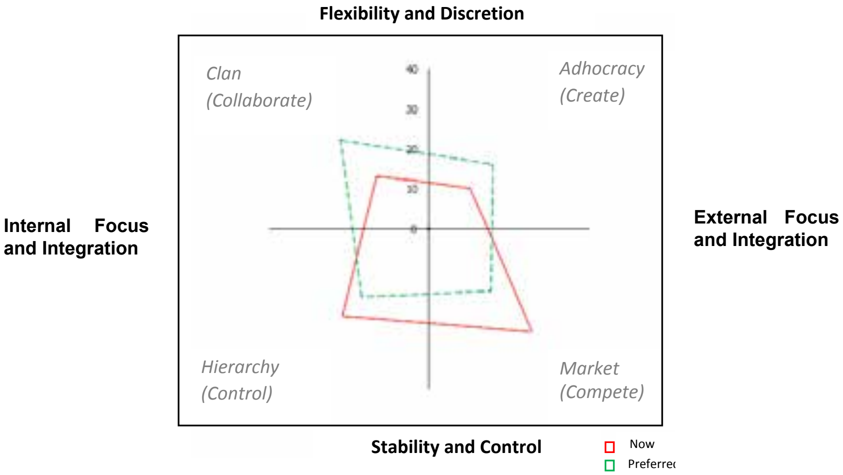


Figure 4.Organisational Culture Model Irish Defence Forces[15]

The study population for quantitative analysis of the DF population was comprised of one hundred and fifty service personnel (one hundred and fifty being identified by Cameron and Quinn as a statistically significant sample size representative of organisational thought). This sample size is comprised of a representative body from all ranks up to that of Commandant thereby allowing the computation of differences in value scores to be calculated across the rank structure. The sample body was comprised of personnel with between two and twenty years of service in the DF.Figure 4 above represents the results of the OCAI distributed to members of the DF as part of this study. The 'now' line indicates respondent's current assessment of the prevailing culture of the DF. The 'preferred' line is what those same respondents indicated that they would like the cultural construct to be in five years. The same data is presented in Table 1 below.

Numeric Values Irish Defence Forces Culture Model				
Culture Type	Clan	Adhocracy	Market	Hierarchy
Now Value	18.65	14.43	36.24	30.66
Preferred Value	31.27	22.70	20.96	24.05

Table 1 – Numeric Values Irish Defence Forces Culture Model[16]

The model indicates that the current membership of the DF perceives the culture of their organisation to be imbalanced and weighted in favour of a *Market* type profile. This cultural dominance indicates that personnel perceive of themselves as being members of a culture that is driven primarily by the achievement of goals, is tough and demanding on personnel and is focused on results. It should be noted, that the term *Market* is not synonymous with the marketplace, as may be assumed, but refers to the type of organisation that is oriented towards

[15] Michael Hosback, "Is the Organisational Culture of the Irish Defence Forces acting as a barrier to the effective integration of Special Operations Forces" Master's Thesis, Fort Leavenworth, Kansas, (2019).
[16] Ibid

responsiveness to the external environment instead of internal affairs. The leadership type associated with a Market culture is one of hard driving competitiveness, highly focused on satisfying the demands of the external environment. Participants also indicated a significant perception that the DF demonstrates a *Hierarchical* type organisational culture. The hierarchical environment is one in which clear lines of decision-making, authority, standardised rules and procedures, control and accountability are valued as the keys to success. Day to day actions tend to be governed by procedural mechanisms and effective leaders are coordinators and organisers. In the long term, the goals of the organisation are predictability and stability. Consensus in the hierarchical organisation is achieved by adherence to rules and policies.

The extent to which these results are demonstrated across the rank structure are outlined below.

Numeric Values Irish Defence Forces Culture Model Cross Rank Comparison

Culture Type	Clan	Adhocracy	Market	Hierarchy
Corporal Rank				
Now Value	16.67	15.44	35.85	32.01
Preferred Value	33.00	24.68	19.83	22.47
Captain Rank				
Now Value	20.05	15.85	34.66	29.41
Preferred Value	30.75	22.16	22.62	24.45
Commandant Rank				
Now Value	16.78	11.30	36.85	35.05
Preferred Value	28.78	23.48	21.65	26.07

Table 2 – Numeric Values Irish Defence Forces Culture Model Cross Rank Comparison[17]

Analysis and Conclusions

Analysis

The degree to which survey participants identify the dominant cultural characteristic of the organisation to be that of achievement of externally mandated goals is significant. The magnitude of *Market* rating is almost 2.5 times greater than the *Adhocracy* rating and 2.0 times greater than the *Clan* rating. Similarly, the *Hierarchy* rating is 2.2 times greater than the *Adhocracy* rating and 1.6 times greater than the *Clan* rating. The low cultural strength of the Clan score is notable and indicates that personnel feel that team and employee involvement and commitment of the organisation to employees are not highly valued in the current cultural construct.

[17] Hosback, Op Cit.

Respondents consistently rated the *Clan* and *Adhocracy* culture types as least congruous with their perception of the organisations current profile. The extent to which these results are reflected, with only slight numeric deviation, across the rank structure are also significant. They suggest that the same perception, possibly accepting slight change reflecting experience, is consistent across the population, at least up until the rank of Commandant.

Given the DF espousal to practice a mission command type leadership doctrine and to be a learning organisation, these results are discouraging. The espoused culture of the DF (the learning organisation) is best represented by the *Adhocracy* culture type, one in which innovation and transformation are encouraged. This suggests that there is a dissonance between what the organisation suggests its values are and what surveyed personnel believe those values to be in actuality.

The results of this analysis suggest that personnel hold the opinion that the leadership of the defence organisation values the fulfilment of externally mandated requirements at the expense of personnel development. They consider that the organisation is primarily concerned with achieving mandated tasks, through rigid control structures and possesses a management style which is characterised by strict adherence to regulation and which contravenes the DF espoused values. The results indicate that the capacity for building a cohesive organisation characterised by effective teamwork and built on trust, as espoused by DF doctrine, is currently inhibited in the organisations cultural construct.

Cameron and Quinn have indicated that "discrepancies between the 'now' profile and the 'preferred profile' of between five and ten points usually indicate the need for a substantial culture change effort".[18] Indeed, in the representative culture model of the US Army outlined at Figure 3 discrepancies in perceived versus espoused culture indicated in the results were the impetus for substantial cultural change initiatives. It is apparent that in this case a major culture change initiative was initiated in a situation where the score discrepancies were not as stark as that displayed in the model developed here for the DF.

Numeric Values US Army Culture Model				
Culture Type	Clan	Adhocracy	Market	Hierarchy
Now Value	21.17	11.77	37.95	28.84
Preferred Value	28.97	24.55	27.08	19.34

Table 3 – Numeric Values Irish Defence Forces Culture Model Cross Rank Comparison (Source: Pierce, 2019, p.57)[19]

Pierce's findings in the above referenced Table and associated research are that "the characteristics of the Army professional culture are not supportive of long term environmental adaptability, flexibility and innovation".[20] The current failure to acknowledge the requirement for cultural understanding, evidenced by lack of existing analysis, farther supports the contention of incomplete situational awareness.

[18] Kim S. Cameron and Robert E. Quinn, Diagnosing and Changing Organizational Culture: Based On the Competing Values Framework, 83.
[19] James G. Pierce, "Is the Organizational Culture of the US army Congruent with the Professional Development of its Senior Level Officer Corps?" (Letort Papers, US Army War College, Strategic Studies Institute, Carlisle, PA, 30 September 2010), 57.
[20] Ibid., 52.

Conclusions

The current organisational profile of the DF as indicated by this research is inconsistent with the organisation's espoused values as enshrined in DF leadership doctrine. The cultural model presented by this analysis indicates that of four specifically identified cultural types outlined, the current profile of the DF is least like that which the organisation professes to possess; the learning organisation. The research suggests that there is a dissonance between the espoused values of the DF and the unconscious beliefs of members. It also indicates that the current organisational climate of the DF is not disposed towards innovative behaviour. This is a negative outcome for the DF as innovation and flexibility are two key characteristics it has identified as necessary to succeed in the future operating environment.

Low levels of group cohesion and morale indicated by the 2015 climate survey support the accuracy of a low clan culture organisation profile for the DF as evidenced in this research. When considered in conjunction with the work of O'Brien (2013) who asserted that personnel do feel an affinity towards DF values and feel that they are indicative of DF culture this would suggest that the foundations of DF organisational culture are being eroded over time and specifically that significant erosion has taken place since 2013.[21] The Climate Survey revealed large levels of dissatisfaction with life in the DF, particularly since the reorganisation and downsizing in 2012 and the significant adjustments to pay, conditions and structure as a result of the prevailing economic environment. This dissatisfaction has been characterised by the significant and operationally damaging loss of personnel in recent years. The dissonance between espoused values and perception of personnel surrounding organisational culture are suggestive of an increasing disconnect between defence management and the personnel of the DF, reflected in contemporary commentary.

A great deal of time and energy has been invested in recent years in the investigation and classification of workplace phenomenon in the DF. Engagement in these areas is the subject of ongoing consultation and revision. Training practices and interpersonal relationship policies in the DF continue to be subject to review and effective oversight. It is arguable however that the DF focus on climate without an effective appreciation of the established culture of the organisation is erroneous. Attempts to address work place climate change are unlikely to be successful in the short term as a result of a lack of awareness of cultural underpinnings of organisational frames of reference. Climate is more easily measured than culture, which perhaps explains why organisations have a tendency to engage in climatic introspection without properly understanding the unconscious belief system that affects personnel. This research suggests however that despite associated difficulties there is a requirement for the DF to be more cognisant of the effect of organizational culture on workplace climate. The lack of understanding of a common cultural basis for the DF is unfortunate given the widely accepted levels of organisational culture as developed and postulated by Schein and acknowledged by the DF in leadership doctrine. There are measures that the DF can take however to address the perceived disconnect between espoused values and the beliefs of personnel. It is noteworthy that the survey results indicated that personnel expressed a noted desire to move towards a learning organisation culture in the medium term and expressed a preference for an organisational culture more closely reflective of espoused DF values. The key takeaway for

[21] Darragh O'Brien, "Culture Eats Strategy for Breakfast but what is the Prevailing Culture of Óglaigh na hÉireann" (Master's Thesis, National University of Ireland, Maynooth, 2013).

the DF in this regard that a considered approach to cultural change supported by a more wide ranging cultural audit and examining the existing reasons for the differences between espoused values and beliefs of personnel is likely to contribute to effective change.

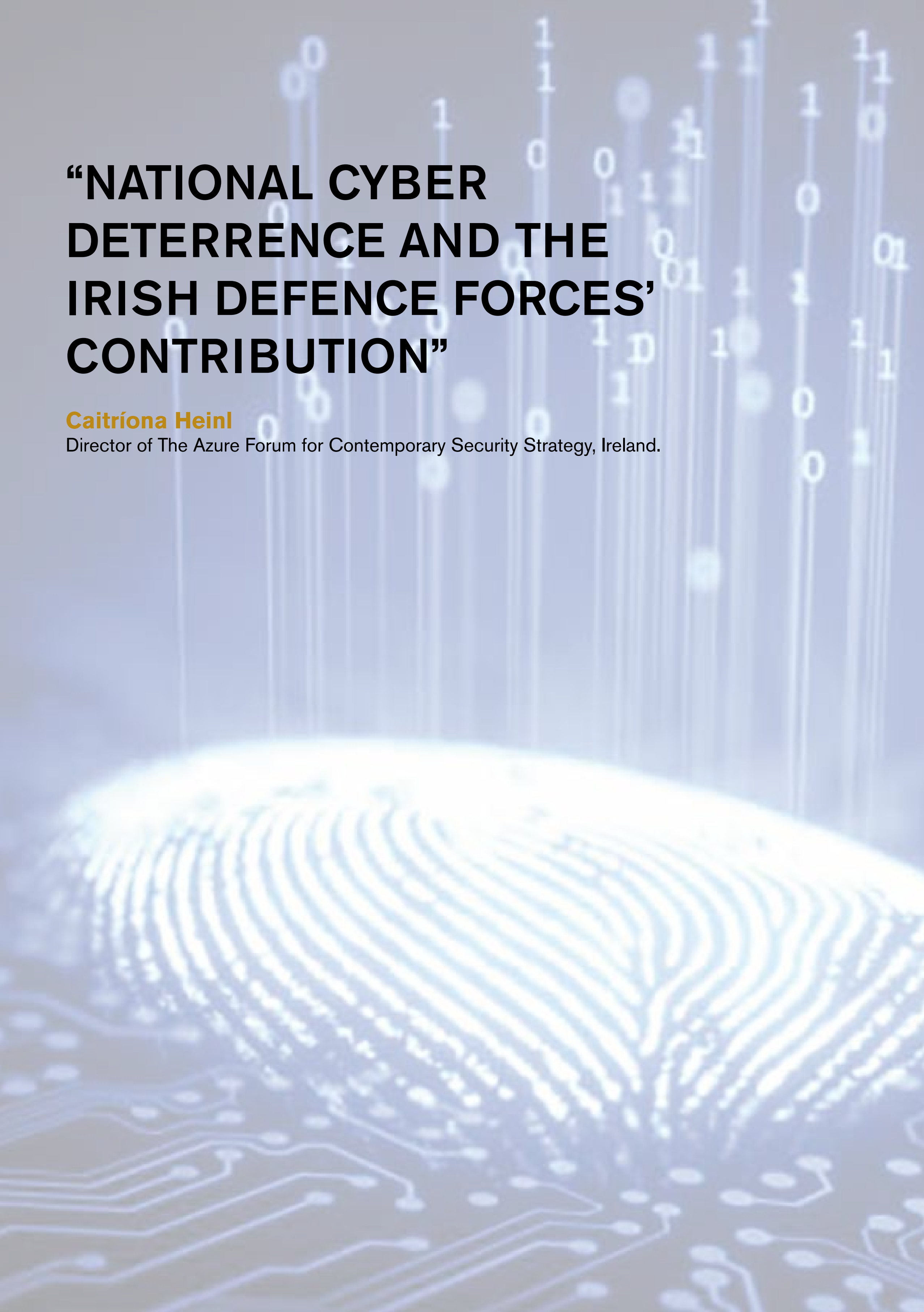
Previous studies of DF organisational culture have recognised the importance and impact civil military relations in this area. Despite this knowledge it is arguable the DF has failed to effectively educate their personnel in the importance of the civil-military relationship and in particular the role and space for dissent or disagreement in the civil military sphere. Since the time of writing of the two previous theses specific to the DF referenced here (O'Brien in 2013 and Crummey in 2014 respectively),[22] the findings of this research indicate that ambivalence surrounding the status of the military, on the part of military personnel, may be a contributing factor to an undermining of military culture in Ireland. It is assessed as probable that the current construct of the defence organisation, which limits military control of the levers of organisational innovation (limited control of finance, restricted ability to restructure) may be acting as an impediment in this regard and contributing to the impression of cultural dissonance amongst serving personnel. Effective climate and cultural change measures are both frustrated by the relative inability of DF leadership to take minimal ownership of the levers of organisational change.

Given the current status of discourse surrounding resourcing of defence in the Irish model, it is not speculative to state that lack of understanding of defined roles has impacted on the operational capability of the DF. It is also apparent that the appreciation of DF personnel for traditional values is likely to deteriorate further unless these issues are addressed.

[22] Declan Crummey, "Exploring Dissent in Civil Military Relations" (Master's Thesis, National University of Ireland, Maynooth, Ireland, 2014).

“NATIONAL CYBER DETERRENCE AND THE IRISH DEFENCE FORCES’ CONTRIBUTION”

Caitríona Heinl
Director of The Azure Forum for Contemporary Security Strategy, Ireland.



Abstract

There is a significant rethinking of deterrence and cyber deterrence being conducted in many countries. This article will explore how other countries and military forces are now approaching these questions with a view to adapting such thinking to suit the Irish national security context. New national security strategies and second-generation cyber strategies must now integrate such developments.

If it is expected that we will see even closer and more rapid integration of civil and military agencies in the deterrence of and response to cyber aggression, how could (and should) this be developed in Ireland? In the wake of tackling contemporary cyber aggression and grey zone conflict during peacetime, the author will explore how both caution and willingness to bring about constructive change are beginning to be exercised in other states (and by extension may need to be exercised in Ireland) when questioning, and potentially modifying, the traditional role of military for 21st Century risks.

Introduction

Even where adverse state activity within the cyber sphere in Ireland may not be immediately evident, it would make little sense to not examine how trends elsewhere could unfold were they to occur in the State by identifying appropriate responses and mitigation measures for persistent and multi-faceted cyber aggression.[1] Foreign states' ability to impact Irish security in the cyber sphere will continue to be dependent upon the Irish state's capacity and continuing willingness to take additional actions to prevent, reduce, deter and respond to espionage activities as well as malevolent and hostile state activity. Such deterrence is traditionally understood to work by conveying the message that costs – including political, economic, diplomatic and strategic - will be imposed on a given action, either by making success more difficult or by threatening a punitive response, so that a malevolent actor will likely consider the benefits of action outweighed by the costs or punishment and thus choose not to act.[2]

A simple understanding of cyber deterrence is laid out within the EU's latest cyber strategy whereby effective deterrence is achievable if a framework of measures are put in place that are both credible and dissuasive.[3] The EU strategy argues that perpetrators who do not fear reprisal will only continue their activities unless the chances of being caught and punished by joint diplomatic or political response are increased. Ireland is not considered immune and there is a belief that groups linked to other states are in Ireland and carrying out operations in the State.[4] Stronger, coordinated cross-governmental measures and responses will continue to be needed nationally to address present-day cyber aggression – and like the EU strategy lays bare, these steps must be both credible and dissuasive. At the time of writing, the still applicable Irish National Cyber Security Strategy dating back to 2015 does indeed explain that the strategy presents a cross-government framework for ensuring cyberspace remains safe, secure and reliable with an emphasis on task-sharing and building trust between stakeholders.[5]

[1] This adapted article comprises thinking based on a number of "think pieces" and speaking engagements by the author throughout 2019. These include: "Food for thought: The cybersecurity landscape and role of the military", 8 May 2019; and "Russia and China – Their impact on Irish security from a cyber perspective", 30 May 2019.
[2] Wilton Park, "Military operations in cyberspace", 5-7 September 2018.
See also HM Government, "National Cyber Security Strategy 2016-2021", 2016, 47.
[3] European Commission and High Representative of the Union for Foreign Affairs and Security Policy Joint Communication to the European Parliament and the Council, "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", 13 July 2017, 12.
[4] Anonymous speaker, "Cyber Security Transatlantic Policy Forum", Killarney Economic Conference, 10 May 2019.
[5] Department of Communications, Energy & Natural Resources, "National Cyber Security Strategy 2015-2017", Government of Ireland, 2.
At the time of writing, the second cyber strategy is due to be published.

The strategy further observes the changing nature of these technologies, rightly stating that flexibility will be needed for the strategy's implementation in an adaptive manner.[6]

Nonetheless, experts are scrambling to unpack the multi-level characteristics of cyber conflict that include ideological, policing, security and economic dimensions – astutely described as a humbling experience where we are advised to ideally exercise intellectual, political and strategic humility in this space.[7] The national security communities and militaries of technologically advanced democracies are still trying to better understand the character and implications of the phases of potential conflict in cyberspace - our understanding of cyberspace as an environment, of conflict in that environment, and of the military role in such conflict is still work in progress.[8] It is thus safe to conclude that the military role in advanced democratic states' endeavours, including Ireland, to deter and manage the use by state or non-state actors of contemporary and future cyber capabilities needs both significant strategic refinement and investment.

Experts now ask, for instance, what exactly the role of the military is where there are several types of persistent cyber activity such as espionage, attack, influence campaigns, and races to acquire strategic future capabilities. What is the role of the military during "unpeace" defined by Lucas Kello in his recent book as "mid-spectrum rivalry lying below the physically destructive threshold of interstate violence but whose harmful effects far suRPAS the tolerable level of peacetime competition and possibly even of war". In other words, how should we analyse and manage military operations that are in fact taking place in cyberspace?[9] This begs the deeper question as to how the Irish government should now approach cyber deterrence where the nature of traditional deterrence is already evolving – military doctrine is beginning to recognise that it is "no longer a defensive or semi-passive theory based on conveying intent and capability; instead, it now has to involve active measures as part of a constant conflict below the traditional threshold of what used to be called war".[10]

This article argues that a number of steps can be taken to better enhance Ireland's cyber resilience, deterrence, and response in the 21st Century. This includes work that continues to strengthen cyber resilience to reduce vulnerability, and to allow government freedom of action for responding to and preventing future malevolent activity. These steps, which are described in more detail below, include the following actions: (1) Continue to enhance cyber resilience as part of deterrence by denial; (2) Increase all-source intelligence; (3) Align cyber deterrence alongside national deterrence frameworks; (4) Unpack and adapt contemporary military thinking on 21st Century cyber risks; (5) Recognise the Defence Forces' workforce as a critical cyber asset; (6) Adapting EU frameworks at national level for response to malicious cyber activities; (7) Continue to increase the State's international action and engagement; and (8) Continue efforts to protect Ireland's reputation vis-à-vis surveillance and cybersecurity issues.

[6] Department of Communications, Energy & Natural Resources, "National Cyber Security Strategy 2015-2017", Government of Ireland, 3.
[7] Wilton Park, "Military operations in cyberspace", 5-7 September 2018.
[8] Ibid., 5-7.
[9] Ibid., 5-7.
[10] Ministry of Defence, "Deterrence: the Defence Contribution", Joint Doctrine Note 1/19, UK Government, February 2019.

Continue to enhance cyber resilience as part of deterrence by denial

Without citing each of the measures laid out within the Irish cyber strategy that aim to enhance cyber resilience, the strategy already identifies tangible ways to enhance resilience on an ongoing basis. Cyber resilience is understood to be the ability to prepare for, respond to and recover from cyber incidents where traditional cybersecurity measures are no longer perceived to be sufficient to protect against persistent activity.[11] This is important given that enhanced cybersecurity and resilience are in essence "a means of deterring attacks that rely on the exploitation of vulnerabilities".[12] In other words, resilience is a key pillar of any deterrence strategy.[13]

By continuing the State's work to strengthen cyber resilience, this not only helps to reduce vulnerability; it further supports the Government's need for freedom of action and the confidence to sometimes take unfavourable cyber and non-cyber related positions in relation to other states. The Government would therefore be enabled to respond to unacceptable behaviour and to possibly also prevent future malevolent state activity where the State's own vulnerability to possible retaliatory responses in the cyber sphere is reduced. For example, where Irish decision-makers may decide to expel diplomats or take other actions in relation to cyber and non-cyber state activity, then consistently strong cyber resilience will be required as a factor in this decision-making process to buffet against possible cyber retaliation. Possible examples of this quandary come to mind in the context of the discussion in 2018 about alleged Russian involvement in the chemical incident in Salisbury involving a toxic chemical and poisoning of three people where a review was then held on the presence and activities of Russian diplomats and agents (which was ultimately followed by expulsions).[14] Or more recent reports about the potential for Chinese activity at Leinster House where queries were made about the installation of surveillance cameras by a Chinese state-backed company.[15] This means that the State's so-called "cyber house" must be in good shape to support, for example, Irish leaders' decisions and high-level statements where there is an intention to signal that the State will not be bullied.[16]

Increase all-source intelligence

The presence of foreign actors on systems must naturally be taken very seriously, perhaps more seriously than heretofore given the nature of the blurred lines between cyber espionage and disruptive capabilities where actual intentions can often be difficult to decipher. Because of the distinctive nature of the cyber sphere, this means that it may now bring about a need for more debate in the Irish context about the greater need for all-source intelligence such as sigint,

[11] ITGovernance.co.uk, "What is cyber resilience?", Accessible at: https://www.itgovernance.co.uk/cyber-resilience.

[12] HM Government, "National Cyber Security Strategy 2016-2021", 2016, 47.

[13] Ministry of Defence, "Deterrence: the Defence Contribution", Joint Doctrine Note 1/19, UK Government, February 2019.

[14] See also: Elaine Loughlin, "Ireland extremely vulnerable to cyber attacks from Russia", 26 March 2018, https://www.irishexaminer.com/ireland/ireland-extremely-vulnerable-to-cyber-attacks-from-russia-468749.html: "Michael Murphy has raised serious questions around this country's capacity to deal with any Russian retaliation if Taoiseach Leo Varadkar orders an expulsion of diplomats….The former deputy director of military intelligence said we are "naive" in relation to intelligence and espionageand could face attacks including the cutting of electricity or water in the event of actions deemed unfriendly
towards Russia."

[15] Hugh O'Connell, " Chinese cameras in Leinster House spark espionage concerns", The Business Post, 28 April 2019.

[16] See Niall O'Connor, Irish Mirror, 23 March 2018, https://www.irishmirror.ie/news/irish-news/russian-hackers-already-accessed-hse-12242336: In relation to Russian activity last year, see the commentary "When you step in to meet it the chances are it will decrease. What Varadkar is doing is saying find some other small state to bully."

osint, and humint (including foreign capabilities) in combination with technical attribution where technical attribution alone is not sufficient. This situation is currently exacerbated given concerns that the increasing use of publicly and commercially available cyber tools is increasing the volume of unattributed cyber activity globally and the risk of misattribution and misdirected responses by both governments and the private sector is higher.[17] In other words, cyber challenges should likely now be a forcing function to bring about wider changes in the Irish national security apparatus.

Align cyber deterrence alongside national deterrence frameworks

It would seem that a nations’ wider deterrence framework (which is often relayed by way of a national security strategy) should ideally support and establish stronger strategic thinking on deterrence in cyberspace and take the evolving geopolitical and cyber threat landscape into account. The current Irish cybersecurity strategy, by no fault of its own, must draw on disparate documents such as the 2015 White Paper on Defence. The upcoming cybersecurity strategy must likely draw on a number of other policy documents too. While this is likely a challenge for other security fields in the Irish context, there is clearly a need for a higher order strategic overlay for national security to establish better deterrence in cyberspace. The difficulty in this case is that Ireland does not yet have a national security strategy. While a national security strategy is expected to be developed in the near future under the mandate of the National Security Analysis Centre, this will likely occur after the expected release of the next national cybersecurity strategy in 2019. Consequently, the new cyber strategy could include an objective that lays out future intentions that next generation cyber strategies will complement the national security strategy (or strategies) in the interests of stronger deterrence in cyberspace.

Unpack and adapt contemporary military thinking on 21st Century cyber risks

In the Irish context, general emergency planning processes in the State lie with the Principal Response Agencies (including an Garda Síochána, the Health Service Executive and the Local Authorities), Government Departments and other agencies overseen by the Office of Emergency Planning within the Department of Defence and the Government Task Force on Emergency Planning, chaired by the Minister for Defence and the National Framework for Emergency and Crisis Management in Ireland aims to foster national resilience in the face of crises.[18] The Department of Communications, Climate Action and Environment operates as the lead Government Department for emergency situations relating to the failures of, or attacks on, Information and Communications Technologies, and will operate in a secondary role to other Departments in cases where incidents may have a cybersecurity dimension.

Although the current Irish cyber strategy includes an objective to build capacity across public administration and the private sector to engage fully in the emergency management of cyber incidents, the current shortfall of military personnel in the field of cyber does not seem to be meeting this objective. Other objectives expected to be met under the current cyber strategy

[17] Daniel R. Coats, Director of National Intelligence, “Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community”, Senate Select Committee on Intelligence, 29 January 2019.
[18] Department of Communications, Energy & Natural Resources, “National Cyber Security Strategy 2015-2017”, Government of Ireland, 7.

include civil-military cooperation whereby the Irish Defence Forces continue the strong culture of cooperation between the National Cyber Security Centre (NCSC) and Defence Forces in areas such as development of technical skill sets, technical information sharing and exercise participation. The Defence Forces must also maintain a capability in the area of cybersecurity to protect its own networks and users. Moreover, a Service Level Agreement was due to be formalised with the Department of Defence to include a mechanism for sharing technical expertise in the event of a national cyber incident or emergency. Specifically, two members of the Defence Forces are generally seconded to NCSC (albeit dependent on the Defence Forces having two officers to second which seems a challenging ask given the current exodus of Defence Forces' officers).[19] In July 2019, the Defence Forces' internal cybersecurity unit was shut down because of a lack of resources and qualified staff, and they are no longer in a position to provide staff to NCSC.[20]

In any case, the NSCS maintains close cooperation with the Defence Forces and An Garda Síochána on national security issues with this secondment arrangement for both entities.[21] The 2015 Defence White Paper also observes that the Department of Communications has lead responsibilities relating to cybersecurity and the primary focus of the Department of Defence and Defence Forces will remain the protection of Defence networks, but in emergency situations, once Defence systems are supported, they will provide support to the CSIRT-IE team. Nevertheless, it seems uncertain that the Irish Defence Forces can could currently assist in past months in the event of a significant cyber crisis or national cyber-attack given the media reporting of the more recent standing down of the Defence Forces' cybersecurity unit. Moreover, the ability to routinely and effectively defend and protect the Defence Forces' networks from cyber-attacks and intrusions, which is regarded as an essential capability that must be retained and developed, must now beshould have been more seriously called into question at the highest levels if this reporting is accurate.[22]

Notably, these objectives do not seem to include advanced military strategic thinking on cyber matters. These developments in Ireland seriously call into the question the ability of the State to implement a credible and dissuasive deterrence framework with a defence contribution. This is particularly concerning where other important questions about the role of military in these types of contemporary "conflict" and "unpeace" should be addressed.[23] Such questions that are currently being explored in other advanced economies include the following: (1) Is the role of military to fight in the traditional sense of an action/reaction struggle with an adversary? The latest United States Department of Defense (DoD) cyber strategy posits, for instance, that its military's ability to fight and win wars in any domain, including cyberspace, is a foundational national security requirement to deter aggression including cyber-attacks – it will now "defend forward" to halt or degrade cyberspace operations targeting the DoD which could be construed as pre-emptive behaviour. Nonetheless, experts are continuing to unpack the meaning of such new strategies; (2); Is the military's task to contain hostile actions in cyberspace and to prevent them spreading to and compromising military activity in conventional domains like land, sea, air and space?; (3) Should this defensive function be extended to society more broadly, with military tasked not just to defend their own networks and platforms but to also ensure the

[19] White Paper on Defence, Government of Ireland, August 2015, 43.
[20] John Mooney, "Lack of staff stops army cyber-security team", The Sunday Times, 7 July 2019.
[21] Department of Communications, Climate Action & Environment, "National Cyber Security Strategy Draft Public Consultation", March 2019, 3.
[22] White Paper on Defence, Government of Ireland, August 2015, 63.
[23] Wilton Park, "Military operations in cyberspace", 5-7 September 2018.

resilience of society's critical infrastructure as a whole? Again, the U.S. DoD is now working to defend, when directed, non-DoD critical infrastructure and Defense Industrial Base entities. It will work (including by defending forward) to pre-empt, defeat or deter malicious cyber activity targeting U.S. critical infrastructure that could cause a significant cyber incident "regardless of whether that incident would impact DoD's warfighting readiness or capability"; (4) Are military-related activities such as cyber defence and resilience the most that can be expected of military deterrence in cyberspace, or should the role of military be more organisational than operational? For example, should military have a liaison and coordination function intended to ensure integrated cross-governmental and intra-alliance responses?; and (5) Is there a need, as laid out in the UK's national cyber strategy, to improve the focus of intelligence agencies, law enforcement and military in coordination with international partner agencies to identify, anticipate and disrupt hostile cyber activities by obtaining pre-emptive intelligence on the intent and capabilities of malevolent state and non-state actors?[24] The U.S. DoD also alludes to the need to increase "bi-directional" information sharing to advance mutual interests with allies and partners.[25]

What is certain from recent expert reports is that militaries cannot effectively undertake this analysis on their own and they must ideally be conducted as part of a "comprehensive, integrated civil-military approach to conflict in cyberspace". Nor is cyberspace seen to be exclusively a military responsibility. Instead, it is recommended that there should be effective coordination of civil-military capacity if cyber activities – of all kinds and at whatever levels – are to be deterred and defeated. It is argued that military operations in cyberspace should be fought as part of a comprehensive integrated civil-military approach in which civil and military efforts are interdependent and thus more effective. A recent Wilton Park report on military operations, which draws on the findings of key thought leaders and government representatives, emphasises that civil-military cooperation is no longer optional and it is expected that we will see even closer and more rapid integration of civil and military agencies in the deterrence of and response to cyber aggression. This concept is known as fusion doctrine in the United Kingdom whereby UK military operations in cyberspace should be seen as only one element of a full spectrum cross-governmental strategic approach so that political leadership can at all times receive advice from military commanders as to what military operations can and cannot achieve in cyberspace. However, experts' contributions in the Wilton Park report accept that deterrence of cyber-attacks that constitute use of force seems to remain relatively straightforward insofar as it comprises the traditional combination of denial and punishment. However, it is more challenging where malicious activity falls below the threshold of the use of force, thus calling for more nuanced positions, including during peacetime.

The EU also considers that it is well placed to promote synergies between military and civilian efforts given the blurring lines between cyber defence and cybersecurity and the dual use nature of cyber tools and technologies as well as the very different EU Member State approaches.[26] While the United States DoD is now tasked to respond to cyber-enabled campaigns that erode U.S. military advantages, threaten its infrastructure and reduce its economic prosperity. It will work to expose, disrupt and degrade cyber activity threatening U.S. interests, strengthening the

[24] See the United Kingdom's approach: HM Government, "National Cyber Security Strategy 2016-2021", 2016, 28.
[25] United States Department of Defense, "Summary: Department of Defense Cyber Strategy 2018", September 2018, 2.
[26] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament and the Council, "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", 13 September 2017.

cybersecurity and resilience of key potential targets and working closely (thus expanding DoD cyber cooperation) with other departments and agencies, industry and international partners.[27]

Recognise the Defence Forces' workforce as a critical cyber asset

It is already recognised in the 2015 White Paper on Defence that the key requirement to maintain the capability to effectively defend Defence Forces' networks is for personnel with appropriate cybersecurity skills sets – this was already considered difficult to maintain in 2015 given the transferability of such skills to the business environment.[28]

While the National Cyber Security Centre's primary focus is on securing government networks, assisting industry and individuals and securing critical national infrastructure, thought leaders and seasoned practitioners conclude that since future crises will likely include a cyber component and the military will not only likely be a target but also be required to contribute to national security and defence in cyberspace. Therefore, the Defence Forces will need enough highly trained practitioners for cyber defensive and counter-offensive operations. The U.S. DoD cyber strategy captures this point succinctly by explaining that its "workforce is a critical cyber asset". At a time when defence budgets are constrained and talent can be attracted to the more profitable private sector, this point is critical. EU strategies similarly recognise this very important skills gap in cyber defence.[29] The Cyber Education Training Evaluation and Exercise Platform at the European Security and Defence College has subsequently been established as one way to address this need for cyber defence training and education across EU Member States. While this initiative is laudable, it is currently light years behind other initiatives such as the NATO Cooperative Cyber Defence Centre of Excellence. The United Kingdom, for its part, is still developing its own Defence Cyber Academy for cyber training and exercise across its Ministry of Defence and wider Government, addressing specialist skills and wider education.[30] This includes developing opportunities for collaboration in training and education between government, the Armed Forces, industry and academia.

Adapting EU frameworks at national level for response to malicious cyber activities

Given Ireland's membership of the EU and close working relationship on cyber-related matters, additional initiatives to examine for possible adaptation at national level in Ireland could include response frameworks such as the EU's so-called cyber diplomacy toolbox. The Irish government already considers the EU as having taken a particularly coherent and comprehensive approach.[31] The toolbox is a framework for a joint EU diplomatic response to malicious cyber activities that harm political, security and economic interests. Similarly, the more recently released framework that allows the EU to impose targeted restrictive measures like sanctions to deter and respond to cyber attacks that have significant impact (or potentially significant effect) and constitute an external threat to the EU or its Member States is another

[27] United States Department of Defense, "Summary: Department of Defense Cyber Strategy 2018", September 2018, 2-3.
[28] White Paper on Defence, Government of Ireland, August 2015, 63-64.
[29] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament and the Council, "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", 13 September 2017.
[30] HM Government, "National Cyber Security Strategy 2016-2021", 2016, 56-57.
[31] Department of Communications, Climate Action & Environment, "National Cyber Security Strategy Draft Public Consultation", March 2019, 1.

example.[32] This framework is regarded as an important step in the development of signalling and reactive capacities at EU and Member State level by increasing capacity to attribute to influence the behaviour of potential aggressors and taking into account the need to ensure proportionate responses.[33] In terms of developing such national response frameworks, the State may need to again consider the role of all-source intelligence that is sourced primarily from Irish agencies when making decisions related to attribution to support the political legitimacy of its responses vis-à-vis foreign actors, and to ensure that a sovereign political decision is made given that attribution continues to be a sovereign political decision based on all-source intelligence. The EU cyber strategy makes clear that such attribution is essential to bring perpetrators to justice, warranting an urgent need to improve capacity to identify those responsible for cyber attacks.[34]

A topical discussion related to collective deterrence and response for consideration in the Irish context is the viability of the cyber deterrence initiative of the United States which builds upon the United States National Cyber Strategy's proposal in 2018 that collective action by a coalition of states will have a more powerful effect than the efforts of one state alone to deter. This raises the question as to how Ireland should engage in group initiatives like the United States' cyber deterrence initiative. The State must ideally examine how these initiatives align with its own interests to promote a peaceful and prosperous environment that is in line with the country's democratic values and security needs. By doing so, this means that the State does not (or is not seen to) unwittingly become part of such a group alignment that could be perceived in alienating terms where current descriptions such as a "coalition of the willing" or "the like-minded" could possibly bring military and five-eyes intelligence alliance images to mind. Instead, the State could likely join such a group initiative where it finds that it has like-minded foreign policy and economic interests including mutual security, economic and value interests, as well as understandable information sharing needs. Moreover, how the EU will choose to engage on this matter may further support Irish needs. By communicating these types of decisions carefully, the State could then continue to protect its international reputation as an honest broker and a country open to business, further protecting its ability to negotiate favourably in other non-cyber related international discussions. Furthermore, this type of thinking and action by the State could be in line with Irish foreign policy to work with like-minded partners as laid out in the 2015 "Global Island" paper, while also meeting other concerns that might arise in relation to collective security and neutrality/non-alignment.

Further examples of the types of actions that could be taken as part of a framework for effective deterrence can be identified within the EU's current cyber strategy, which reflects more evolved thinking on cyber since the Irish cyber strategy was first written. These include (1) Improving the capacity to identify malicious actors; (2) Stepping up law enforcement response to cybercrime through effective investigations and prosecutions, updating the procedural framework, and adhering to the Budapest Convention; (3) Enhancing public private cooperation against cybercrime; and (4) Focusing on Member States' defence capability by promoting synergies between military and civilian efforts given the dual-use nature of these technologies and tools. A number of other states, such as the United Kingdom, The Netherlands, and Australia also

[32] Council of the European Union, "Cyber-attacks: Council is now able to impose sanctions", 17 May 2019, https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/?utm_source=dsms-auto&utm_medium=email&utm_campaign=Cyber-attacks%3a+Council+is+now+able+to+impose+sanctions

[33] European Commission and High Representative of the Union for Foreign Affairs and Security Policy Joint Communication to the European Parliament and the Council, "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", 13 July 2017, 16.

[34] Ibid., 13.

emphasise that they have the means to take offensive action in cyberspace should they choose to do so – in other words, the Irish national security community could examine whether the ability to take offensive action by cyber and non-cyber means as part of a defensive posture is a necessity for effective and credible cyber deterrence, including how this should be communicated as part of an effective strategic communication framework given concerns about neutrality.

Continue efforts to protect Ireland's good reputation vis-à-vis national surveillance and cybersecurity issues

For many reasons, Ireland continues to be an attractive destination for Foreign Direct Investment. One such reason that relates particularly to tech companies in the wake of the Snowden fall-out is the State's palatable approach to surveillance issues. There could, however, be a risk of potential damage to this reputation if a perception were to grow that other states, including friendly nations, have the ability to run amok with their own cyber-enabled surveillance activities in the State. Where this is only a perception challenge and the reality of the situation is markedly different, solutions will likely boil down to creating strong communication strategies that relay otherwise. Otherwise, it could be damaging to the State's reputation if efforts are not made to counter negative perceptions about the strength of the State's cybersecurity initiatives. In addition, given the argument for a potential debate about new structures for all-source intelligence due to the unique nature of cyber questions, this situation will likely need to be further examined in the context of the State's positive reputation vis-à-vis surveillance.

In relation to those global tech companies with European headquarters in Ireland, some politicians are concerned that cyber "attacks" could have major repercussions for the Irish economy and jobs.[35] Even where these global corporations are likely to have their own very strong cybersecurity measures in place – sometimes possessing more sophisticated capabilities than individual nation states - the State's reputation for protecting FDI could arguably take a hit. As the current national cybersecurity strategy outlines, "Ireland faces a more complex set of risks than many other countries. The presence of a large number of data centric international companies here, and the growing number of data centres present in the State means that the potential for reputational damage is an important consideration." While it has now become relatively safe for states to communicate to their citizens that the nature of cyber risks means that no one actor or State has the ability to fully secure against cyber risks, growing negative public commentary about Ireland's ambivalence or an ineptitude to deal with security and cybersecurity could take hold. This could cause further damage to the country's reputation, which is a priority for the State to preserve. Examples include recent commentary citing the Comptroller and Auditor-General report notes that the 'top-level government committee tasked with developing cyber security policy "had not met since July 2015"' as well as the recent standing down of the Defence Forces' cyber unit.[36]

Even though the State continues to prioritise the importance of attracting FDI, those companies – including those choosing to relocate because of Brexit concerns – could then instead consider other EU Member States that already have strong global reputations for cybersecurity. Ideally,

[35] See https://www.fiannafail.ie/irish-businesses-at-risk-of-cyber-attacks-as-government-leave-them-ill-prepared-kelleher/
[36] See https://www.computerweekly.com/opinion/GCHQ-offers-help-to-embryonic-Irish-cyber-security-organisation

Ireland should therefore continue to leverage the reputation that the country is safe from disproportionate surveillance while also deepening its reputation for being a safe place to do business in relation to malevolent use of cyber capabilities.[37]

Continue to increase the State's international action and engagement

The current cybersecurity strategy includes an objective to continue to engage with international partners and international organisations to ensure that cyberspace remains "open, secure, unitary and free and able to facilitate economic and social development". In terms of international actions, the new strategy could add further depth to these objectives by going beyond the current strategy's short statements (for example, "European and global discussions on network and information security, including in the context of the global debate on the future of Internet governance"). By publishing Ireland's thinking on these questions within the new strategy (or by way of a more comprehensive international policy given the importance of this field to Irish security and economic interests), it could help to foster a more transparent and stable international environment that is conducive to reducing both global and national cyber threats. At a minimum, it could include an objective to examine these questions at length in the near future, including through public debate, and to become more involved in shaping the international framework for global cyber stability in a way that is in line with Ireland's values, national interests and foreign policy priorities. This could include showing solidarity with EU endeavours, fellow EU Member States, and like-minded partners where interests clearly converge, including against malicious activity and greyzone state activity during peacetime

The Irish Defence Forces' could support such international cooperation in a number of ways, including by continuing their engagement with the European Defence Agency (albeit limited), the EEAS and Commission services that are tasked with advancing Member States' cooperation and better guiding EU efforts to build cyber deterrence by facilitating strategic level engagement between Member States' cyber defence policymakers. Finally, it is worth exploring whether there is space for defence diplomacy so that the Irish Defence Forces promote such international cyber stability frameworks. By way of example, the U.S. DoD cyber strategy now highlights that the DoD will work alongside its national and international partners to promote international commitments regarding behaviour in cyberspace as well as to develop and implement cyber confidence building measures.

[37] See https://www.computerweekly.com/opinion/GCHQ-offers-help-to-embryonic-Irish-cyber-security-organisation - See for example "Behind the scenes, there was also tensions over American mass surveillance in Ireland. While Martin was in Dublin, the Supreme Court was examining a bid by Facebook to get off the hook of an Irish High Court finding that Facebook engaged in "mass and indiscriminate surveillance" in the Republic of Ireland and the EU. Facebook was found to be acting as an agent for the US National Security Agency, which is a close partner of GCHQ. Earlier this year, the Irish Government was forced to remove the Irish mass surveillance act from the statute book, following a critical report from the former chief justice of Ireland, judge John Murray. He had condemned the act, placed on the statute book under intense American pressure, for innumerable breaches of the European Convention of Human Rights, to which both the Republic of Ireland and the UK are signatories as members of the Council of Europe, which is not part of the EU."

Conclusion

While the Irish government already encourages civil-military cooperation (including in the event of a national cyber incident or emergency) and the Defence Forces are expected to maintain a capability in the area of cybersecurity to protect its own networks and users, this capacity more recently came under threat with the apparent standing down of the Defence Forces’ internal cybersecurity unit in 2019. This recent development could hinder effective civil-military cooperation if left unresolved, and it seems unclear that the Defence Forces could then assist in the event of a serious cyber crisis or attack. It is further uncertain that the Defence Forces could routinely and effectively defend its networks. In short, it is not clear that the Irish state would be able to implement an effective, credible and dissuasive deterrence framework without such a defence contribution based on these media reports.

To conclude, this situation is exacerbated at a time when advanced military strategic thinking is needed for contemporary analyses of cyber deterrence in the wake of modern cyber threats that are often persistent and below the threshold of conflict, as exemplified in most advanced democratic states. Such strategic thinking is described in this article, whereby a number of measures could be considered in the Irish context. These include, steps such as (1) Continuing the Irish government’s ongoing work to enhance cyber resilience as part of deterrence by denial where resilience is understood to be a key pillar of deterrence strategy; (2) Unpacking and adapting military thinking on 21st Century risks for the Irish security ecosystem as part of comprehensive civil-military approaches to conflict in cyberspace; (3) Protecting the Irish Defence Forces’ workforce as a critical cyber asset; (4) Adapting EU frameworks at national level for response to malicious cyber activities where the Irish government already considers the EU as having taken a particularly comprehensive approach; (5) Continuing to protect Ireland’s reputation vis-à-vis national surveillance when tackling cybersecurity issues; and (6) Increasing the State’s international action and engagement with a possible role for defence diplomacy to promote Irish government positions on international cyber stability frameworks.

PERSISTENT ENGAGEMENT AND INFORMATION CAMPAIGNING

Steven Harland
Defence and Security Advisor

Dick Hemsley
Director, Vedette Consulting (Ireland) Limited

Introduction

Our societies are changing fundamentally, becoming ever more complex and interconnected. Ease of access to information and its enabling digital technologies is rapidly shifting the balance of power from governments and formal organizations towards informal groups and individuals. Access to near real-time information via digital channels provides fora to the latter two to engage in activities previously reserved only to states and supranational organisations. The all-pervasive nature of digitally-shared information makes it an immensely powerful multi-dimensional agent of change, facilitating an unprecedented level of connectedness across the globe. Given this context, we will argue that Western states and supranational organisations are inextricably engaged in a non-discretionary contest in which their core values are held at risk, and that Smart Power responses are needed in pursuit of their legitimate interests. We contend that this has implications for current security policy paradigms, which need to be adjusted to encompass Information Campaigning approaches matched to the new and dynamic competitive space. Finally, we will argue that the core of the advocated approach is directed at an Influence Nexus; that locus in an Information Campaign design where strategic, operational and tactical-level activities will, together, realise a set of mutually-reinforcing behavioural outcomes across selected target audiences.

A New Seam

The evolving character of contemporary strategic competition and armed conflict increasingly encompasses complexity, instability, uncertainty, all-pervasive information and rapid technological development. The emergent networked world is characterised by diverse audiences that cannot be usefully categorised in conventional ways; these are no longer passive, but are now themselves acting as influencers, opinion-formers and 'news-makers'.[1] Issues of identity, trust and security[2] in the virtual dimension now play out in a wider political discourse about data privacy, inequalities and unfettered global enterprise. These developments have ushered in a new seam of inter-state competition that challenges states to align their strategic approaches to the structural realities of multiple information environments.[3] The distinction between conflict and peace is fast eroding, and adversaries of the West, both state and non-state, increasingly threaten the stability of the extant international order. There is a continuing competition among diverse state and non-state actors, one conducted largely with non-military means, which involves subversion, political agitation, sabotage, espionage and crime, and is mediated through and by cyberspace. Hybrid Warfare, Asymmetric Warfare and Reflexive Control[4] are all examples of how states are already conducting such a contest in and via cyberspace to gain strategic advantage.[5]

[1] Slaughter (2009) comments that the emerging networked world exists 'above the state, below the state, and through the state'. A.M. Slaughter, 'America's Edge: Power in the Networked Century', Foreign Affairs, January/February, 2009. For mass self-communication see M. Castells, Communication Power, Oxford University Press, 2009. For media ecology see J van Dijck, Culture of Connectivity: A Critical History of Social Media, Oxford University Press, 2013, R. Grusin, Premediation: Affect and Mediality After 9/11, Basingstoke: Palgrave Macmillan, 2010; J. Mackinlay, The Insurgent Archipelago, London: Hurst & Co, 2009

[2] Edward Lucas, Cyberphobia: Identity, Trust, Security and the Internet, 2015.

[3] R.J. Harknett, Cyber Persistence: Re-thinking Security and Seizing the Strategic Cyber Initiative, National Academies of Sciences, Engineering, Medicine, Decadal Survey of Social & Behavioural Sciences for Applications to National Security, October 11, 2017; M.P. Fischerkeller and R.J. Harknett , Deterrence is Not a Credible Strategy for Cyberspace, ORBIS, Vol 61, Issue 3, 2017, 381-393; R.J. Harknett and E.O. Goldman, The Search for Cyber Fundamentals, Journal of Information Warfare, Volume 13, Issue 2, 2016. Harknett suggests that complexity arises from the fact the terrain is both a 'space' and a 'means'.

[4] Reflexive control is defined as a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action.

[5] For commentary on Hybrid Warfare, see Galeotti, M, 'Hybrid, Ambiguous, and Non-Linear? How New Is Russia's "New Way of War"?' Small Wars and Insurgencies, Vol. 27, No. 2, 2016, pp. 282–301; R. Seely, Defining Contemporary Russian Warfare: Beyond the Hybrid Headline, RUSI Journal, Vol 162, No 1, February-March 2017. For Asymmetric Warfare, see R. Thornton, The Russian Military's New 'Main Emphasis': Asymmetric Warfare, RUSI Journal, Volume 162, No 4, Oct 2017; For Reflexive Control, see T.L. Thomas, Russia's Reflexive Control Theory and the Military, Journal of Slavic Military Studies, Vol. 17, No. 2, 2004, 237–56.

States are now, essentially, persistently engaged at below the threshold of armed conflict.[6] The effect of this on the present international order may be to dramatically reshape relations between states, and between states and non-state actors, and bring a multitude of spatially distant, previously objectively weak actors into the strategic mix.[7] Some states have been swift to recognise both the threat and opportunity these developments present, and have adopted new long-term strategies as a result.

Russia and China have been characterised as executing Sharp Power strategies to '…penetrate, or perforate, the political and information environments in the targeted countries…to manipulate their target audiences by distorting the information that reaches them'.[8] In so doing, they are exerting pressure on their perceived adversaries using all four classical levers of national power (Diplomatic, Informational, Economic and Military – DIME), without regard to Western norms of behaviour. Via extensive multi-dimensional campaigns of disinformation, Sharp Power users seek to amplify the tensions between audiences which seem suspicious of authority and unwilling to await the rebuttal of unsupported opinions by governmental actors.[9] Attribution of activity to actor is often difficult, in cyberspace, particularly in the social media environment, and so the scope for deception and denial is immense.[10] Actions by the West's strategic competitors are not nearly so constrained by legal and ethical considerations. New 'rules of the game' are emerging, and so Western states must swiftly learn how to play well by them – without compromising their liberal democratic values. However, Western actors' notions of the nature and primacy of truth appear to be stressed in these new circumstances, and so may distort their strategic responses.[11] Furthermore, Joseph Nye observes that the West should be cautious about offensive responses to the growing Sharp Power threat. Whilst accepting the tactical utility of information warfare, he warns the West against launching major programmes of covert information warfare which, if compromised and correctly attributed, could undermine its strategic efforts at exerting its Soft Power[12].

Information Campaigning

Within this dynamic strategic context, bringing influence to bear on actors and audiences is becoming more complex and competitive, and yet is increasingly central to the protection,

[6] Referred to by Chief of the General Staff, Gen Sir Nicholas Carter at this Opening Address to the RUSI Land Warfare Conference, 28 June 2016.

[7] Mackinlay, ibid. Cairncross talks about the 'death of distance'. F. Cairncross, Death of Distance: How the Communications Revolution is Changing Our Lives, Cambridge, MA: Harvard Business School Press, 2001.

[8] C. Walker and J Ludwig, The Meaning of Sharp Power: How Authoritarian States Project Influence, Foreign Affairs, November 2017. C. Walker, S. Kalathi and J. Ludwig, How Democracies Can Fight Authoritarian Sharp Power: New Laws Aren't Enough, Foreign Affairs, August 16, 2018. Wigell (2019) characterises this form of interference as a 'wedge strategy' that seeks to undermine governance. M. Wigell, Hybrid interference as a wedge strategy: a theory of external interference in liberal democracy, International Affairs 95: 2 (2019) 255–275.

[9] For example, S. Bradshaw and P.N. Howard, Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation, Oxford Internet Institute, Oxford University, 2018. P.N. Howard, B. Ganesh, D. Liotsiou, J. Kelly and C. Franciois, The IRA, Social Media and Political Polarization in the United States, 2012-2018, Oxford Internet Institute, Oxford University, 2018. An assessment of the Internet Research Agency's U.S.-directed activities in 2015-2017 based on platform-provided data, Senate Select Committee on Intelligence Research Summary, New Knowledge Report, December 2018.

[10] In a 'post-truth' world, what does attribution achieve after the event when addressing social media manipulation, for example, Russia's Internet Research Agency (IRA) extended attacks on the United States using computational propaganda to misinform and polarize US voters. See P.N. Howard, B. Ganesh, D. Liotsiou, J. Kelly and C. François, The IRA, Social Media and Political Polarization in the United States, 2012-2018. Working Paper: UK Project on Computational Propaganda, Oxford Internet Institute, Oxford University, 2018.

[11] K. Giles, Russia's 'New' Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power, Royal Institute of International Affairs, March 2016.

[12] J.S. Nye Jnr, How Sharp Power Threatens Soft Power: The Right and Wrong Ways to Respond to Authoritarian Influence, Foreign Affairs, 2018. J.S. Nye Jnr, Soft Power: The Means to Success in World Politics, Public Affairs; New Ed edition, 2005.

or advancement, of national and/or supranational interests. This makes it necessary for state and supranational actors to understand the key structural characteristics of the various information environments – a complex terrain characterised by constant contact and continuous change, and one requiring persistent activity by protagonists in strategic competition.[13] Individuals, groups and formal organisations are increasingly interacting in several different information environments – often simultaneously. The latter are not defined by physical location, but by proximity to the consciousness of audiences, each one interacting with others via both traditional and social media. We offer the following framework, based on our analysis to date:

The Global Information Environment – a vast interplay of voices and activities, some of which have indirect relevance to influencing a target audience.

The Strategic Information Environment – competing macro-narratives of ideas, words and deeds, some of which have direct relevance to influencing a target audience.

The Local Information Environment – competing micro-narratives of words and deeds, most of which have direct relevance to influencing a target audience.

The Intimate Information Environment – competing micro-narratives of words and deeds, all of which have intimate, immediate relevance to influencing a target audience.

In the ongoing strategic competition, actors' intentions are relatively difficult to discern, and actions are very difficult to attribute. Hybrid tactics complicate attribution and create dilemmas for any response.[14] Effective deterrence in the virtual dimension is not defensive or passive, but active in nature. It requires the building of a set of deterrent effects as part of a dynamic contest, in which move and counter move may only be dimly perceived, and often misunderstood, by those subject to their effects.[15] Ambiguity and plausible deniability are now the hallmarks of covert military operations which are synchronized with intelligence agency-led clandestine operations to achieve strategic effects, whilst still allowing de-escalation options and 'off-ramps'.

We contend that to do these things within a liberal-democratic ethical and legal framework is to exert 'Smart Power' in support of legitimate national or supranational interests.[16] Smart Power entails the development of an integrated strategy, building alliances and global networks to achieve strategic objectives, drawing judiciously on elements of both Hard and Soft Power. This conception of Smart Power is consistent with that offered by Chester Crocker: the strategic use of diplomacy, persuasion and capacity building, aligned with the projection of power and influence, which has political and social legitimacy.[17] Legitimacy rooted in an adherence to liberal-democratic norms differentiates Smart Power from Sharp Power.

Given the centrality of the virtual dimension in this new competitive space, activities undertaken within carefully selected information environments should increasingly be

[13] R.J. Harknett, Op Cit.

[14] Deterrence: The Defence Contribution, UK Joint Doctrine Note 1,19, 2019.

[15] NATO defines deterrence as: The convincing of a potential aggressor that the consequences of coercion or armed conflict would outweigh the potential gains. This requires the maintenance of a credible military capability and strategy with the clear political will to act.

[16] Center for Strategic and International Studies (CSIS) Commission on Smart Power: A Smarter, More Secure America, 2007.

[17] C. A. Crocker, F.O. Hampson and P.R. Aall, Leashing the Dogs of War: Conflict Management in a Divided World, United States Institute of Peace Press, 2007.

a primary focus of Western security strategies. Smart Power can best be delivered through Information Campaigning, which we define as: the operationalization of a defined Information-led strategy via the exercise of 'Smart Power' in order to secure beneficial influence in pursuit of national/supranational interests. Information Campaigning opens up a new channel for strategic competition by seeking primacy in the contest of ideas and the battle to attract. Its conduct therefore has profound implications for national and supranational security.

Protection and advancement of interests is at the heart of sound foreign and security policy-making. Palmerston asserted that: 'We have no eternal allies, and we have no perpetual enemies. Our interests are eternal and perpetual, and those interests it is our duty to follow'[18]. It follows that strategy-making should seek to promote and protect explicitly-identified interests, encapsulated in policy which provides its ends. Only in, or on the very threshold of conflict, should the West's use of the military lever of power be predominant. In other circumstances, the Diplomatic, Informational or Economic lever of DIME will be the supported one. When a strategy has been chosen, it will be enacted via one or more campaigns, each of which will be rooted in one of the levers of power. Given the centrality of the virtual dimension, the Informational lever is now becoming predominant. As with military campaigning in the physical domain, there may well be an 'offensive premium'[19] to be exploited in Information Campaigning in the virtual one.

An Adaptive Approach

A liberal-democratic state can only undertake successful Information Campaigning by creating, integrating and coherently developing a federation of capabilities which are typically owned and separately exploited by different elements of the governmental enterprise. These governmental capabilities include a set of 'effectors' responsible for: Diplomacy; Overseas Development Aid[20]; International Trade Relations; Strategic Communication; Military Information Operations; Active Cyber Operations and Secret Intelligence. They also include those capabilities responsible for Homeland Security and Defensive Cyber Operations (as 'protectors'), and for the provision of Information Systems and Services and Science and Technology advice (as 'enablers').

Credible and effective Information Campaigning requires that bespoke combinations of these key instruments operate across multiple domains (cyberspace and the electromagnetic spectrum, space, sea, land and air) as part of cross-government efforts, integrated with those of allies and partners. This integrated approach must go much wider, and deeper, than previous initiatives (such the EU's 'Comprehensive Approach'[21] or the UK's 'Fusion Doctrine'[22]). Furthermore, the challenge to state primacy is growing, as cyber and other

[18] Henry Temple, 3rd Viscount Palmerston, British Foreign Secretary, speech in the House of Commons, 7th August 1844 (Hansard https://api.parliament.uk/historic-hansard/commons/1844/aug/07/foreign-policy-of-ministers accessed on 31st July 2019).

[19] For example, Dr Philip Sabin (The Counter Air Contest, in The Dynamics of Airpower, HMSO 1996) asserts that, given the nature of the air environment, offensive action has an inherent advantage and therefore, in principle, is more likely to lead to success in what is termed the 'counter-air contest'.

[20] The sensitivities associated with the internationally agreed objectives of Overseas Development Aid are acknowledged, but these may nonetheless align with security objectives more often – and more seamlessly – than might at first be thought.

[21] Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy; European Union, June 2016.

[22] National Security Capability Review. Her Majesty's Government, March 2018.

information activities can be undertaken ever more easily by non-state actors. This changes the risk calculus for states, as it blurs the distinction they typically make between 'home' and 'away' operating spaces. In the new era of persistent engagement, states require a broader range of tools, and both attributable and non-attributable methods with which to apply effective pressure on adversaries below the Western military response threshold. Synchronization of disparate activities in domain, space and time is essential in order to realise intended influence effects. A useful capacity for Information Campaigning therefore requires pan-governmental enterprise alignment, laterally, vertically and temporally[23]:

Horizontal alignment: Across each relevant governmental agency and department, including between functional teams, to optimise strategic alignment and co-ordination of activity.

Vertical alignment: Along multiple developmental pathways to cohere strategies with operational planning and design activities to enable the delivery of full spectrum effects.

Temporal alignment: Through active monitoring and evaluation, over time, to understand the realisation of effects, and objectives and the nature and level of risk.

Given the dynamic nature of their security challenges and continual developments in digital technologies, Western governments need to be robustly adaptive – technologically, organisationally and behaviourally – in approaching capability innovation in support of Information Campaigning.

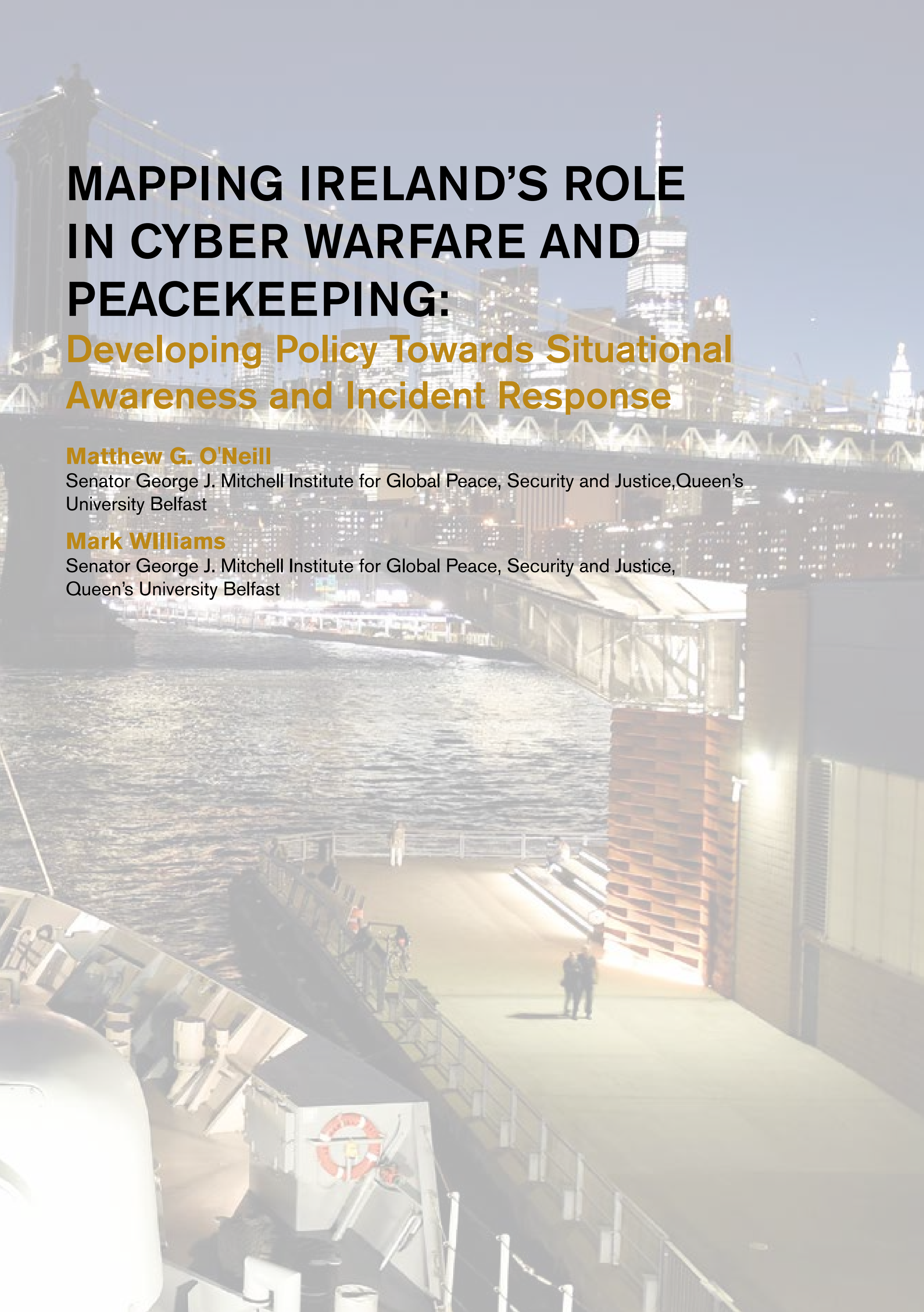
Influence Nexus

Western states are inextricably engaged in a non-discretionary contest, one in which their core values and interests are held at risk. Individual and collective responses to their adversaries' use of Sharp Power have tended to be reactive, and largely defensive in nature. We have argued that a more effective response is to exert Smart Power in support of legitimate national or supranational interests. In their current form and by their inherent nature, Western states and their supranational organisations exert more Soft than Hard power. However, much of their Soft Power remains latent at the seams between their governmental institutions. Furthermore, in response to Sharp Power approaches such as those of Russia and China, their application of a wholly Soft Power strategy risks overmatch.

Current Western security policy paradigms should be adjusted to accommodate active Information Campaigning within today's dynamic competitive space: engaging multiple target audiences whilst constraining adversaries' freedom of manoeuvre; and changing their risk calculus by creating a set of complimentary deterrence and compellence effects. The core of this approach lies in carefully planned and coherently managed activities directed at an Influence Nexus across selected target audiences, including adversaries and other actors. The Nexus is that point within an Information Campaign design when all strategic, operational and tactical-level activities realise a set of mutually-reinforcing behavioural outcomes across all chosen target audiences. To affect an Influence Nexus requires the continuous conduct of an analytical process of mapping and characterising targets of interest, combined with the active

[23] At a supranational (for example, EU or NATO) level, an additional dimension of complexity obviously applies, as supranational institutional capabilities must be confederated with Member States' own federations.

monitoring and evaluation of the effects realised on them. Both these processes should drive, and be intimately supported by, a dynamic and layered intelligence framework and architecture. If states can acquire a capacity for effective Information Campaigning focused on an Influence Nexus, they will gain the sophistication to use Smart Power to secure their societies without compromising their core values.



MAPPING IRELAND'S ROLE IN CYBER WARFARE AND PEACEKEEPING:

Developing Policy Towards Situational Awareness and Incident Response

Matthew G. O'Neill
Senator George J. Mitchell Institute for Global Peace, Security and Justice,Queen's University Belfast

Mark WIlliams
Senator George J. Mitchell Institute for Global Peace, Security and Justice,
Queen's University Belfast

Introduction

This paper aims to explore how Ireland's Defence Forces and the Irish Department of Foreign Affairs and Trade can leverage their extensive experience of peacekeeping within conflict and post-conflict societies in the context of potential future cyber conflicts. Such an exploration is set within the context of Ireland's collaboration within the European initiative, the Permanent Structured Cooperation (PESCO)[1] and in a geo-political landscape where cyber security threats are used as a form of diplomatic leverage.

Ireland has a strong and proud heritage of peacekeeping through the United Nations with significant recent examples including activities in Liberia (2003), Chad (2007) and Syria (2013). At present Ireland is involved in two major EU PESCO projects; *Harbour and Maritime Surveillance and Protection*[2] and the *EU Training Mission Competence Centre*[3]. Based on its peacekeeping history and well-developed cyber sector, this research proposes Ireland should play a leading role in the formation and development of cyber peacekeeping by also seeking membership of the following PESCO mechanisms; the *Cyber Threats and Incident Response Information Sharing Platform*[4] and *Cyber Rapid Response Teams and Mutual Assistance in Cyber Security*[5].

As cyber warfare becomes more prevalent it is increasingly important for peacekeeping missions to have a cyber element to fully reflect future challenges and contexts and to ensure a full reconstruction of post-conflict societies. It could be built upon within the Department of Foreign Affairs and Trade's combined approach of developing a conflict resolution function in order to export Ireland's own model[6], based around the 4 Ps: Prevention, Participation, Protection and Promotion[7].

This proposed diplomatic model could be leveraged for other states focused on peacekeeping while reinforcing Ireland's leadership within this field, focusing on new initial cyber assessment for conflict and post-conflict societies and exploring how monitoring can contribute towards peace by identifying actions that violate ceasefire agreements, human rights abuses and network infractions.

This model could also develop 'new multinational strategies and institutions' to ensure the 'sovereignty and survival of states'[8] by assessing the level of aid resources needed and the capacity of the local IT sector to act.

[1] European Deference Agency, The Permanent Structured Cooperation, [Accessed on 25.07.2019] https://www.eda.europa.eu/what-we-do/our-current-priorities/permanent-structured-cooperation

[2] PESCO Projects, Harbour and Maritime Surveillance and Protection (Harmspro), [Accessed on 25.07.2019] https://pesco.europa.eu/project/harbour-and-maritime-surveillance-and-protection/

[3] PESCO Projects, European Union Training Mission Competence Centre (EU TMCC), [Accessed on 25.07.2019] https://pesco.europa.eu/project/european-union-training-mission-competence-centre/

[4] PESCO Projects, Cyber Threats and Incident Response Information Sharing Platform, [Accessed on 25.07.2019] https://pesco.europa.eu/project/cyber-threats-and-incident-response-information-sharing-platform/

[5] PESCO Projects, Cyber Rapid Response Teams and Mutual Assistance in Cyber Security, [Accessed on 25. 07. 2019] https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/

[6] William A. Hazleton, 'Look at Northern Ireland': Lessons Best Learned at Home. In Lessons from the Northern Ireland Peace Process, The University of Wisconsin Press, 2013, 34 - 60

[7] Department of Foreign Affairs and Trade, Speech by Tánaiste at launch of Ireland's Third National Action Plan on Women, Peace and Security, 21 June 2019 [Accessed on 25.07.2019] https://www.dfa.ie/news-and-media/speeches/speeches-archive/2019/june/speech-by-tanaiste-at-launch-of-irelands-third-national-action-plan-on--women-peace-and-security.php

[8] Stephen Herzog, Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses, In Journal of Strategic Security Vol. 4, No. 2, Strategic Security in the Cyber Age (Summer 2011), 49-60. [Accessed on 25.07.2019] https://www.jstor.org/stable/26463926?seq=10#metadata_info_tab_contents

Cyber Warfare and the move toward Blended Warfare

The term cyber warfare is frequently contested, with no agreed definition in international law, with some experts claiming it does not and cannot meet any traditional definition of warfare.[9] Nevertheless there is a general consensus that cyber warfare refers to the use of digital technology to launch an attack on the network, infrastructure, systems and/or data of another nation to cause comparable damage, disruption or destruction as would be caused by conventional weaponry. The Tallinn Manual[10] uses the term Computer Network Operations (CNO) to describe three types of activities comparable to cyber warfare[11]:

Computer Network Attack (CNA) – Operations aiming to "disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[12]

Computer Network Exploitation (CNE) – Operations aimed at collecting intelligence and data from adversary automated information systems or networks. This is linked to and has parallels with espionage[13].

Computer Network Defence (CND) – Actions taken to protect, monitor, analyse, detect, and respond to unauthorised activity within information systems and computer networks. And prevention of CNA and CNE through intelligence, counterintelligence, law enforcement, and military capabilities[14].

Increasingly, cyber attacks have also been used as part of information warfare not only for espionage purposes but also to distribute and disseminate propaganda, disinformation and misinformation; as well as undermining democratic institutions, political processes and the validity of the press[15] [16].

While a clear example of cyber warfare with specified antagonists is yet to occur – or at least is yet to be discovered – a number of incidents have occurred that have inflicted serious disruption to a nation's infrastructure, suggesting they were sponsored by a nation state or state-backed actors[17]. Examples of these sorts of attacks include the Titan Rain attack of 2003 and the attack on Estonia in 2007, which resulted in the West reconsidering the importance of network security to modern military doctrine and led to the creation of NATO's Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia[18] [19].

[9] Thomas Rid, Cyber war will not take place. Journal of strategic studies, 2012, 35(1), 5-32.

[10] The International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press

[11] Ziyad Hayatli, Cyber Warfare in International Law, The New Jurist, 6 December 2018, [Accessed on 25.07.2019] http://newjurist.com/cyber-warfare-in-international-law.html

[12] Ibid

[13] Ibid

[14] Ibid

[15] Steve Ranger, Cyber war isn't turning out quite how it was expected, In ZD Net, 18 July 2016 [Accessed on 25.07.2019] https://www.zdnet.com/article/cyber-war-isnt-turning-out-quite-how-it-was-expected/

[16] Emilio Iasiello, Cyber Strikes Do Not Equate to Cyber Warfare, In Technative, 10 July 2019 [Accessed on 25.07.2019] https://www.technative.io/cyber-strikes-do-not-equate-to-cyber-warfare/

[17] Steve Ranger, What is cyberwar? Everything you need to know about the frightening future of digital conflict, In ZD Net, 4 December 2018 [Accessed on 25.07.2019] https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/

[18] North Atlantic Treaty Organization, Cyber Defence, NATO, 16. July.2018 [Accessed on 25.07.2019] https://www.nato.int/cps/en/natohq/topics_78170.htm

[19] Stephen Herzog, Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses, In Journal of Strategic Security Vol. 4, No. 2, Strategic Security in the Cyber Age (Summer 2011), PP.49-60. [Accessed on 25.07.2019] https://www.jstor.org/stable/26463926?seq=10#metadata_info_tab_contents

While attribution was never fully confirmed in those two attacks, since states increasingly find it easier to cover their tracks than do individuals involved in cyber offensives, it is nevertheless possible based on the geopolitical situation to speculate on which aggressors might be responsible[20].

NATO's recognition in July 2016 that cyberspace constituted a theatre of war/domain of operations alongside air, land and sea, and the possibility that a cyber attack on a member state if severe enough could trigger an Article 5 response, illustrates the increased reliance on digital systems to operate and maintain most nations' infrastructures and highlights the potential harm a cyber attack could inflict on both an individual national ecosystem as well as the global economy[21][22].

The International Strategy for Cyberspace outlined by President Obama in May 2011, further underlined this point by stating that "all necessary means" including military operations would be used to counter "hostile acts conducted through cyberspace"[23]. This move towards a blended warfare model in which a digital attack can be met with a kinetic response was recently illustrated by Israel's attack on Hamas (June 2019)[24] in response to a cyber attack and the mobilisation of the US Air Force in response to the Iranian downing of a US surveillance drone (July 2019)[25].

These two events should not be seen as trivial or unique and the potential for future conflict to be triggered by a digital attack cannot be downplayed. As the UN Secretary General, Antonio Guterres, recently noted: "I am absolutely convinced that, differently from the great battles of the past, which opened with a barrage of artillery or aerial bombardment, the next war will begin with a massive cyber attack to destroy military capacity… and paralyse basic infrastructure…" (2018)[26].

While the full impact of cyber warfare is not yet fully appreciated, what *is* known is that cyber related interventions will be needed to restore peace and security and assist the recovery and rebuilding of nation states in both the physical and digital realms (Dorn, 2017)[27]. Peacekeeping, therefore, will increasingly require a cyber element and Ireland can be well-placed to offer this expertise[28] [29].

[20] Emilio Iasiello, Cyber Strikes Do Not Equate to Cyber Warfare, In Technative, 10 July 2019 [Accessed on 25.07.2019] https://www.technative.io/cyber-strikes-do-not-equate-to-cyber-warfare/

[21] North Atlantic Treaty Organization, Cyber Defence, NATO, 16. July.2018 [Accessed on 25.07.2019] https://www.nato.int/cps/en/natohq/topics_78170.htm

[22] Press Release, Exposure to cyber-attacks in the EU remains high – New ENISA Threat Landscape report analyses the latest cyber threats, European Union Agency For Cybersecurity 28 January 2019 [Accessed on 25.07.2019] https://www.enisa.europa.eu/news/enisa-news/exposure-to-cyber-attacks-in-the-eu-remains-high

[23] John M. Donnelly, National security experts say America is woefully unprepared for cyber warfare, In Security Infowatch, 15 July 2019 [Accessed on 25.07.2019] https://www.securityinfowatch.com/cybersecurity/news/21088486/national-security-experts-say-america-is-woefully-unprepared-for-cyber-warfare

[24] Lily Hay Newman, What Israel's Strike on Hamas Hackers Means For Cyberwar, 05 April.2019 [Accessed on25.07.2019] https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/

[25] Scott Shane, Nicole Perlroth and David E. Sanger, 'Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core. In The New York Times, 12.November, 2017 [Accessed on 25.07.2019] https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html

[26] Report, ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends, January 2019, [Accessed on 25.07.2019] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[27] Walter Dorn, Cyberpeacekeeping: A New Role for the United Nations. In Georgetown Journal of International Affairs, 18, Issue 3 (Fall 2017). [Accessed on 25.07.2019] https://heinonline.org/HOL/Page?handle=hein.journals/geojaf18&div=54&?&collection=journals

[28] Aleksandar Shopski, Cyber Peacekeeping Forces: the solution to a contemporary matter, In Techruption, May 2018, [Accessed on 25.07.2019] https://www.techruption.org/cyber-peacekeeping-forces-the-solution-to-a-contemporary-matter/

[29] Helge Janicke, Cyber peacekeeping is integral in an era of cyberwar – here's why, In The Conversation, 29 January 2019, [Accessed on25.07.2019] https://theconversation.com/cyber-peacekeeping-is-integral-in-an-era-of-cyberwar-heres-why-90646

The European Union and Cybersecurity

The European Union's approach to cybersecurity has been one which focused internally on setting policy and law in the direction of protecting its own internal market and combating criminal law. With the incoming von der Leyen Administration, security and foreign affairs matters will be at the top of the new commission's five-year agenda. As addressed in the above section, an emerging approach concentrating on cybersecurity techniques is being used to develop leverage[30].

The EU has already discussed plans to empower EU law enforcement agencies to respond to cross-border cyber incidents, but the question remains, are these plans sufficient in the face of the changing threat of cyber warfare? There will be a need to review issues within existing legal practices and treaties that do not define specific areas of responsibility, while forming an approach to tackling them[31]. Developing a cyber defence approach can no longer simply be about protecting the internal nature of the EU but will have to move outside of the Union's internal borders[32]. Such a move will be in terms of direct cyber defences, but also - as addressed in this paper - within the physical realm. It will be vital that EU battle groups can operate within both these contexts[33]. For example, with the recent, and unusually highly reported, cyber attack by the US on Iran, it is clear that cyber security is no longer used solely as a form of gaining and collecting intelligence and protecting one's own information. In many respects the use of cyber attacks has developed into a form of 21st century gunboat diplomacy[34].

The EU will, within the limitations of its own Internal Digital Single Market, move towards reform of cyber security policies with the aim of developing a holistic approach to the Common Foreign and Security Policy (CFSP) framework[35]. This however will not come without challenges, as we have observed with the development of PESCO, which was not easy to advance, build upon or harness. The EU's strength as a security actor will remain its ability to lend its sovereignty – and scale – for competence-based decision-making[36].

To understand the role of Ireland within the emerging EU security framework it is important to note the EU's current approach to cybersecurity. This is built upon a legalistic framework and a multi-stakeholder approach that ensures an 'open and secure internet'[37]. Traditionally, the EU has taken a bottom-up approach to the development and goal setting of its security and of PESCO[38]. Despite this, different views on the concepts of Fortress Europe are useful

[30] Alex Barker and Mehreen Khan, What to expect from President von der Leyen, 17 July 2019, [Accessed on 25.07.2019] https://www.ft.com/content/f15b3e28-a818-11e9-984c-fac8325aaa04

[31] Mette Eilstrup-Sangiovanni, Why the World Needs an International Cyberwar Convention, In Philosophy and Technology, September 2018, Vol 31, Issue 3, 379-407.

[32] Council on Foreign Relations, Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms, 23 February 2018, [Accessed on 25.07.2019] https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms

[33] European Union External Action, Towards a stronger EU on security and defence, 19 November 2018, [Accessed on 25.07.2019] https://eeas.europa.eu/headquarters/headQuarters-homepage/35285/towards-stronger-eu-security-and-defence_en

[34] Zak Doffman, Cyber Warfare Threat Rises As Iran and China Agree 'United Front' Against U.S., In Forbes, 6 July 2019 [Accessed on 25.07.2019] https://www.forbes.com/sites/zakdoffman/2019/07/06/iranian-cyber-threat-heightened-by-chinas-support-for-its-cyber-war-on-u-s/

[35] Political and Security Committee, CFSP Report – Our priorities in 2017, [Accessed on 25.07.2019] https://eeas.europa.eu/sites/eeas/files/st10650_en-cfsp_report_2017.pdf

[36] EU Competency Framework, EU Competency Framework for the management and implementation of the European Regional Development Fund and the Cohesion Fund, [Accessed on 25.07.2019]

[37] Anri Van der Spuy, What if we all governed the Internet? Advancing multi-stakeholder participation in Internet governance, 2017, [Accessed on] https://unesdoc.unesco.org/ark:/48223/pf0000259717_eng

[38] European Commission, Questions and Answers – EU Cybersecurity, 26 June 209, [Accessed on 25.07.2019] http://europa.eu/rapid/press-release_QANDA-19-3369_en.htm

to employ here, as within this concept Europe has become a laboratory of different security practices, with cybersecurity no different[39].

The current EU approach to designing cybersecurity policy has been one of a purely technical nature or 'logic of control'[40]. As this paper outlines, because cybersecurity will be used as a form of diplomacy in coming decades it is vital that governments have policy and procedures to enact in case they are in areas or conflict zones that have been affected by a diplomatic cyber attack[41].

The EU's role on the international stage will be brought to the fore when institutions need to be protected. With PESCO and the different strands of policy development under the new commission it is clear that cybersecurity and cyber defence will be a key pillar for the EU to become a 'normative global actor'. This of course depends on whether the issues addressed in this paper are resolved, and the EU could fully enact its potential to be a leading actor[42].

A significant question within this context will be whether the EU will still be committed to an open and free internet and making sure its citizens rights are not diminished. Within the EU, individual members remain dominant in cybersecurity; and while Ireland still has a lot it can learn from its neighbours, it is clear that within the emerging cybersecurity approach it has a lot of experience to offer in how cyber warfare can affect conflict and post-conflict assistance on the ground[43].

The EU has an opportunity to be more than only a coordinator and facilitator of policies. It could become a powerful cybersecurity actor in its own right and it is important that Ireland's voice is heard in this context, as it continues to support and consider its roles and responsibilities within PESCO. The question is, will member states be able to produce an attributable response to these pressing issues. The Defence Forces has had a distinguished history both of providing peacekeeping missions on the ground and balancing practical diplomacy. Where it has not yet been given the attention it rightly deserves is in the area of cyber peacekeeping within the digital and real worlds[44].

Currently small EU member states such as Belgium and Portugal are bringing together its private, public and higher education sectors to lead on cyber defence projects under the auspices of PESCO. Ireland could adopt a similar strategy to utilises the expertise of research and development being carried out in Irish higher education institutions and in the private sector to develop its cyber peacekeeping capabilities, as at present the Defence Forces currently have minimal cyber capability.

[39] European Defence Matters, PESCO: More Than Just Projects, 2019 [Accessed on 25.07.2019] https://www.eda.europa.eu/webzine/issue15/cover-story/pesco-more-than-just-projects

[40] European Union External Action, New tool to address cyber threats: the EU's Rapid Response Force, 27.06.2018 [Accessed on 25.07.2019] https://eeas.europa.eu/topics/eu-international-cyberspace-policy/47525/new-tool-address-cyber-threats-eus-rapid-response-force_en

[41] The European Files, Guaranteeing Cybersecurity: Ambitions for a European Cyberspace, March 2019, No 57, [Accessed on 25.07.2019] https://aioti.eu/wp-content/uploads/2019/03/Guaranteeing-Cybersecurity-Ambitions-European-Cyberspace-issue-57.pdf

[42] Nathalie Tocci, Who is a Normative Foreign Policy Actor? The European Union and Its Global Partners, CEPS, 27 May 2008, [Accessed on 25.07.2019] https://www.ceps.eu/ceps-publications/who-normative-foreign-policy-actor-european-union-and-its-global-partners/

[43] Department for Digital, Culture, Media and Sport, Cyber Security Breaches Survey 2019, [Accessed on 25.07. 2019] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf

[44] Council of the European Union, Cyber defence: Council updates policy framework, 19 November 2018, [Accessed on 25.07.2019] https://www.consilium.europa.eu/en/press/press-releases/2018/11/19/cyber-defence-council-updates-policy-framework/

Ireland's Potential Role as a Cyber Peacekeeper

The above paragraphs map out the political and structural challenges facing the Irish Government and Defence Forces. In this section we will explore how both can take a proactive approach in preparing Irish Peacekeepers to becoming Cyber Peacekeepers. The expertise of Robinson, Jones, and Janicke[45] can be used as a lens to frame how Ireland can fulfil this role. Additionally, the case study of Ireland's involvement within the Colombian peace process will be utilised to highlight how the Irish Government and Defence Forces can start mapping out a digital course of action for strategies in aiding societies within conflict or post-conflict[46].

Ireland has played an important role in aiding the Colombia peace process, offering its model as well as being the head of the EU special delegation[47]. Sergio Jaramillo, Colombia peace commissioner, stated that the "last part of renegotiation was exhausting. It took us to the limit. But now we pass to something more difficult, which is to change the conditions on the ground and benefit our *campesinos*. . . and to worry about the security of communities'"[48]. Two years later in 2018 President Juan Manuel Santos announced the foundation of the Integrated Centre for Electoral Intelligence to ensure the integrity of future elections free from foreign and domestic interference. President Santos addressed the issue of hacking and issue of the spreading of false information to create a climate of apprehension and mistrust that may influence voters and undermine a fragile peace[49] [50].

If Ireland is to develop a government department whose main mission is to export a post-conflict model, it will have to consider the use of technology within societies and how its use will affect the local population within their everyday lives.

This paper argues that the form of blended warfare that emerges from any new conflict will inevitably have a digital element because of the very nature of globalisation. As such, any society emerging from conflict will need corresponding peace agreements which cater for cyber protection and reconstruction. Furthermore, this will benefit the development of communications and infrastructure for the multi-level governance of the many strands of former combatants, political actors and innocent parties within emerging societies. We also must be cautious of the threat of misinformation and disinformation to the validity of any peace accords signed and agreed. As Robinson, Jones, and Janicke stated, cyber peacekeeping must not only preserve peace but also "assist in implementing agreements achieved by the peacemakers."[51] Increasingly, this mission to secure hearts and minds must operate within the digital realm.

[45] Robinson, M., Jones, K., Janicke, H. and Maglaras, L., 2018. An introduction to cyber peacekeeping. Journal of Network and Computer Applications, 114, 70-87.
[46] Ibid.,70-87.
[47] Press Release, 'Colombia Peace Agreement' Department of Foreign Affairs and Trade, 2016 [Accessed on 25.07.2019], https://www.dfa.ie/annualreport/2016/our-influence/colombia-peace-agreement/
[48] Adriaan Alsema, Intelligence unit to fight 'fake news' and cyber-attacks in Colombia's elections, Colombia Reports, 23 January 2018, [Accessed on 25.07.2019] https://colombiareports.com/intelligence-unit-fight-fake-news-cyber-attacks-colombias-elections/
[49] Ibid.
[50] Ted Piccone, Is Colombia's fragile peace breaking apart?, Brookings Institute, 28 March 2019, [Accessed on 25.07.2019] https://www.brookings.edu/blog/order-from-chaos/2019/03/28/is-colombias-fragile-peace-breaking-apart/
[51] Robinson, M., Jones, K., Janicke, H. and Maglaras, L., 2018. An introduction to cyber peacekeeping. Journal of Network and Computer Applications, 114, 70-87.

Within the Irish Government's 4 Ps strategy: Prevention, Participation, Protection and Promotion it will be vital that a cybersecurity element will be created, noting that whatever the mission is within peacekeeping, the first and foremost task is always to defend and 'preserve' peace'[52].

Key Term[53] [54]	Definition	Irish Application (4P's)[55]
Adoption	If cyber peacekeeping can be demonstrated to work within the established framework, decision makers are more apt to adopt it	Participation and Promotion Having all key groups round the table Using the domestic framework set out by the National Cyber Security Centre As well as current peacekeeping frameworks
Comprehension	By understanding existing doctrine, it is more likely proposed ideas will address issues significant to peacekeeping operations.	Participation and Prevention Observation, Monitoring and Reporting Aid socio-economic recovery Restore State Authority Protection and promotion of human rights
Integration	By sharing a common approach, cyber peacekeeping is flexible enough to either operate alone or as part of a "boots on the ground" peacekeeping operation	Protection Disarmament, Demobilisation and Reintegration Security sector Reform Electoral Assistance Malware clearance / responsible publication

Figure 1: compiled using the Tallinn Manual on the International Law Applicable to Cyber Warfare; NATO's Cyber Defence Principles; and Department of Foreign Affairs and Trade Strategy 2017-2020

As Robinson, Jones, and Janicke note, current UN peacekeeping doctrines will need to be altered to apply to conflicts involving digital elements. To quote, "Organizations such as the UN will find it an increasing necessity to operate in cyberspace in order to maintain peace."[56] How can this be achieved and what role could Ireland play? Any cyber peacekeeping activity will need to observe and respond to potential violations of ceasefire agreements and ensure incidents are responded to.

[52] Department of Foreign Affairs and Trade, Statement of Strategy 2017-2020, [Accessed on 25.07.2019] https://www.dfa.ie/media/dfa/alldfawebsitemedia/aboutus/DFAT-Statement-of-Strategy-2017-2020.pdf

[53] The International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press

[54] North Atlantic Treaty Organization, Cyber Defence, NATO, 16. July.2018 [Accessed on 25.07.2019] https://www.nato.int/cps/en/natohq/topics_78170.htm

[55] Department of Foreign Affairs and Trade, Statement of Strategy 2017-2020, [Accessed on 25.07.2019] https://www.dfa.ie/media/dfa/alldfawebsitemedia/aboutus/DFAT-Statement-of-Strategy-2017-2020.pdf

[56] Robinson, M., Jones, K., Janicke, H. and Maglaras, L., Op Cit, 70-87.

This task not only reflects observation, monitoring and reporting activities currently carried out by UN Peacekeepers but also the work carried out domestically by the National Cyber Security Centre (NCSC)[57]. The NCSC could gain international recognition and be utilised to undertake work securing systems and responding to incidents within an EU/UN context by becoming a global centre of excellence that ensures the validation and continued verification of ceasefire agreements in societies affected by cyberwarfare[58] [59].

Working with domestic and international partners, Ireland could ensure that risks to the digital infrastructure of post-conflict societies are recorded and mitigated appropriately[60]. As Robinson, Jones, and Janicke posit, this activity could be extended to include monitoring the cessation of cyber attacks, maintaining a register of compromised systems, known vulnerabilities and attacks and assisting with the reestablishment of critical systems and the dismantling of botnets, malware etc.

Robinson, Jones, and Janicke also suggest that this activity is akin to the UN policies of creating buffer zones and Disarmament, Demobilisation and Reintegration, in which cyber peacekeepers improve cybersecurity in areas under their control by rendering systems safe through the dismantling of malware and holding attackers to account[61]. At present there is no mechanism to gain access to international and national IT systems for these purposes.

Furthermore, Robinson, Jones and Janicke suggest that the United Nations could fund and develop a framework in which service providers could be approached to aid in the attribution of cyber attacks (Robinson et al, 2018). For example, this would be similar to how Interpol currently assists member states efforts by coordinating and delivering specialised policing services to ensure that transnational cybercrimes are combatted[62].

This allows a society afflicted by digital conflict to be reintegrated into peacetime activities and the wider global ecosystem. As such, future peacekeepers should not only improve cybersecurity in a given area but also ensure that local capacity is developed to maintain cyber peace once peacekeepers have left [63] [64].

Ireland could be a leading voice within the EU and PESCO framework on how cyber peacekeeping will be needed within the new era of blended warfare and how societies can be restored following such conflict. Ireland can work towards this through its international links and domestic institutions, while the EU should be at the heart of its development and implementation.

The Irish Government and Defence Forces should consider being a part of the *Cyber Threats and Incident Response Information Sharing Platform* and *Cyber Rapid Response Teams and Mutual Assistance in Cyber Security*. A new resolution adopted by the EU parliament on 12 March 2019

[57] Mission Statement, 'National Cyber Security Centre', Department of Communications, Climate Action and Environment, 2019 [Accessed on 25.07.2019] https://www.dccae.gov.ie/en-ie/communications/topics/Internet-Policy/cyber-security/national-cyber-security-centre/Pages/National-Cyber-Security-Centre.aspx

[58] Ibid.

[59] Robinson, M., Jones, K., Janicke, H. and Maglaras, L., Op Cit,.70-87..

[60] Steve Ranger, What is cyberwar? Everything you need to know about the frightening future of digital conflict, In ZD Net, 4 December 2018 [Accessed on 25.07.2019] https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/

[61] Robinson, M., Jones, K., Janicke, H. and Maglaras, L.,Op Cit, 70-87.

[62] Interpol, Our Cyber Operations, https://www.interpol.int/en/Crimes/Cybercrime/Our-cyber-operations [Accessed on 25.07.2019]

[63] TechRepublic, Cyberwar and the future of cybersecurity TechRepublic, 2018 [Accessed on 25.07.2019] https://www.techrepublic.com/resource-library/whitepapers/special-report-cyberwar-and-the-future-of-cybersecurity-free-ebook/

[64] Robinson, M., Jones, K., Janicke, H. and Maglaras, L., Op Cit, 70-87.

on building EU capacity on conflict prevention and mediation (2018/2159(INI)) has not included the threat cyber security issues present and potentially damage the preservation of peace[65].

Conclusion

Based on the arguments in this paper it is vital that an EU state institution should be taking the lead.

Furthermore, this paper posits that Ireland is in a prime position to fulfil this role based on its experience of UN peacekeeping, its domestic digital infrastructure and its developing role within PESCO. Based on EU requirements grounded on its foreign policy relating to conflict and post-conflict societies, it will be vital in a world created by technology, that responses to technological events will be required to also preserve the *physical* world and the societies which will need diplomatic and military assistance.

The National Cyber Security Centre's Computer Security Incident Response Team stated as part of its mission to "seek international recognition… in the respective government and national CSIRT communities so that it can effectively undertake its work on situational awareness and incident response'. Ireland can achieve this aim because it has the mechanisms and expertise to utilize both strategies together to realise a vision for aiding other nations who have been through a period of cyber conflict.

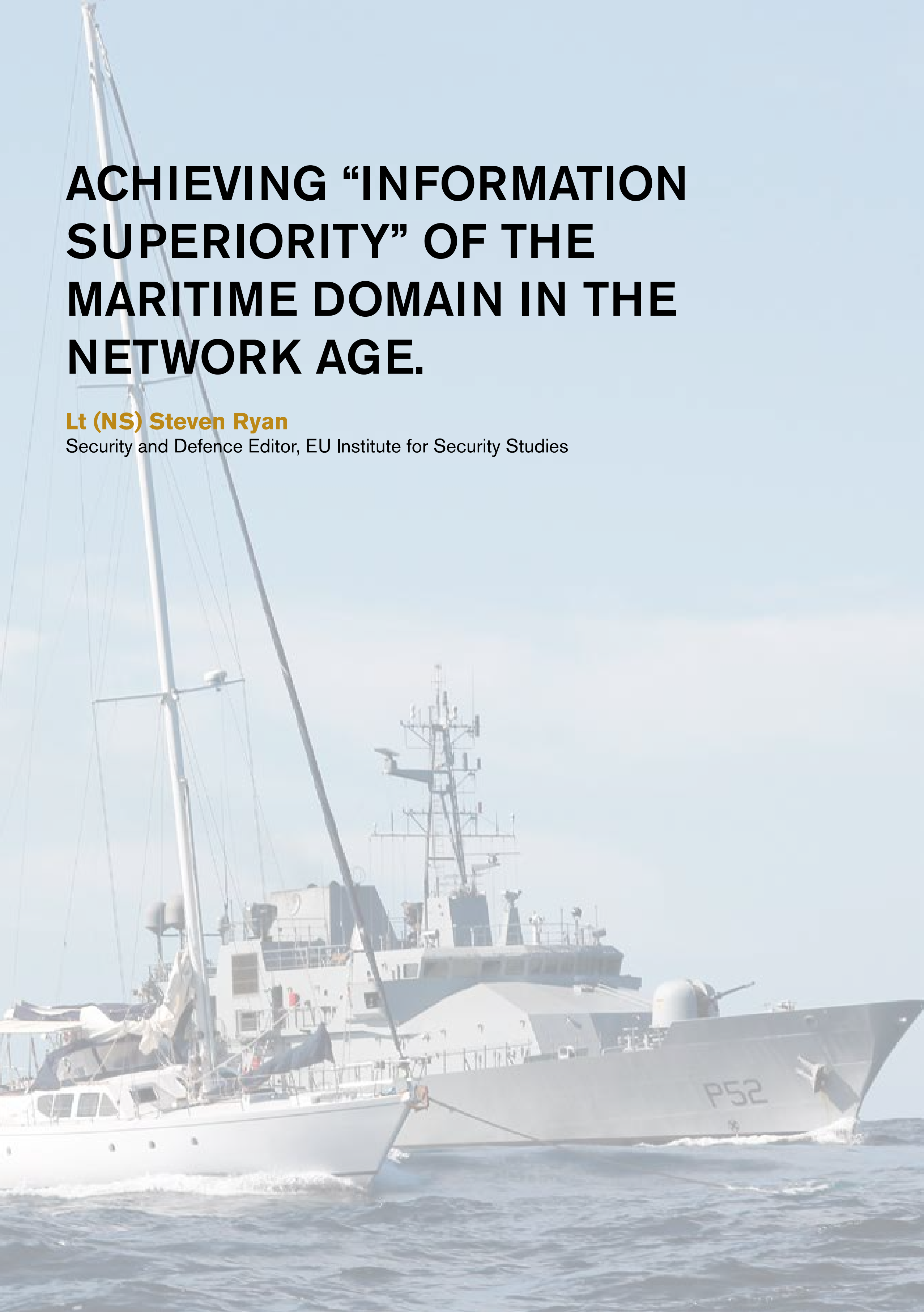
This paper has proposed a concept of how this approach and international institutions can work together. It seeks to instigate a timely discourse on cyber peacekeeping and the role smaller nations can play. Such an approach should be integrated into *The Irish Defence Force*, *National Cyber Security Centre* and the *Department of Foreign Affairs and Trade* working group on Ireland's post-conflict Model.

There are clear potential benefits including transparency, ease of collaboration, information sharing and the potential for states to contribute their cyber expertise – and experts – without diminishing their capability at home.

[65] European Parliament, European Parliament resolution of 12 March 2019 on building EU capacity on conflict prevention and mediation (2018/2159(INI)), [Accessed on 25.07.2019] http://www.europarl.europa.eu/doceo/document/TA-8-2019-0158_EN.html

ACHIEVING "INFORMATION SUPERIORITY" OF THE MARITIME DOMAIN IN THE NETWORK AGE.

Lt (NS) Steven Ryan
Security and Defence Editor, EU Institute for Security Studies



Abstract

Naval warfare is platform centric and the 22nd century Naval Service (NS) will increasingly rely on information and communications technology (ICT) to enable these platforms to achieve mission success. Leveraging technology to enhance capabilities at sea and ashore will allow this to be conducted more efficiently. The NS use of the Sitaware suite to achieve sensor feed integration, ship-shore connectivity, and decision support, is a small scale example of the concept of network-centric warfare (NCW) in the Defence Forces.

Introduction

Exploiting the advances in technology over time and integrating them into a C4ISR system will allow the NS to gain full situational awareness across domains, and achieve “information superiority” over an opponent, whether they are state or non-state actors. Ship launched remotely piloted aircraft systems (RPAS) will wirelessly feedback video data to operators in a VR environment, acquire targets and enable over-the-horizon engagements, while supporting command decisions. Copernicus satellites currently produce visual imagery and synthetic aperture radar returns of the sea surface with access times dependent on priority. Indigenously developed Cubesats with AIS and radar signal detection software will directly feed NS operations and allow the NS to call upon near real time satellite data, fed through correlation software, and then into Sitaware. Vessel wake analysis programmes will determine course and speed of vessels who do not correlate to AIS/VMS tracks allowing NS operations to direct interception assets.

The future NS platform will require significantly increased bandwidth to rely on the integrated communications infrastructure and multi-sensor data fusion necessary to achieve and maintain this “information superiority”. Maintaining this network access will involve developing defensive capabilities in the cyber and electromagnetic domains with the resulting requirement for the seagoing warfighter to be both sailor and network manager, necessitating the remodelling of the Irish professional military education system.

The Need for Maritime Surveillance

Maritime security is a pressing issue for any coastal state, and the requirements of international law to enforce both national and international legislation along this coastline and outwards into jurisdictional waters pose a challenge for the agencies tasked with this mission. In order to fulfil this mission, all available resources must be utilised. The modern maritime security field is helped by an abundance of technologies across all domains and the Irish Naval Service (NS) makes use of these when patrolling Irish waters. Due to the vast expanse of sea area it is impossible to be in all places at once.

As a signatory to United Nations Convention on the Law of the Sea (UNCLOS) and an island nation, Ireland possesses a significant maritime jurisdiction relative to its land area. The extension of the continental shelf westwards into the Atlantic gives Ireland a strong claim under UNCLOS to extend our Exclusive Economic Zone (EEZ) westwards to an area of over 490,000 square kilometres, a significant area to be managed [1]. With a nine ship fleet and maintenance and crewing requirements limiting the number of operational sea days per ship per annum, it is vital for the NS to gain every advantage from technology to enforce jurisdictional control of the Irish EEZ and maintain maritime situational awareness. This shift is ongoing with the increasing use of a C4ISR suite, Symantec Sitaware, and the employment of remotely piloted aircraft systems (RPAS) in overseas operations to expand the NS ability to conduct maritime surveillance.

Current and Future Threats in the Maritime Domain

The contemporary security environment is vast and global. Law enforcement and state security agencies need to utilise all available resources to combat the ever increasing threats. In terms of the maritime security environment, the potential risks are numerous. Human trafficking, drug and illegal goods smuggling, and illegal, unreported, and unregulated (IUU) fishing are some of the major challenges facing maritime law enforcement agencies[2]. The increasing availability of commercial off the shelf (COTS) products that would previously have been the domain of state organisations are levelling the battlespace for non-state actors who exploit smuggling and IUU activities at sea. A specific example would be how these actors can use numerous ways to hide or spoof a vessels position: Global Positioning System (GPS) offsets, where the GPS receiver software is modified to change the vessel’s position; switching off automatic identification system (AIS); interfering with communications or communications jamming, that is blocking or modifying the signal; or not reporting into coastal states at compulsory radio call in points[3].

Vessels can use a technique known as meaconing, which is a system of receiving radio beacon signals from NAVAIDs and rebroadcasting them on the same frequency to confuse navigation, or mask their position[4]. This process can be used to rebroadcast an AIS or other identifying signal to generate a false location for the vessel. With all the spoofing methods available to bad actors, the one thing a ship cannot hide is its visual presence[5]. Once it is seen by a patrol vessel or aircraft it can be identified, risk determined, and then the vessel can be tracked and followed; the same concept applies to stealth vessels, a plane or ship that is “near-invisible” to radar can still be seen with the naked eye[6]. Countering these threats as they evolve will require investment in new and upcoming technologies and better connectivity between seagoing units and shore based command.

[1] Department of Housing Planning and Local Government, “Towards a Marine Spatial Plan for Ireland,” 2017, www.housing.gov.ie.

[2] Christian Bueger, “What Is Maritime Security?,” *Marine Policy* 53 (March 1, 2015): 159–64.

[3] Nina Louisa Remuss, “Space and Maritime Security-Strategies for Countering the Pirates,” *Space Policy* 26, no. 2 (2010): 124–25.

[4] US Army, “FM 24-33 Communications Techniques: Electronic Counter-Countermeasures,” 1990.

[5] Jonathan F Solomon, “Maritime Deception and Concealment: Concepts for Defeating Wide-Area Oceanic Surveillance-Reconnaissance-Strike Networks,” *Naval War College Review* 66, no. 4 (2013): 87–116, https://doi.org/10.2307/26397418.

[6] Urška Kanjir, Harm Greidanus, and Krištof Oštir, “Vessel Detection and Classification from Spaceborne Optical Images: A Literature Survey,” *Remote Sensing of Environment* 207 (2018): 1–26, https://doi.org/10.1016/j.rse.2017.12.033.the number of studies based on optical satellite data is quickly growing. Altogether we analysed 119 papers on optical vessel detection and classification for the period from 1978 to March 2017. We start by introducing all the existing sensor systems for vessel detection, but subsequently focus only on optical imaging satellites. The article demonstrates the temporal development of optical satellite characteristics and connects this to the number and frequency of publications on vessel detection. After presenting the methods used for optical imagery-based vessel detection and classification in detail, along with the achieved detection accuracies, we also report possibilities for fusing optical data with other data sources. The studied papers show that the most common factors greatly influencing the vessel detection accuracy are the following: different weather conditions affecting sea surface characteristics, the quantity of clouds and haze, solar angle, and imaging sensor characteristics. All these factors bring great variations in the selection of the most suitable method; some still continue to pose unsolved challenges. For higher relevance and wider usage, we suggest that the algorithms for detection and classification should support a variety of targets and meteorological conditions, and ideally also a variety of optical satellite sensors. At least, they should be tested on many images under different conditions. This is not usually the case in the existent literature. We also observed that many authors omit an appropriate performance quantification, which is critical for a practical assessment and a numerical comparison of the presented algorithms. Overall it can be seen that vessel monitoring from spaceborne optical images is a popular research topic and has a great operational potential in the near future due to the large amount of satellite data, much of it free and open.

Advancing Current Technology Assets

Naval warfare is platform centric and the 22nd century NS will increasingly rely on information and communications technology (ICT) to enable these platforms to achieve mission success. Leveraging technology to enhance capabilities at sea and ashore will allow this to be conducted more efficiently. The NS currently operations Phantom 4 Pro drones with an air time of approximately 28 minutes and are can be operated in light weather conditions. While they can enhance the visual detection abilities of the ship, their 'time on-station' limits the extent to which they can constantly update the tactical picture. Improvements in battery capacity and high-strength lightweight plastics will permit enhanced 'time on-station', thus resulting in a future scenario where ship launched RPAS will enable over-the-horizon engagements, while supporting command decisions for the full duration of an operation. Advancements in virtual reality and augmented reality can integrate these video feeds into an operations room allowing the command team to visualise the target and allow for better planning.

The European Commission's Copernicus earth observation programme and its Sentinel satellites currently produce high resolution visual imagery and synthetic aperture radar (SAR) returns of the sea surface with access times dependent on priority[7]. These images are accessible by partner nations and can be utilised for maritime surveillance, however due to limited satellite paths and image processing time, by the time the image can be observed in an operational setting it can be significantly out of date, up to several days[8]. Future programmes may possess a near real time earth observation and surveillance satellite constellation over European waters, which in conjunction with satellite AIS will allow the creation of a clear maritime situational awareness picture[9].

Satellite technology is becoming increasingly compact and accessible to smaller nations and organisations. Ireland has the potential to be a maritime and technology research and development hub and is well placed to progress this technology. Ireland is poised to launch its first satellite in mid-2020. The Educational Irish Research Satellite-1 (EIRSAT-1) is a CubeSat, a small satellite around the size of a shoebox, and will be used for educational research. However, it is not beyond the realm of possibility that Ireland could launch its own SAR satellite in the future, or launch a satellite as part of a European maritime surveillance satellite cluster[10].

The European Maritime Surveillance (MARSUR) project, of which Ireland is a member, allows rapid information sharing across seventeen European nations to share information such as ship positions, tracks, identification data, or images[11]. The infrastructure is already in place to share this information and integrating satellite imagery and radar information can add a

[7] Carlos Santamaria et al., "Mass Processing of Sentinel-1 Images for Maritime Surveillance," *Remote Sensing* 9, no. 7 (July 2, 2017): 678, https://doi.org/10.3390/rs9070678.

[8] Nina Louisa Remuss, "Space and Maritime Security-Strategies for Countering the Pirates," *Space Policy* 26, no. 2 (2010): 124–25.

[9] Iraklis Oikonomou, "'All u Need Is Space': Popularizing EU Space Policy," *Space Policy* 41 (2017): 5–11.

[10] UCD, "EIRSAT-1," 2018, https://www.eirsat1.ie/.

[11] Basil Germond and Celine Germond-Duret, "Ocean Governance and Maritime Security in a Placeful Environment: The Case of the European Union," *Marine Policy* 66 (2016): 124–31.this article proposes that ocean governance and maritime security have translated into states' and regional organisations' increasing control over maritime spaces. This leads to a certain territorialisation of the sea, not so much from a sovereignty and jurisdictional perspective but from a functional and normative perspective. The article starts by discussing the ways oceans have been represented and shows that they are far from a placeless void, both in practice and in discourse. The article then frames the analysis of ocean governance and maritime security within critical geopolitics, and elaborates on the case of the European Union's narrative and practice. It concludes on the mutually reinforcing link between discourse and practice in the field of ocean governance and maritime security in general, and on the consequences for the EU in particular. Scholars working on ocean governance and maritime security are encouraged to challenge the traditional view that oceans are placeless.

vital confidence and certainty to the available information[12]. The technology to determine ship heading and speed has been tested[13] and the ability to discern vessels against backgrounds is constantly improving[14]. This continuous development in satellite technology and quality is matched by improvements in the ground based segment of the system where the analysis takes place. Recent tests have shown a dramatic increase in the turnaround time of this information; that is the time from the satellite taking an image to it being sent to the ground station, analysed and interpreted, and then sent to an end user, be they military or other state agency [15]. Due to the large distances involved and the limited speed of vessels, the data need not be available instantaneously, however, the sooner it is available, the better it can contribute to the decision making process. The more quickly this information is made available to the end user, the more valuable it is.

As an example, Norway is already developing and launching indigenous AIS detection and radar detection satellites for its NorSat constellation, a geostationary maritime surveillance network for monitoring its EEZ[16]. By including navigational radar which, in addition to AIS, is required by international law, the ability to hide or falsify a vessel position will be greatly reduced, and NorSat can help verify that ships in traffic meet those regulations. In the future Irish maritime environment, indigenously developed Cubesats with AIS and radar signal detection software will directly feed NS operations and allow the NS to call upon near real time satellite data, fed through correlation software, and then into Sitaware. Vessel wake analysis programmes will determine course and speed of vessels who do not correlate to AIS/VMS tracks allowing NS operations to direct interception assets.

Network-Centric Warfare and the Naval Service

The NS use of the Sitaware suite to achieve sensor feed integration, ship-shore connectivity, and decision support, is a small scale example of the concept of network-centric warfare (NCW) in the Defence Forces. NCW aims at increasing the efficiency of the transfer of maritime information among participating units (or nodes)[17]. NS elements operating as part of a Task Group whether on counter narcotics operations or other missions need to be able to share

[12] BOSILCA Ruxandra-Laura, "The Use of Satellite Technologies for Maritime Surveillance: An Overview of EU Initiatives," *Incas Bulletin* 8, no. 1 (2016): 151–61.

[13] Maria Daniela Graziano, Marco D'Errico, and Giancarlo Rufino, "Ship Heading and Velocity Analysis by Wake Detection in SAR Images," *Acta Astronautica* 128 (2016): 72–82.

[14] Haibo Wang et al., "Detecting Ship Targets in Spaceborne Infrared Image Based on Modeling Radiation Anomalies," *Infrared Physics and Technology* 85 (2017): 141–46.

[15] Kanjir, Greidanus, and Oštir, "Vessel Detection and Classification from Spaceborne Optical Images: A Literature Survey."the number of studies based on optical satellite data is quickly growing. Altogether we analysed 119 papers on optical vessel detection and classification for the period from 1978 to March 2017. We start by introducing all the existing sensor systems for vessel detection, but subsequently focus only on optical imaging satellites. The article demonstrates the temporal development of optical satellite characteristics and connects this to the number and frequency of publications on vessel detection. After presenting the methods used for optical imagery-based vessel detection and classification in detail, along with the achieved detection accuracies, we also report possibilities for fusing optical data with other data sources. The studied papers show that the most common factors greatly influencing the vessel detection accuracy are the following: different weather conditions affecting sea surface characteristics, the quantity of clouds and haze, solar angle, and imaging sensor characteristics. All these factors bring great variations in the selection of the most suitable method; some still continue to pose unsolved challenges. For higher relevance and wider usage, we suggest that the algorithms for detection and classification should support a variety of targets and meteorological conditions, and ideally also a variety of optical satellite sensors. At least, they should be tested on many images under different conditions. This is not usually the case in the existent literature. We also observed that many authors omit an appropriate performance quantification, which is critical for a practical assessment and a numerical comparison of the presented algorithms. Overall it can be seen that vessel monitoring from spaceborne optical images is a popular research topic and has a great operational potential in the near future due to the large amount of satellite data, much of it free and open.

[16] Norsk Romsenter, "Norway's Satellites - Norsk Romsenter," Norwegian Space Agency, 2018, https://www.romsenter.no/eng/Norway-in-Space/Norway-s-Satellites.

[17] Paul T Mitchell, "Small Navies and Network-Centric Warfare: Is There a Role?," *Naval War College Review* 56, no. 2 (2003): 83–99.

target information and tracking both within the Defence Forces and with foreign military partners. Information sharing is the backbone of modern military cooperation[18].

How Information Superiority Defeats Maritime Threats

Traditionally, navies have practiced a system of decentralized C2 owing to the vast distances involved and the difficulty of maintaining constant lines of communication. By contrast, the modern networked and multi-domain environment create a new context within which C2 will be practiced at sea[19]. Exploiting the advances in technology over time and integrating them into a C4ISR system will allow the NS to gain full situational awareness across domains, as part of a joint common operating picture between the Defence Forces component services, and achieve "information superiority" over an opponent, whether they are state or non-state actors. This is only achievable with the focused development of technological solutions and commitment to system upgrades to maintain a competitive edge, and through cooperation with allies[20]. Through PESCO, Ireland is a member of the Upgrade of Maritime Surveillance project which aims to "*enhance the Maritime Surveillance, Situational Awareness and potential Response Effectiveness of the EU, by using the existing infrastructure, deploying assets and developing related capabilities in the future*"[21]. This increased cooperation helps offset the large capital expenditure required to develop and maintain the data centres and computing technologies and ship hardware upgrades that enable NCW.

Future Challenges

The future NS platform will require significantly increased bandwidth to rely on the integrated communications infrastructure and multi-sensor data fusion necessary to achieve and maintain this "information superiority". Cybersecurity and cyber defence will be a major tenet of future naval operations, as once the link to other units or information sharing platforms such as a C4ISR system is cut, the ability to conduct NCW and maintain a full spectrum operational picture dissipates[22]. A dedicated cyber division on board ships will be required to maintain this network access and will be involved in the development and deployment of defensive capabilities in the cyber and electromagnetic domains with the resulting requirement for the seagoing warfighter to be both sailor and network manager, necessitating the remodelling of the Irish Naval Service professional military education (PME) system. In order to maximise the advantages granted by technological solutions, a commitment to upgrade both hardware and software is required. The capital cost of this is one of the barriers to maintaining NCW capability in small navy. In order for the NS to operate in a NCW environment and utilise available technologies, a considerable investment in training will be required at all ranks, from operator to maintainer level. This will require modifying the training environment, with the use of augmented or virtual reality settings to facilitate training while allowing ships to remain at sea.

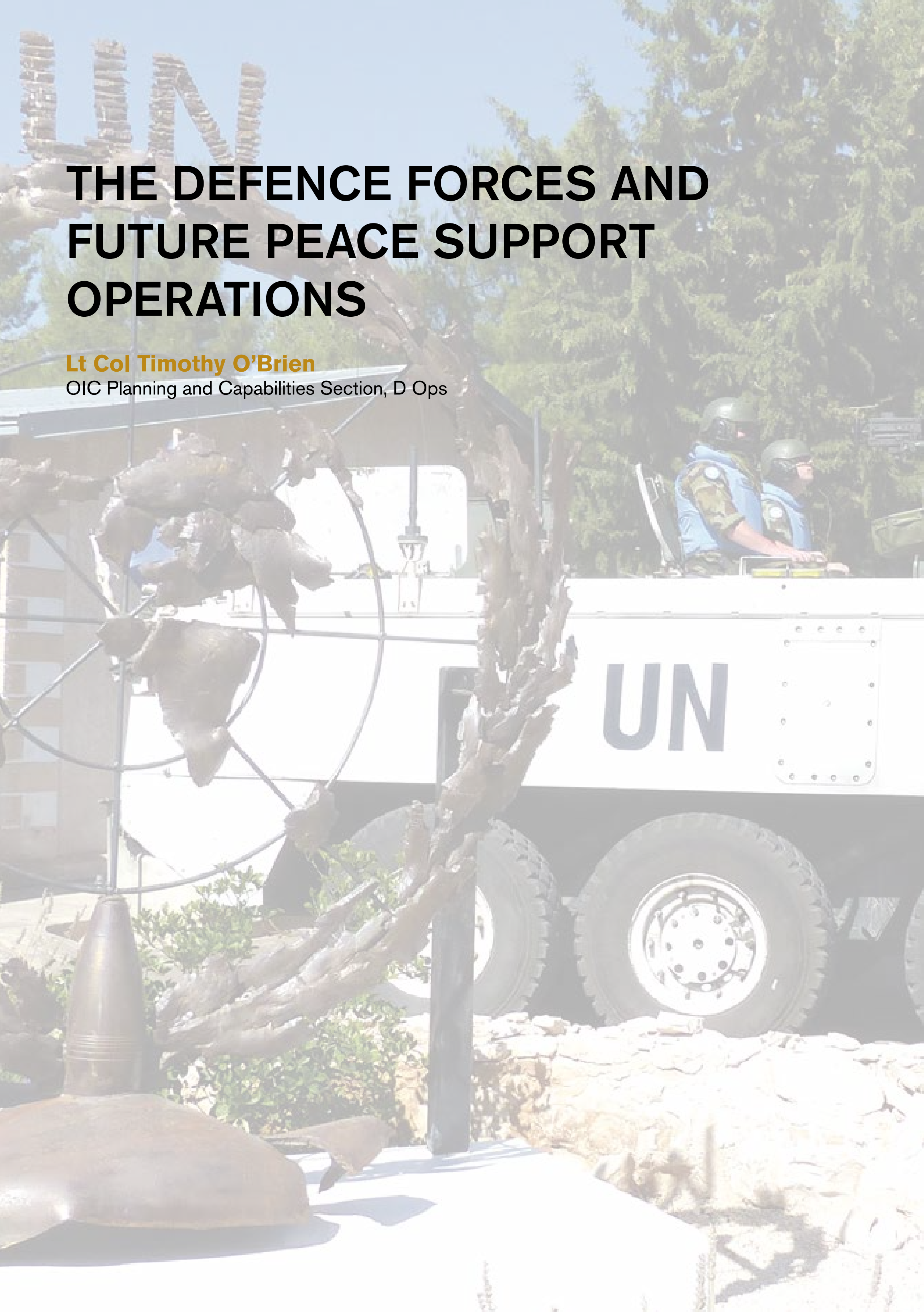
[18] Stephanie Hszieh et al., "Networking the Global Maritime Partnership," *Naval War College Review* 65, no. 2 (2012): 10–29.
[19] Robert C Rubel, "Mission Command in a Future Naval Combat Environment," *Naval War College Review* 71, no. 2 (2018): 109–21.
[20] Patrick M Stillman, "Small Navies Do Have A Place in Network-Centric Warfare," *Naval War College Review* 57, no. 1 (2004): 95–101.
[21] "Upgrade of Maritime Surveillance | PESCO," accessed June 30, 2019, https://pesco.europa.eu/project/upgrade-of-maritime-surveillance/.
[22] Peter Dombrowski and Chris C. Demchak, "Cyber War, Cybered Conflict, and The Maritime Domain," *Naval War College Review* 67, no. 2 (2014): 70–96.

Conclusion

The future NS structure will have to adapt to and exploit the increasing tactical and operational advantages that technology provides, while developing doctrine to ensure effect use of these systems across multiple domains. Due to the ever changing nature of NCW and fast-paced technological developments, a robust research and development organisation will be required to bridge the gap from trial to full implementation in the NS. The integration of these concepts at the earliest stage of training and platform development, supported at all levels, will be crucial in the ability to attain and maintain information superiority over an adversity.

THE DEFENCE FORCES AND FUTURE PEACE SUPPORT OPERATIONS

Lt Col Timothy O'Brien
OIC Planning and Capabilities Section, D Ops



Abstract

Although the grandparents of Defence Forces personnel who will serve on 22nd Century Peace Support Operations (PSO) have yet to be born it is arguable that attempting to predict future PSO challenges is worthwhile. Predicting the future is of course impossible but perhaps the best way to proceed is by analysing current PSO challenges.

The Defence Forces 60-year PSO journey has taken us from the traditional peacekeeping operations of the Cold War, through the regional peace enforcement operations of the 1990s, to today's multidimensional crisis management operations. While the bulk of our peacekeepers remain infantry, our response to PSO has evolved from only sending infantry units abroad during the Cold War, to dealing with the challenges of the 1990s onwards by using a combination of transport, military police, naval, special forces and medical units, complemented by today's training teams, experts in consular security and on island stand by forces. Future PSO may see the Defence Forces having to conduct counter insurgency operations in Africa, deal with the effects of migration and climate change on the EU's southern borders and assist Irish citizens worldwide on Non-combatant Evacuation Operations.

An innovative use of our limited resources and budgets will be essential and this may, for example, see the RDF being used to enhance our limited language capabilities and to increase the number of female personnel we deploy, or the Naval Service and Air Corps only procuring vessels and aircraft that can conduct joint PSO operations with the Army and Army Ranger Wing. Members of the artillery corps currently use UAV technology on PSO in the Democratic Republic of the Congo and this is a prime example of how in the future we will have to turn to technology to enhance our effectiveness on PSO.

Introduction

> *"The future security environment cannot be predicted with certainty."*[1]

On 24 June 2018 the Irish state marked the 60th anniversary of Defence Forces' participation in United Nations (UN) led or mandated Peace Support Operations (PSO) with a ceremony in Dublin Castle attended by President Michael D. Higgins. In his address to veteran and serving peacekeepers, President Higgins highlighted how over six decades nearly 66,700 individual members of the Defence Forces had served in peace support missions in Europe, Africa, the Middle East, Asia and South America and how this participation marked a tangible demonstration of Ireland's commitment to the pursuit of international peace[2]. This paper will use that anniversary, which shone a light on the demanding PSO conducted by the Defence Forces from the second half of the 20th century onwards, as a platform to consider what PSO challenges future generations of the Defence Forces may face and what role innovation, and in particular innovation in military education, future structures of the army and the role of the Reserve Defence Forces (RDF), is likely to play in determining how they will plan, train for and execute PSO.

[1] Irish Government White Paper on Defence, (2015).

[2] 'Address on 60 Years of Peacekeeping, Dublin Castle, 24 June 2018', President of Ireland. Last modified June 20, 2019. https://president.ie/en/media-library/speeches/address-on-60-years-of-peacekeeping

An uncertain future global environment

The roles of the Defence Forces, including their participation on PSO, are determined by government policy. The 2015 White Paper on Defence, which outlines Ireland's current defence policy, describes an uncertain security environment facing the state, encompassing several overarching trends which are likely to have implications for the Defence Forces in the years ahead. These include the evolving nature of conflict to what is commonly characterised as hybrid warfare, the proliferation of weapons, the potential vulnerability of Ireland's sea transport routes, climate change, large scale illegal migration, energy and resource security, cyber-attacks, terrorism, transnational organised crime and what are described as unknown future threats or strategic shocks[3]. Preceding the White Paper by a matter of months the government also published its first review of foreign policy priorities since 2006 and this document bore witness to shifting patterns of global power and influence, conflicts, wars and terrorism, as well as new technologies facilitating instantaneous worldwide communication and a growing interdependence between economies, societies and people.[4] All of these highlighted concerns offer some food for thought in the years ahead for Defence Forces staff planning either capability development, future training requirements or equipment procurement.

Analysing the past to help predict future challenges

While the above concerns can serve as guides to anticipating potential tasks the Defence Forces may have to respond to as part of future PSO, this paper suggests that to speculate with any reasonable authority on future challenges it is also helpful to analyse and understand how throughout the last 60 years, but especially since the ending of the Cold War, Defence Forces involvement in PSO has seen constant change, unexpected challenges and a diversity of roles, all phenomena which there is no reason to believe will not continue into the coming decades.

The Defence Forces have participated in UN peacekeeping operations since 1958, when Ireland was asked urgently to deploy officers as part of an observation force to Lebanon, as a result of a deteriorating security situation resulting from that country's dispute with neighbouring Syria. The first of the Irish military observers deployed on 28 June 1958, only five days after the UN's request[5]. During the thirty years following that deployment, members of the Defence Forces took part in a myriad of what are now labelled traditional UN peacekeeping operations. These were of two types: either lightly armed infantry units deployed to separate warring parties in areas of operation as diverse as Congo, Cyprus, Sinai and from 1978 onwards, once again in Lebanon, or unarmed military observers sent to conflict zones worldwide including Afghanistan, Central America, the Middle East, Namibia, the Indian Pakistan border, Iran and Iraq[6].

[3] Department of Defence. *White Paper on Defence*. Dublin: Defence Forces, 2015.

[4] Department of Foreign Affairs and Trade. *The Global Island. Ireland's Foreign Policy for a Changing World.* Dublin, 2015.

[5] Heaslip, Richard. "Ireland's First Engagement in United Nations Peacekeeping Operations: An Assessment.*" Defence Forces Review* 5 (2008):12

[6] For an overview of the original or traditional peacekeeping operations see: Harbottle, Michael. *The Blue Berets – The Story of The United Nations Peacekeeping Forces.* London: Leo Cooper, 1975 and Smith, Raymond. *Under the Blue Flag,* Dublin: Aherlow Publishers, 1980.

Contemporary PSO

However, in the early 1990s, it became apparent to both the UN and the international community, especially following the Bosnian and Rwandan genocides, that the traditional model of peacekeeping that had served the organisation during the Cold War was no longer effective. Traditional peacekeeping operations were insufficient to deal with post-Cold War intra state conflict, where civilians rather than armed forces were deliberately targeted by armed groups conducting asymmetrical warfare.[7] These challenges required a new type of peacekeeping response and the UN reacted by gradually expanding its field operations from the traditional model, to today's complex multi-dimensional operations which are designed to ensure the implementation of comprehensive peace agreements and assist in laying the foundations for sustainable peace[8]. Although the military remain the backbone of most peacekeeping operations, there are now many faces to modern peacekeeping including police officers and a range of civilians such as legal experts, electoral observers, human rights monitors, civil affairs officers, gender advisors and governance specialists.[9] The Security Council mandates authorising these PSO have also changed and today 95% of all UN mandated peacekeepers are on missions where their priority tasking is no longer to monitor ceasefires or separate belligerents but rather the protection of civilians[10]. In 2019 Defence Forces personnel operate under such protection mandates in Lebanon, Mali and the Democratic Republic of the Congo.[11] The requirement to protect civilians is likely to continue well into the future as despite having been a mandated task for all new missions established since 1999 there are still thousands of civilians killed in armed conflict each year worldwide[12].

Examples of previous innovative PSO responses

While the term innovation might not necessarily have been used by the organisation in the early 1990s to describe how it was responding to the significant peacekeeping challenges outlined above, with the benefit of hindsight innovative responses can be traced to 1991 when Defence Forces personnel deployed on the organisation's first non-UN led peacekeeping operation. That was to the European Community's Monitoring Mission to the former Yugoslavia[13]. Over the next three decades the Defence Forces would continuously adapt to the demands of a variety of UN, EU and NATO-led PSO, by establishing, training and deploying a diverse range of units compiled of personnel with different skill sets to those of their Cold War predecessors. Since the end of the Cold War the Defence Forces have successfully deployed quick reaction forces as well as military police, transport, special forces and naval units on PSO, while the light infantry battalions of the Cold War have been replaced by mechanised equivalents which have significantly greater force protection, fire power, mobility and communications. Smaller specialist contingents such as training, liaison and medical teams have also deployed

[7] For an example of such a conflict see Jean-Pierre Lacroix, "Peace, progress and potential: The legacy of UN Peacekeeping in Liberia, Côte d'Ivoire and Sierra Leone, *UN Peacekeeping*, July 19, 2018, https://medium.com/unpeacekeeping/peace-progress-and-potential-the-legacy-of-un-peacekeeping-in-liberia-c%C3%B4te-divoire-and-sierra-696ef83cb165.

[8] For the background and rationale to this shift see Durch, William J., Victoria K. Holt, Caroline R. Earle, and Moira K. Shanahan. The Brahimi Report and the Future of the UN Peace Operations. Henri L. Stimson Center,2003.

[9] Peace Operations Training Institute. *Protection of Civilians,* by Julian Harston, Williamsburg. 2016, 19-20.

[10] For details see "United Nations Peacekeeping." United Nations. Last modified June 29, 2019. https://peacekeeping.un.org/en/protecting-civilians

[11] On 20 June 2019 Dáil Éireann approved the deployment of Defence Forces personnel to a third mission with a protection of civilian's mandate. This was for the UN Mission in Mali. See Marie O'Halloran, 'Army Rangers set for Mali mission', *Irish Times,* 21 June 2019.

[12] For details of worldwide civilian casualties in 2017 see United Nations. Security Council. *Report of the Secretary General on the protection of civilians in armed conflict.* New York.14 May 2018.

[13] Daly, John. "Monitor Mission to Yugoslavia", *An Cosantóir* 51, No. 7(1991): 2.

as have experts in remotely piloted aircraft systems and disarmament, demobilisation and reintegration. The Defence Forces now also deploy specialist personnel, on request from the Department of Foreign Affairs and Trade, to Irish embassies worldwide to assist consular staff, normally during periods of heightened security or crisis management and since 2007 they have also participated in the EU's Battlegroups[14].

The potential face of future PSO

In the current decade the Defence Forces have engaged in several new types of PSO that give hints of the potential taskings that the coming decades might bring. The following four types of operation are examples:

Training Teams

In 2010 a military training team was deployed abroad for the first time as part of the EU Training Mission to Somalia. Its task was to train the emerging post-civil war Somalian national army. A similar team has been deployed to Mali since 2013 and in 2018, again for the first time, the Defence Forces deployed a UN requested mobile training and education team to Burkino Faso to assist that country's army's PSO pre deployment training for the UN Mission in Mali.[15] Therefore, this paper suggests that training post conflict militaries to international standards as well as assisting non-western militaries to operate in a PSO environment will become a significant role for the Defence Forces in the coming decades. It is perhaps worth noting from a planning perspective the importance that our nearest neighbours, the British Army, have given to such training operations. Their infantry corps has been restructured to create four specialised units which contribute to the United Kingdom's overseas defence engagement, by deploying a series of 12-man teams, each consisting of highly qualified soldiers, to train, advise, assist and mentor foreign militaries.[16]

Non-combatant evacuation

In 2011 the non-combatant evacuation of Irish citizens from Libya[17] saw the Air Corps deploy fixed wing aircraft abroad for the first time in a crisis management role. While that was a relatively small scale operation, larger evacuation operations involving Irish or indeed EU citizens would require an innovate use of limited Defence Forces resources in the coming years to procure appropriate vessels, vehicles and aircraft as well as training that would facilitate combined naval, air, land and special forces personnel that such off island operations may demand. Defence Forces planners considering the potential likelihood of such operations in the coming years, will have taken note of the 2019 decision of the Department of Foreign Affairs and Trade, to tender for the first time to procure the services of a global security company to provide it with worldwide security advice and assistance including evacuation at short notice for its officers and their eligible dependents. Media reports concerning this tender noted that

[14] For an overview of these operations see O'Brien, Timothy. "The Origins and Evolution of Defence Forces Peacekeeping", *An Cosantóir* 78, No. 5(2018): 12-14.

[15] Ibid., 12-14.

[16] For examples of these types of training missions see https://www.army.mod.uk/deployments/africa/

[17] For details of the successful evacuation of 115 Irish nationals and family members from Libya see https://www.dfa.ie/news-and-media/press-releases/press-release-archive/2011/march/successful-evacuation-irish-citizens-from-libya/-taoiseach-praises-successful-evacuation-of-irish-citizens-from-libya.php and Lally, Conor. "BBC interview may have made Smith's bid to get home more difficult", *Irish Times,* July 6, 2019:2.

Irish diplomatic staff currently operate in several regions with a recent history of instability including Sierra Leone, Palestine, South Sudan, Syria and the Central African Republic.[18]

Naval Operations

In May 2015 there was a momentous occasion for the Defence Forces, arguably of equal significance to the army's 1960 deployment to Congo, when the Naval flagship LÉ *Eithne* deployed to the Mediterranean to take part in, what were initially bilateral migrant rescue operations with the Italian navy, before the government subsequently approved follow on naval vessels to participate in the EU's naval force in the Mediterranean[19]. Naval vessels continued to deploy as part of that force until 2018 and this paper suggests that similar deployments are likely to occur in the coming years as Naval Vessels form part of multinational UN, EU or NATO-led maritime task forces.

Crisis Management Operations

In the same year Sierra Leone was almost overwhelmed by an outbreak of the Ebola virus in West Africa. The Defence Forces, on government direction for the first time, rather than at the request of an international organisation such as the UN or EU, deployed medical teams to assist in a British Army operation to counter the virus while simultaneously teams of logistics, engineering and security specialists reinforced the consular staff manning the Irish Embassy in Freetown[20]. Again, this paper suggests that similar operations, deploying the skill sets of specialists within the Defence Forces, will be a feature of future PSO.

PSO Professional Military Education

Within the Defence Forces the Military College is the principle institution responsible for the provision of training and doctrine to the organisation[21]. In 1993, as the Defence Forces faced the significant challenges, outlined above, resulting from the post-Cold War transformation of PSO, the first major change to the structure of the Military College since the early 1930s occurred when a new school was established to specialise in PSO pre-deployment training[22]. Twenty six years later the United Nations Training School Ireland (UNTSI) remains the location where both Defence Forces and foreign military personnel are educated to, amongst other things, understand how to protect civilians, and how, as military, they have to recognise and overcome the challenges posed by the necessity to work with civilian and police actors from a variety of different cultural backgrounds on complex multi-dimensional operations[23].

During 2018 two educational innovations occurred in the Military College which will benefit future contingents of Defence Forces personnel deployed on PSO.

The Joint Command and Staff Course

The introduction by the Command and Staff School of a new joint Command and Staff course will prepare the next generation of senior officers for PSO deployments while simultaneously

[18] Gallagher, Conor. 'Irish Diplomatic staff to get armed security', *Irish Times,* 31 August 2019.
[19] For an overview of these naval operations conducted see "Mission of Mercy", *Signal* 13, No.2 (2015): 19-23.
[20] Byrne, Karl. "Tackling Ebola", *An Cosantóir* 75, No. 2 (2015): 12-13.
[21] "The Military College." Irish Defence Forces. Last modified June 30, 2019. https://military.ie/en/who-we-are/army/defence-forces-training-centre/the-military-college/
[22] Hodson, Tom. *The College -The Irish Military College 1930-2000.* Dublin: The History Press Ireland, 2016.
[23] For information on courses run in the school see UNTSI. *UNTSI Course Prospectus 2019,* Dublin, Defence Forces Printing Press, 2018.

developing their understanding of single service, joint, combined and multi-agency operations. Given the overarching trends highlighted in the 2015 White Paper on Defence, the new course's training objectives include helping students to develop a comprehensive grasp of strategy, security, communications and defence in political, international and financial contexts. Graduates will have an enhanced understanding of the national and international context within which the Defence Forces operate, covering policy and strategy, diplomacy, politics, economics and military technological trends[24].

Security Sector Reform

A new PSO training initiative was also introduced by UNTSI during 2018. This was the first Security Sector Reform course to be run in the Defence Forces. This course formalised education within the organisation on the emerging topic of human security, while also giving students a comprehensive understanding of the more traditional state centric concept of the term. An understanding of human security will be essential on all future PSO undertaken by the Defence Forces as human security encompasses the important PSO cross cutting thematic issues of human rights, good governance, the protection of civilians, the gender perspective and the access by a population to basic services[25].

Planned innovation in military education

At the time of writing the Defence Forces are planning further innovative educational responses to help future peacekeepers face what are yet unknown challenges. A new strategic leadership course is being developed to cater for the educational needs of senior officers holding the rank of Colonel or equivalent[26], while a joint military and Department of Defence steering group are working with civilian consultants to evaluate the potential of a new Institute for Peace Support and Leadership Training. The latter initiative has its genesis in the 2015 White Paper on Defence which foresees such an Institute having an international standing while contributing to the overall development of knowledge and experience in the areas of peace support and conflict resolution. If developed, the White Paper foresaw the Institute building on and forging new educational partnerships with the world's leading universities while developing strategic partnerships with other appropriate organisations, including industry[27].

Other potential innovations to support future PSO

Education is not the only area where innovation can be employed to prepare members of the Defence Forces for the unpredictable PSO challenges that the future may hold. Two other suggested areas are:

Future Defence Forces Structures

This paper has noted how the British Army has restructured several of its infantry battalions so that they have the appropriate personnel resources to be able to conduct continuous train, advise, assist and mentor missions, primarily on the African continent. While within the

[24] '*The Military College Delivery of Professional Military Education*', PowerPoint Presentation delivered in Military College on March 11, 2019 to visiting New Zealand Armed Forces Delegation.

[25] The International Security Sector Advisory Team. *SSR in a Nutshell, Manual for Introductory Training on Security Sector Reform*, Geneva, 2016,1-13.

[26] '*The Military College Delivery of Professional Military Education*', Op CIt.

[27] Department of Defence. *White Paper on Defence*. Dublin: Defence Forces, 2015.

Defence Forces both the army and the naval service have a proven record of operating in a multinational environment, with the UN since 1958, the EU since 1991 and NATO since 1997, since the establishment in 1960 of the very first unit to serve overseas in the Congo, the army has, with minor exceptions[28], always chosen to establish new units to deploy overseas[29]. These units train, deploy and are then disestablished as soon as they return home. In many cases these units often bear no resemblance to those existing in the current Defence Forces structure. PSO units currently deployed by the army in Lebanon and Syria are in effect mechanised infantry heavy, all arms battlegroups[30], but such units do not exist in the army's established organisation. What this means in effect is that for each deployment of a unit overseas, commanders and staff officers throughout the army must expend considerable effort in establishing these units, normally by bringing together soldiers from a disparate number of units and locations. This is arguably an inefficient way to conduct force generation for PSO and this paper suggests that an important future innovation will be to restructure the army so that its units are equipped to conduct PSO, without extensive outside assistance.

The role of reservists

Members of the RDF have never served on PSO and the 2015 White Paper on Defence makes no reference to reservists deploying on PSO in the future. This is government policy[31]. However, looking forward to the coming decades, there is no reason why an organisation as small as the Defence Forces would not utilise the skill sets of individual members of the reserve to complement the permanent Defence Forces on PSO. On 13 July 2018, acknowledging the growing importance that the reserve plays in the organisation, the Chief of Staff announced that the army's Director of Combat Support and ISTAR would in future be also tasked with overseeing the RDF[32]. Commenting on his new role in September 2018 the new Director with responsibility for Reserve Forces stated that he was working to harness RDF skills and talent to maximise their development in the areas of training and operations.[33]This paper suggest that the organisation, as is currently the case with its EU counterparts, will not be able to ignore the skill sets and talents of the reserve in the coming decades when selecting personnel to serve on PSO and that it would be an innovative decision by government to change their policy on this matter.

Conclusion

On 28 June 2019, the 61st anniversary of the first PSO deployment, there were 676 members of the Defence Forces serving on UN, EU, OSCE and NATO led operations. They were deployed as mechanised infantry units in Lebanon and Syria, as military observers in Western Sahara and in the Middle East, as training teams in Mali and as land and maritime headquarter

[28] The deployment of the ARW to Liberia and Chad, as well as the deployment of ARW and Infantry Battalion personnel as part of a New Zealand Battlegroup to East Timor.

[29] This approach has its origins in the 1960 decision of the then Chief of Staff, Lt Gen Sean McEoin to task each of the army's Commands to provide an infantry company for 32nd Infantry Battalion. Speaking in 1995 Lt Gen McEoin stated that this was "the easiest possible way" to establish an overseas unit given the time constraints involved. In 1978 as the 43rd Infantry Battalion was being established to deploy to Lebanon, DFHQ planners considered "the possibility of making a break with the past and sending out an existing battalion, or at least basing the unit on an existing battalion". This possibility was however disregarded as being impractical for a diverse, but unrecorded set of reasons. See E.D Doyle, "The Beginning of UNIFIL", *An Cosantóir,* 48 (10), October 1998,8.

[30] A battlegroup, in the Defence Forces context, would consist of a combined arms battalion, reinforced with combat support and combat service support elements

[31] Department of Defence. *White Paper on Defence*. Dublin: Defence Forces, 2015.

[32] Fitzgerald, Wayne. "The Reserve Defence Forces Supporting the Front Line", *An Cosantóir* 78, No. 7 (2018): 13.

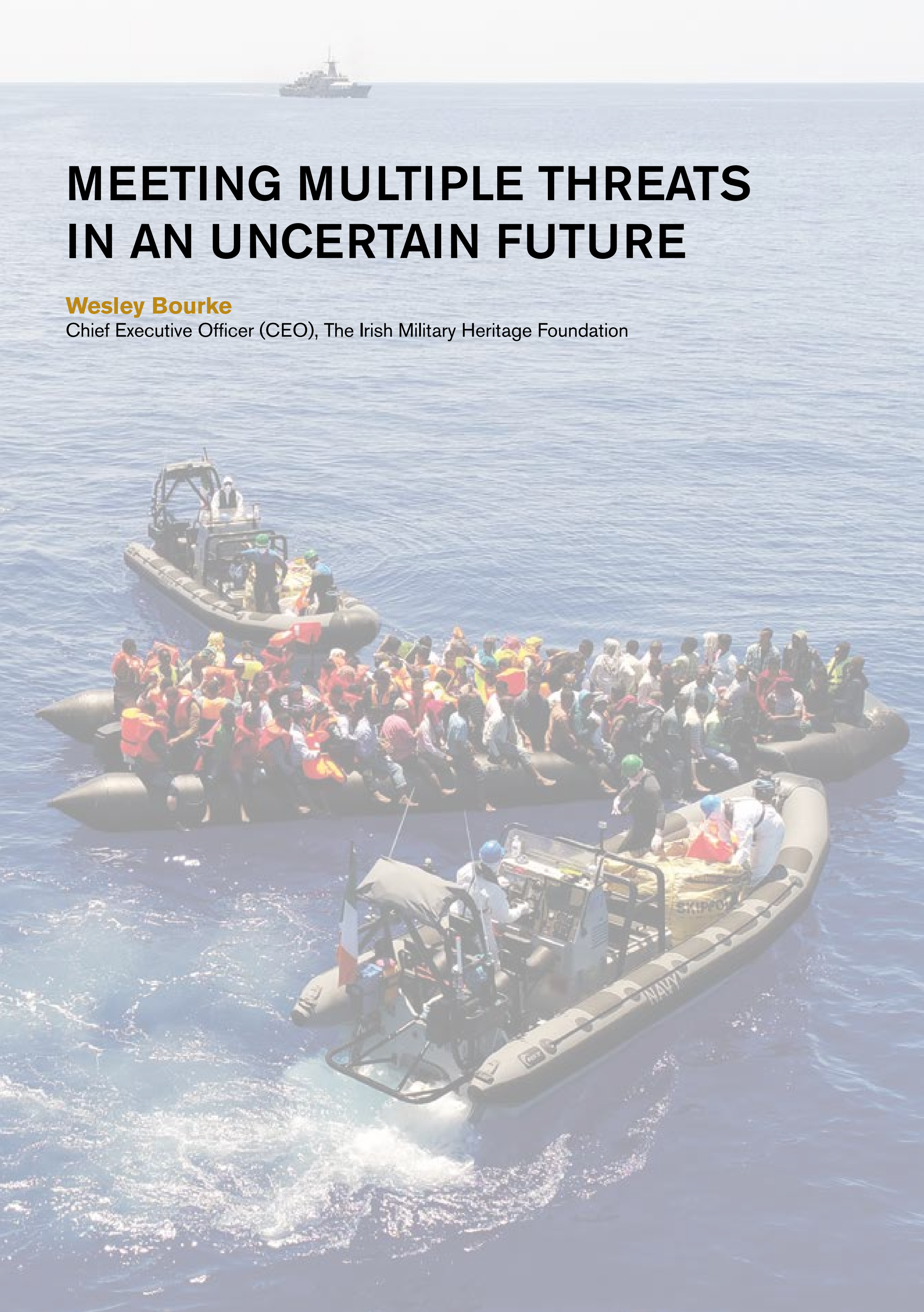
[33] Cleary, Brian. "Director with Responsibility for Reserve Forces", *Connect* 22, No.3 (2018):1

staff throughout Africa, the Middle East, the Mediterranean and the Balkans. At home, 152 soldiers were preparing to commence training for a German army led EU battlegroup,[34] while members of the Army Ranger Wing were preparing to deploy to the UN PSO in Mali[35]. The ability of the Defence Forces to conduct such a diverse range of operations is a function of their training, leadership and equipment. Additionally, this paper has demonstrated how the current generation of peacekeepers have innovatively built on the experience of their predecessors in responding to the demands of contemporary PSO. The paper has also highlighted how educational initiatives in the organisation are preparing the next generation of peacekeepers to deal with whatever challenges the future holds. Finally, in the spirit of innovation, the author has suggested some changes to the army's structure and to government policy on the RDF which would potentially enhance the ability of the Defence Forces to conduct PSO in the lead up to the 22nd century.

[34] O'Halloran, Marie. 'Dáil to debate Army's EU role', *Irish Times,*25 June 2019.
[35] O'Halloran, Marie. 'Army Rangers set for Mali mission', *Irish Times,*21 June 2019.

MEETING MULTIPLE THREATS IN AN UNCERTAIN FUTURE

Wesley Bourke
Chief Executive Officer (CEO), The Irish Military Heritage Foundation



Abstract

A new chapter in world history has opened filled with uncertainty. The defence and security environment have never been more obscure. China, Iran and Russia – are increasingly asserting themselves on the world stage; geopolitics is back.[1] A further challenge are Non-State Armed Group – Islamic State of Iraq and the Levant or trams-national drug traffickers for example – whose presence and impacts have destabilising effects regionally and globally. The use of hybrid threats - a combination of low risk activities including the use of organised crime, cyber-attacks, and information disruption – is becoming commonplace. The above challenges generally take place in a space regarded as the 'gray zone' resulting in strategic disruption rather than all-out war.

The challenges posed from the broader security spectrum - climate change, food security, bad governance for example – have risen substantially. They not only directly challenge a state's ability to provide for its people, but can become threat multipliers by interacting and converging with other existing risks and pressures thus increasing the risk of fragility or violent conflict.

In an era where traditional distinctions between defence and security are becoming increasingly blurred, what approach a state should take to meet the uncertainties of the 21st century is a prevailing question. In order to predict, prevent, and manage these challenges this paper promotes a holistic intergovernmental approach at an international level, mirrored with a whole-of-government approach at a national level. Such an approach will maximise all available resources to meet challenges head on.

Introduction – the Post-Cold War

Reacting to regional and international challenges in the 1990s and early 2000s – intrastate conflicts in the former Yugoslavia and the Al Qaeda attacks of 9/11 for example – it was realised no single state could tackle the changing security environment.[2] Relationships formed within intergovernmental organisations (IGOs); the European Union (EU), the North Atlantic Treaty Organisation (NATO), and the Organisation for Security and Co-operation in Europe (OSCE) will be used as examples for this paper.[3] Cold War territorial collective-defence was put aside for security challenges such as: world governance, humanitarian relief, and peace-building. Each with its own unique skillset, a comprehensive holistic approach involving political, civilian and military instruments devolved.[4] It became understood that the broadening security challenge were complex affecting every facet of a state; political, security, economic and social; failure in one risk failure in all.[5] Through crisis-management mechanisms such as the EU's External Action Service (EEAS) frameworks developed ranging from: 'counter-terrorism to governance, conflict prevention and peacebuilding, trade promotion or development co-operation'.[6]

[1] In this paper China refers to the People's Republic of China; Iran refers to Islamic Republic of Iran; Russia refers to the Russian Federation.

[2] European Union, *European Security Strategy: A Secure Europe in a Better World* (Brussels: Council of the European Union, 2003)

[3] Ugo Caruso, "Interplay between the Council of Europe, OSCE, EU and NATO," (Bolzano: EURAC Research, 2007)

[4] North Atlantic Treaty Organisation, *Lisbon Summit Declaration* (Brussels: NATO, 2010).
url: https://www.nato.int/cps/en/natolive/official_texts_68828.htm
retrieved on 29 May, 2019.

[5] Organisation for Economic Co-operation and Development, *Principles for Good International Engagement in Fragile States* (Paris: OECD, 2007), Principle No. 5.

[6] Organisation for Economic Co-operation and Development, Development Assistance Committee, *Whole of Government Approaches to Fragile States* (Paris: OECD, 2008), 9.

Over the last decade, the security spectrum has shifted again causing the international community to take note. The EU's 2016 *Global Strategy* noted: 'To the East, the European security order has been violated, while terrorism and violence plague North Africa and the Middle East, as well as Europe itself'.[7] The strategy identified five broad security priorities that endanger the EU's future: 'terrorism, hybrid threats, climate change, economic volatility and energy insecurity endanger our people and territory'.[8] The strategy further outlines the need for further integration with partners to predict, prevent, and manage conflicts and crises.[9] The updated framework provides for the 'integration of environment into security, paving the way towards a more holistic approach and interaction between the foreign, security and defence' spheres.[10]

The UN is still the optimal organisation when it comes to international law, peacekeeping, monitoring, mediation and disarmament, demobilisation and reintegration. It is complemented and supported by other IGOs including the EU. NATO has adopted a strategy of 'projecting stability' in which the 'alliance helps to project stability in many different ways – including through its operations, by training partner countries' armed forces, and through political engagement and dialogue'.[11] The OSCE specialises within the fields of early warning, conflict prevention, crisis- management and post-conflict rehabilitation. [12]

A New Chapter – the balance of power

The United States (U.S.) sheer cultural, economic and military power seems unmatchable in the coming century,[13] This unipolar hegemony has allowed many states to reduce their defence spending, in turn geopolitics moved away from territory and military power towards world order, global governance, and the broader concept of human security.[14] However, the west fell into a false sense of security. Known as revisionist states - China, Iran, and Russia – never bought into the geopolitical settlement that followed the Cold War; they were unable to do little if anything about it in their declined state. Today the world is witness to a shift in geopolitics in a way that has elevated the risk of major international crisis. The revisionist states wish to restructure the current international status quo and put in place a system more sympathetic to them; a system that reflects their interests. While U.S. hegemony continues, its commitment to providing defence and security for its allies is faltering; making the continuation of the wests counterbalancing economic and military IGOs – the EU and NATO – all that more critical. [15]

The revisionist states are a long way off matching the west in economic or military power. There is no doubt they are regional powers; China and Russia with a global projection. Primarily in reaction to western sanctions these latter actors have grown closer to the point of not trading in

[7] European Union, *Shared Vision, Common Action: A Stronger Europe*
A Global Strategy for the European Union's Foreign And Security Policy (Brussels: European Union, 2016), 13.
[8] Ibid, 19.
[9] *Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy*, 28-32
[10] Kettunen, Noome and Nyman, *Think 2030: Reinforcing Environmental Dimensions of European Foreign and Security Policy*, 5.
[11] North Atlantic Treaty Organisation, *The Secretary General's Annual Report 2018* (Brussels: 2019), 64.
[12] Organisation for Security and Co-operation in Europe, *Berlin Declaration - OSCE Parliamentary Assembly* (Berlin: OSCE Parliamentary Assembly, 2018)
[13] Robert Kagan, *Paradise and Power. America and Europe in the New World Order* (London: Atlantic Books, 2003), 42.
[14] Walter Russell Mead, "The Return of Geopolitics," *Foreign affairs*, Vol. 93, No. 3 (2014): 69–79.
[15] Paul K. MacDonald and Joseph M. Parent, *Twilight of the Titans: Great Power Decline and Retrenchment* (Ithaca: Cornell University Press, 2018)

U.S. dollars [16] Through their own IGOs - Shanghai Cooperation Organisation, the Collective Security Treaty Organization, and the Eurasian Economic Union – China and Russia are building regional economic and military partnerships. In 2013 China launched a global development strategy; One Belt, One Road (renamed the Belt and Road Initiative (BRI)); a global network of land and maritime silk roads with an aim to invest in infrastructure in 152 countries and international organisations. The BRI has been described as a reincarnation of China's Tribute system, while growing China's economic power it is winning allies through soft power attributes such influence, investment and trade.[17]

Over the past decade confrontations with the revisionist states have taken place in a space referred to as the 'gray zone'. These activities are not formal wars and do not resemble traditional state on state conflicts; strategic disruption is generally the result. While some aggression or use of force is used, ambiguity about the ultimate objective is a defining feature.[18] This results in the international community or the recipient state unsure how to respond. During Russia's annexation of Crimea in 2014 the U.S. and the EU could do little. Grygiel and Mitchel have put forward that the western powers have an extensive 'periphery or frontier problem that invites probing'.[19] Rather than directly challenging the west, the revisionist states are making probing actions along areas of weakness. To the international community these 'probes' at times can seem like minor infractions. The revisionist state then uses the failure of the west to react to its political advantage.[20]

The use of Non-State-Armed-Groups (NSAGs) and hybrid threats are two common characteristics of the 'gray zone' and probes. NSAGs - extremist groups, warlord led militias, organised crime networks – at times with their own proto-states or fiefdoms such as Islamic State of Iraq and the Levant, operate outside the realms of state governance. They can be used by or supported by states to carry out proxy or third-party activities. [21] NSAGs are a threat multiplier exasperating security issues including poverty, migration, human rights.

Hybrid threats are used by states and NSAGs to exploit an adversary's vulnerabilities. There are many definitions of hybrid threats. The European Centre of Excellence for Countering Hybrid Threats best characteristics the unique attributes: a wide range of low risk and ambiguous methods and activities including: 'influencing information; logistical weaknesses, [e.g. targeting] energy supply pipelines; economic and trade-related blackmail; undermining international institutions by rendering rules ineffective; terrorism or increasing insecurity'.[22] Ambiguity can be further exploited with the use of third parties such as non-combatants in the carrying out of cyberattacks. For the most part NSAGs and hybrid threats cause strategic disruption rather than direct conflict.

'Gray zone' or 'probe' activities are not unique to the 21st century, many have reflections of the Cold War. Since 2014 Russia has continued to influence destabilising activities in eastern

[16] "Russia, China to sign agreement on payments in national currencies, says decree," *TASS Russian News Agency,* (5 June, 2019) url: https://tass.com/economy/1061848 Retrieved: 1 September 2019.

[17] Md. Nazrul Islam (ed), *Silk Road to Belt Road: Reinventing the Past and Shaping the Future* (Singapore: Springer, 2019); R. James Ferguson, Rosita Dellios, *The Politics and Philosophy of Chinese Power: The Timeless and the Timely* (Lexington: Lexington Books, 2016)

[18] Frank G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *PRISM* Vol. 7 no. 4, (2018): 30–47.

[19] Jakub J. Grygiel and A. Wess Mitchel, *The Unquiet Frontier: Rising Rivals, Vulnerable Allies, and the Crisis of American Power* (Princeton: Princeton University Press), 52.

[20] Ibid, 64-66.

[21] C. Hofmann and U. Schneckener, "Engaging Non-State Armed Actors in State- and Peace-building: Options and Strategies," *International Review of the Red Cross*, Vol. 93, no. 883 (2011): 2-3.

[22] The European Centre of Excellence for Countering Hybrid Threats. url: https://www.hybridcoe.fi/hybrid-threats/ retrieved: 5 September 2019.

Ukraine and has deployed military assets in support of the Assad regime in Syria; with some in the west seeing it as a proxy war. Iran has repeatedly tested the wests resolve by using Hezbollah as a proxy to antagonise Israel; the continuing slow-motion nuclear proliferation crisis; continuing threats to oil supplies; challenging movement in the Arabian Sea; and support for the Houthis in Yemen. China's aggressive territorial claims and island militarisation in South East Asia is some ten years old. The west's limited response in many of these cases has resulted in allies in the Baltic and South East Asia questioning if they will be protected if directly attacked.[23]

While these actors may be 'light years away from creating an anti-Western alliance,' their IGOs and their growing global influence is providing an incentive for states 'to seek to strengthen the cooperation with like-minded states within IGOs,' whilst still providing a rules-based-system.[24] Both Serbia and Turkey – a NATO member – have sought such cooperation for example. Robert Kagan has put forward a long-cycles-of-history hypothesis. He argues that it is only a question of time before former powers re-emerge.[25] More recently Margaret MacMillan's essay 'The Rhyme of History: Lessons of the Great War' makes the analogy between 1914 and 2014 making the point that geo-politics is back.[26] It is unlikely these actors seek an all-out war. Their activities would indicate geopolitical jousting will be confined to the 'gray zone' for the foreseeable future.

A New Chapter - Climate Change

In recent years climate change has come to the fore of international and national attention and is just one example of the complex challenges faced today. Extreme climate events can have short, medium and long-term effects on a state's economic, political and social stability. For some states or societies climate change can be the principal risk they face; for example, island states/societies are threatened by sea-level rise.[27] Prolonged or recurrent climate extremes lead to: 'diminished coping capacity, loss of livelihoods, distress migration and destitution'.[28] Furthermore, climate-related disasters create and sustain 'poverty, contributing to increased food insecurity and malnutrition as well as current and future vulnerability to climate extremes'.[29]

The links between climate change and conflict are not simple or linear. Climate change's increasing impacts do not automatically lead to more fragility and or conflict; rather it acts as a threat multiplier. As such the impacts of climate change interact and converge with existing risks and pressures in a given context and 'can increase the likelihood of fragility or violent conflict. States already experiencing fragility or conflict are particularly affected'.[30] Climate

[23] Gustav Gressel, "After Crimea: Does NATO have the means to defend Europe?" Commentary, The European Council on Foreign Relations, (2 April, 2019). url: https://www.ecfr.eu/article/commentary_after_crimea_does_nato_have_the_means_to_defend_europe retrieved: 5 September, 2019.

[24] Kenneth Rapoza, "Russia And China Only Look Like They Are Becoming Buddies. It's Mostly Talk," *Forbes*, (5 June, 2019) url: https://www.forbes.com/sites/kenrapoza/2019/06/05/russia-and-china-only-look-like-they-are-becoming-buddies-its-mostly-talk/#1e0b874f64ed retrieved: 5 September, 2019.

[25] Robert Kagan, *The Return of History and the End of Dreams* (New York: Vintage Books, 2009).

[26] Margaret MacMillan, "The Rhyme of History: Lessons of the Great War," *Brookings Institution* (2013) url: http://csweb.brookings.edu/content/research/essays/2013/rhyme-of-history.html retrieved: 10 June, 2019.

[27] Malin Mobjörk (et al), *Climate-Related Security Risks: Towards an Integrated Approach* (Stockholm: SIPRI, Oct. 2016). 14-16.

[28] *The State of Food Security and Nutrition around the World: building climate resilience for food security and nutrition* (Rome: Food and Agriculture Organization of the United Nations, 2018), 79.

[29] Ibid.

[30] Report, *Insurgency, Terrorism and Organised Crime in a Warming Climate Analysing the Links Between Climate Change and Non-State Armed Groups* (Berlin: Climate Diplomacy, October 2016), 8.

security bridges chronic climate-related risks with human security such as famine, disease and rights violations. Climate security and its exasperation of as a threat multiplier is understood by states. [31] Internationally United Nations (UN) Secretary-General, António Guterres, warned in 2016: 'Many conflicts are triggered, exacerbated or prolonged by competition over scarce natural resources; climate change will only make the situation worse'.[32] As an example of the effects of climate change can be shown in Lake Chad which has shrunk by 90% in 40 years. The calamity has exacerbated existing inequalities, poverty and political instability; in turn leading to violent conflict and population displacement. With abundant food and water shortages, seven million people are suffering and two million displaced. The region became a breeding ground for NSAGs Boko Haram and Islamic State West Africa.[33]

With a global population that could grow to around 8.5 billion in 2030, 9.7 billion in 2050, and 10.9 billion in 2100., the increased stresses put on the world's resources by climate change is extreme.[34] Building the capacity for IGOs and states to manage stress, and ultimately prevent risks, emerging from climate change is vital.[35]

Meeting the Challenge – the Intergovernmental Approach

To meet the challenges of the 21st century requires a comprehensive holistic approach – as outlined in the introduction – achieved by deeper intergovernmental cooperation and mirrored by a robust whole-of-government approach at a national level. Rather than taking an aggressive stance against revisionist state that could trigger a Cold War, such an approach will ensure fragile and vulnerable states will remain stable, while at the same time the broader security challenges can be met. This section will discuss the intergovernmental approach.

Securing fragile states and meeting the complex challenges can be shown in the complementary relationship between the EU, NATO, OSCE – in support of the UN; example missions in Kosovo, Armenia, and Mali will be used.[36] Since 1999, NATO has been leading a peace-support operation in Kosovo.[37] Through its stabilisation efforts it has allowed other organisations to undertake diplomatic, judiciary, and development. The EU rule of law mission and the political work by the EU Delegation and Special Representative, the EU supports the UN and OSCE missions which focuses on areas of governance and judiciary.[38] In Armenia the OSCE takes the lead both in terms of the ongoing tensions with Azerbaijan and in its Security Sector Reform activities. In this case the EU plays a supporting role primarily through EEAS programmes of financial and technical cooperation supports; whereas the UN mostly focuses

[31] Karen Parrish, "Hagel Announces DOD's Arctic Strategy," *DoD News* (22 November, 2018) url: https://archive.defense.gov/news/newsarticle.aspx?id=121220 retrieved: 20 June, 2019.

[32] "UN Environment Annual report 2016," *United Nations* (2016) url: https://www.unenvironment.org/annualreport/2016/?page=0&lang=en retrieved: 15 May, 2019.

[33] Kettunen, Noome and Nyman, *Think 2030: Reinforcing Environmental Dimensions of European Foreign and Security Policy*, 8.

[34] United Nations Report, *World Population Prospects 2019: Highlights* (New York: United Nations, Department of Economic and Social Affairs, Population Division, 2019), 1.

[35] Lisa M. Dellmuth, Maria-Therese Gustafsson, Niklas Bremberg, Malin Mobjörk, "Intergovernmental organizations and climate security: advancing the research agenda," *WIREs Climate Change*, Vol. 9, no. 1 (January/February 2018).

[36] European Political Strategy Centre Brief, *Joining Forces The Way Towards the European Defence Union* (Brussels: EPSC, 2019)

[37] NATO: KFOR - JFC Naples. url: https://jfcnaples.nato.int/kfor retrieved: 15 September, 2019.

[38] S. Eckhard & H. Dijkstra, "Contested implementation: The unilateral influence of member states on peacebuilding policy in Kosovo," *Global Policy*, Vol. 8 (S5) (2017): 102–112; EEAS: European Union Office in Kosovo - European Union Special Representative in Kosovo. url: https://eeas.europa.eu/delegations/kosovo_en retrieved: 15 September, 2019.

on development functions.[39] In Mali, the EU is a significant actor with two civil/military CSDP missions; European Union Training Mission in Mali and the EU Capacity Building Mission in Mali. In this respect, the EU works alongside the UN peacekeeping mission (United Nations Multidimensional Integrated Stabilization Mission in Mali) which provides the lead security component. These efforts are securing and stabilising Europe's borders, building governance in fragile states, and tackling the causes of terrorism, organised crime, and population displacement.[40]

These IGOs have taken steps to jointly respond to other challenges such as environmental disasters. One example is NATO's European Atlantic Disaster Response Coordination Centre (EADRCC). The EADRCC consults with the EU Civil Protection Mechanism and the UN Office for Coordination of Humanitarian Affairs providing a civil-military response. The partners have deployed assets to the Balkans, Georgia, and Israel for example, to tackle floods and wild fires.[41]

Meeting the Challenges – Whole-of-Government (WoG) Approach

To meet today's complex and dynamic challenges states have to have an effective, efficient holistic defence and security framework. Such a framework allows a state to support and complement IGOs, and meet any domestic challenges. States have to prepare for the worst-case scenarios resulting from: the collapse of a partner IGO, successful attack on world energy supplies, domestic terrorist attack or environmental disaster, or increased instability in fragile states. Many states have implemented reforms to meet the challenges and implement a holistic approach, but in many cases the basic system remains episodic, stove-piped, non-integrated, horizontal, and with duplication in many areas. This is understandable as each state department has its own remit, priorities, ways of framing issues and understandings of the complex security nexus.[42] A WoG approach brings a unified effort between inter-governmental agencies and departments to maximise all available resources in a collaborative scalable effort. WoG can be defined as: 'where government departments and agencies use joined up structures and processes to eliminate silos and achieve seamless government'.[43]

It is understood that challenges faced today effect every facet of state security, therefore, it is vital that 'every appropriate lever available to the government' is part of the planning and implementation process.[44] A state's defence and security framework needs to operate as a system rather than a collection of separate components. In dealing with fragile states for example the 2005 Organisation for Economic Co-operation and Development (OCED) *Principles for Good International Engagement in Fragile States* highlights that successful development in a fragile environment depends, in part, on well sequenced and coherent progress across the political,

[39] EEAS: Delegation of the European Union to Armenia. url: https://eeas.europa.eu/delegations/armenia_en retrieved: 11 September, 2019; Hylke Dijkstra, Ewa Mahr, Petar Petrov, Katarina Đoki & Peter Horne
Zartsdahl, "The EU's partners in crisis response and peacebuilding: complementarities and synergies with the UN and OSCE," *Global Affairs*, online, Vol. 4, no. 2–3, (23 October, 2018) url: https://www.tandfonline.com/doi/full/10.1080/23340460.2018.1530572 retrieved 7 September, 2019.

[40] Center on International Cooperation Report, *European Military Contributions to UN Peace Operations in Africa Maximizing Strategic Impact* (New York: Center on International Cooperation, 2015)

[41] Niklas Bremberg, "European Regional Organizations and Climate-related Security Risks: EU, OSCE and NATO," *SIPRI Insights on Peace and Security*, No. 2018/1 (2018): 12.

[42] Ibid. 14-15.

[43] Centre for Effective Services Briefing Paper, *Implementing Whole of Government Approaches* (Dublin: CES, 2015), 2.

[44] Patrick Blannin, "The Good Operation: notes on a whole-of-government approach to national security," *Modern War Institute West Point*, 4 May, 2018) url: https://mwi.usma.edu/good-operation-notes-whole-government-approach-national-security/ retrieved: 30 August 2019.

security, economic and administrative domains. This requires donor countries to adopt a WoG approach that will enable the donor state to respond with all available resources: security, political, economic affairs, as well as those responsible for development and humanitarian assistance.[45] A successful WoG engagement in fragile states will result in 'a well-sequenced and coherent progress across the political, security, administrative, economic, and humanitarian and emergency domain'.[46] WoG approaches to the broad security spectrum have been employed by states including Australia, Finland, New Zealand, United Kingdom (U.K.), and the U.S.[47]

There are challenges to WoG, an example of which can be found in climate change. Tackling climate change has proven a challenge for states; there still remains a disconnect between climate change and security. This has resulted in states and their departments developing different approaches to framing and understanding climate change.[48] To overcome such challenges 'all stakeholders should have the same vision and buy-in to the same strategic priorities; furthermore, they should be consulted from the beginning'.[49] Fostering interagency cooperation and understanding can be achieved through joint multiagency training and exercises; and multiagency joint monitoring and readiness centres.[50] Recognising the complexity of the challenge Australia developed the *National Security Capability Plan* which provides a single consolidated picture of the capabilities that enable their nation to achieve national security outcomes.[51] Understanding the broad sphere of defence and security challenges ahead, Australia 'implemented several institutional transformations to ensure effective coordination and integration within the National Security Community'.[52]

Conclusion

Our holiday from history is over. The future is here now. States have to be prepared for all eventualities including thinking the unthinkable. Reacting to challenges is no longer enough, they need to be predicted and met head on before they escalate. Leaving the issues siloed within individual departments will leave a state fundamentally unprepared to adequately manage and prepare for all challenges. The solution is not as opaque as it may seem; a clear strategic objective supported by a balanced framework is a guiding principle. To meet the brood and uncertain challenges requires the international community and states to utilise all available resources. This can be achieved through a comprehensive holistic approach delivered through IGOs and mirrored by a supporting state WoG defence and security framework. This approach will lead to synergy between state agencies, cohesion, capability, capacity, and an adaptable leadership that will ensure a state's ability not just to react to challenges but predict and prevent them.

[45] OECD "Principles for Good International Engagement in Fragile States."

[46] OECD, *Whole of Government Approaches to Fragile States*, 17-18.

[47] Centre for Effective Services Briefing Paper, *A Primer on Implementing Whole of Government Approaches* (Dublin: CES, 2014), 3; For examples see: Her Majesty's Government, *National Security Capability Review - Including the second annual report on implementation of the National Security Strategy and Strategic Defence and Security Review 2015* (London: Her Majesty's Government, 2018); Simo Nikkar (et al), "Joint External Evaluation of Finland: Enhancing Health Security through a Comprehensive Whole-of-Government Approach*," Public Health Panorama*, Vol. 4, issue 1 (March 2018), 91-99.

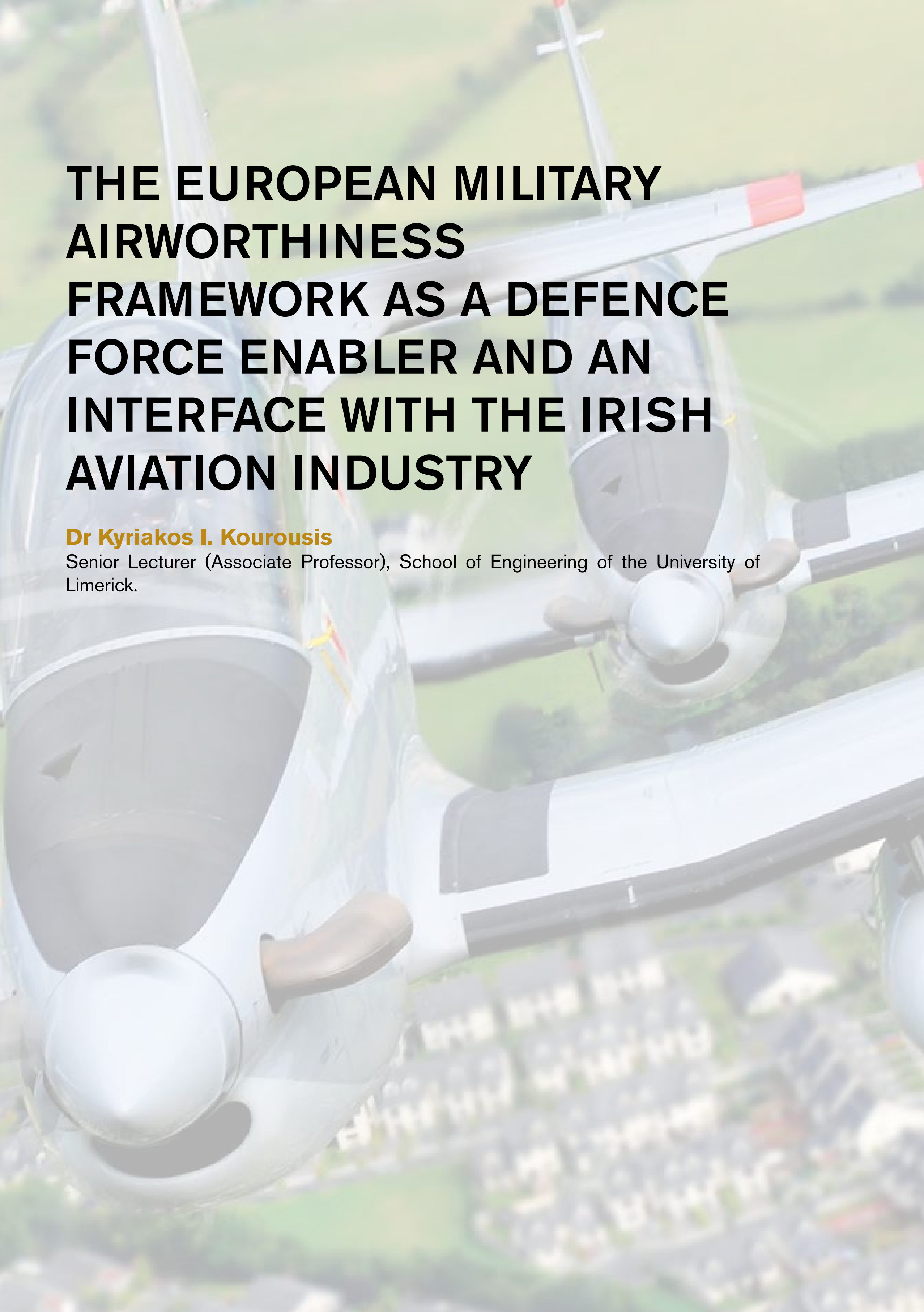
[48] Overseas Development Institute Working Paper, *Climate change in UK Security Policy: implications for development assistance?* (London: Overseas Development Institute, 2012), 13.

[49] Centre for Effective Services Briefing Paper, *A Primer on Implementing Whole of Government Approaches,* 4.

[50] James W. Derleth, "Fostering a Whole-of Government Approach to National Security from the Bottom Up Interagency Training at the Joint Multinational Readiness Center," *Military Review*, online exclusive, (February, 2018) url: https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2018-OLE/Feb/Fostering-Security/ retrieved 10 September 2019.

[51] Australian Government, *Guide to Australia Capability Plan*. (Belconnen ACT: Australian National Security, 2013), 3.

[52] Aaron Philip Waddell, "Security Community Integration in Australia: Cooperation and Integration among Australia's National Security Community," Studies in Intelligence Vol. 59, no. 3 (2015), 25.



THE EUROPEAN MILITARY AIRWORTHINESS FRAMEWORK AS A DEFENCE FORCE ENABLER AND AN INTERFACE WITH THE IRISH AVIATION INDUSTRY

Dr Kyriakos I. Kourousis
Senior Lecturer (Associate Professor), School of Engineering of the University of Limerick.

ABSTRACT

Airworthiness is a key enabler for mission capable defence aircraft, both in peace and conflict time. The European Defence Agency (EDA) has identified in 2008 the need for harmonisation in airworthiness across the European Union (EU), establishing the Military Airworthiness Authorities' Forum and the European Military Airworthiness Requirements (EMARs). EMARs have progressively evolved to a comprehensive framework for managing the design, manufacture, operation and maintenance of defence aircraft within the EU and beyond. The basis of the EMARs is the civil aviation regulatory set of the European Aviation Safety Agency (EASA), adapted to cater for the defence aviation environment. The EMARs have aligned defence regulations with best practice from civil aviation, offering greater focus on safety and a vehicle for efficient interaction with the aviation industry. Moreover, the EMARs enabled a much needed intra and inter-state regulatory standardisation, with a positive impact on interoperability within the EU and the North Atlantic Treaty Organisation (NATO). The Irish Air Corps (IAC) operates a highly diverse fleet of twenty-five aircraft, of seven different types, the majority of which are civil-certified. The performance of aircraft maintenance, management of continuing airworthiness and engineering design changes are governed by the IAC Military Airworthiness Authority (MAA) rules. The adoption of the EMARs has yet to be realised by the IAC, except for the EASA-approved Technical Training School. The retention of an Irish Defence Forces' specific airworthiness framework does not allow Ireland to harmonise with other EU states that have transitioned to the EMARs (e.g. United Kingdom, France, Germany, Sweden, Spain, Netherlands, Portugal), as well as limits the opportunities for interaction of the IAC with the vibrant Irish aviation industry. This paper presents the operational and cost implications of this regulatory disconnect, complemented by a discussion on the benefits of the EMARs' adoption by the IAC.

Military Airworthiness

In broad terms, airworthiness is the condition of a civil or military aircraft for safe operation. Perhaps the most accurate and complete definition of airworthiness comes a historical regulation of the Australian Defence Force, which describes it as a concept:

> *"…the application of which defines the condition of an aircraft and supplies the basis for judgment of the suitability for flight of that aircraft, in that it has been* **designed**, **constructed**, **maintained** *and* **operated** *to approved standards and limitations, by competent and authorised individuals, who are acting as members of an approved organisation and whose work is both certified as correct and accepted on behalf of Defence."*[1]

Moreover, in this definition one can find the activities encompassed by the two distinct (yet interconnected) domains of airworthiness, that of:

- **Initial Airworthiness**, design and construction of aircraft;
- **Continuing Airworthiness**, maintenance and operation of aircraft.

[1] "Glossary of Terms". Australian Defence Force AAP 7001.053 Technical Airworthiness Management Manual, Last modified July 3, 2019. http://www.defence.gov.au/dasp/Docs/Manuals/7001053/eTAMMweb/1307.htm

In civil aviation, the International Civil Aviation Organisation (ICAO) offers the overarching framework for the regulation of commercial aircraft airworthiness. Each of ICAO state is responsible to implement, in a legislated way, this high-level policy. State aircraft, including military aircraft, are specifically excluded from the ICAO provisions. In military aviation, there is no equivalent to ICAO, with each state utilising a unique set of airworthiness rules, orders, etc., for their military aircraft. This is mainly attributed to the role of military aviation, which is to maintain war capability. This role imposes additional, or even, contradicting requirements to airworthiness. Historically, this has led to a fragmented regulatory environment at international level, despite the apparent and unavoidable interactions between different states or even between defence services within the same state (i.e. Air Force, Army, Navy).

The European Military Airworthiness Requirements

In an effort to tackle fragmentation in the military airworthiness space, the European Union (EU) European Defence Agency (EDA) established in 2008 the Military Airworthiness Authorities (MAWA) Forum, having the following goals[2]:

- Develop a common **regulatory framework**;
- Develop a common **certification process** and **certification/design codes**;
- Develop common **approach to organisational approvals**;
- Develop common **approach to preservation of airworthiness**;
- Establish arrangements for **mutual recognition**;
- Promote the formation of a **European Military Joint Airworthiness Authorities Organisation (EMJAAO)**.

The EDA MAWA Forum has developed progressively the European Airworthiness Requirements (EMARs), which constitute a common set of requirements based on the civil airworthiness framework of the European Aviation Safety Agency (EASA) regulations. The EMARs can be adopted by the European Union (EU) States, via national legislation, as regulations specific to military airworthiness management. The following EMARs have been published so far (covering both the initial and continuing airworthiness domain)[3]:

Initial Airworthiness

- **EMAR 21:** Certification of Military Aircraft and related Products, Parts and Appliances and Design and Production Organisations.

Continuing Airworthiness

- **EMAR M:** Continuing Airworthiness Requirements;
- **EMAR 145:** Requirements for Maintenance Organisations;

[2] "Military Airworthiness Authorities (MAWA) Forum", European Defence Agency, Airworthiness, Last modified July 4, 2019. https://www.eda.europa.eu/experts/airworthiness/mawa-forum

[3] "Approved MAWA Documents", European Defence Agency, Airworthiness, Last modified July 4, 2019. https://www.eda.europa.eu/experts/airworthiness/mawa-documents

- **EMAR 66:** Military Aircraft Maintenance Licensing;
- **EMAR 147:** Aircraft Maintenance Training Organisations.

The EMARs are supported by the corresponding **Acceptable Means of Compliance** (**AMC**) and **Guidance Material** (**GM**), as well as the following set of complementary documents for the set up and operation of a military airworthiness framework[3]: **EMAD 1** 'Acronyms and Definitions Document', **EMAD R** 'Recognition Process', **EMAD MFTP** 'Military Flight Test Permit Procedure', European Military Airworthiness Certification Criteria (EMACC) and **EMAR Forms Document**.

The MAWA Forum initiative enjoys a high-level political support, however it has yet to reach to its full potential. According to publicly available information, the following EU States have adopted to date the EMARs (either fully or partially): France, Germany, United Kingdom, Italy, Spain, Netherlands, Belgium, Sweden, Portugal, Finland and Slovenia. It is of note, however, that two non-EU countries have already adopted the EMARs, Australia and Norway. Australia has been a strong advocate of the EMARs, as an emerging international standard for the management of military airworthiness, which is expected to influence countries in the Asia and Pacific region towards adoption of the EMARs (such as Malaysia, which has mirrored in the past the Australian military airworthiness framework).

The EMARs are also utilised by the North Atlantic Treaty Organisation (NATO) and the Air and Space Interoperability Council (ASIC), membered by United States, Canada, United Kingdom, Australia and New Zealand, as a framework facilitating interoperability between different defence forces[4]. The case of the EMAD-R 'Recognition Process' is of interest, as this structured methodology enables mutual recognition of airworthiness systems, which is key in running effectively and efficiently multinational projects (i.e. certification of new/modified aircraft platforms, acceptance of design/maintenance organisations, etc.).

Airworthiness Management in the Irish Air Corps

When examining any military airworthiness system, it is important to consider the primary role assigned to the aircraft operator. The role, in conjunction with the operational environment and the configuration of the aircraft, has a direct impact on both the initial and continuing airworthiness of any military aircraft. In the case of the Irish Air Corps (IAC), the role description (provided in the Defence Force website) sets a clear distinction between the war and peacetime role:

> *"The role of the Air Corps under the Defence Act is to contribute to the security of the State by providing for the Military Air Defence of its airspace. However in times of peace it is more usual for the Air Corps to fulfil the roles assigned by Government through the deployment of a well-motivated and effective Air Corps."* [5]

[4] Purton, Leon and Kourousis, Kyriakos. "Military Airworthiness Management Frameworks: A Critical Review". Procedia Engineering 80 (2014): 545-564. https://doi.org/10.1016/j.proeng.2014.09.111

[5] "Air Corps", Irish Defence Forces, Last modified July 10, 2019 https://www.military.ie/en/who-we-are/air-corps/

Under this umbrella definition of the IAC role, aircraft can be assigned a range of missions: army support, air ambulance, military transport, Presidential, Ministerial and VIP transport, general utility, Garda air support, offshore & inshore maritime patrol, search and rescue top cover, parachuting operations, escort surveillance & monitoring, inshore fishery patrol, drogue towing, ab-initio/advanced/instructor pilot training and close air support. In turn, to fulfil these roles, the IAC operates a highly diverse fleet of twenty-five aircraft, of seven different types, the majority of which are civil-certified[6].

In reviewing the organisation of the IAC on airworthiness management one can find in the Defence Force website[7] a basic overview of the IAC structure and units, including a reference to a **Military Airworthiness Authority (MAA)**. Thus, two secondary sources were used to obtain information on the IAC airworthiness system, an independent review conducted in 2015[8] and a previously published article in the Defence Force Review[9].

The responsibility of the IAC aircraft airworthiness belongs to the *General Officer Commanding* (GOC), obtained through successive delegation from the Minister of Defence to the Defence Force Chief of Staff. It is understood that airworthiness in the IAC is governed by a set of internal rules, the implementation. This set of rules are described in the Air Regulations Manual (ARM), issued by the GOC. It is noted that Air Regulations are not part of the Defence Force Regulations, which are issued by the Minister of Defence. In particular, the Defence Act 1954 stipulates that the Minister of Defence is authorised to regulate the "The flying, certification and maintenance of service aircraft and the certification and maintenance of service aircraft material."[10]. Instead, the issuance of Air Regulations is another responsibility delegated (directly) from the Minister of Defence to the GOC, via the Defence Regulation[11]

The GOC is supported and advised by the MAA. In particular, the scope of work of the MAA includes:

- Oversight of the Air Regulations' implementation (i.e. issuance of technical and flight operations' instructions, certification of staff, approval of maintenance programs, accident/incident investigation, aircraft modifications, liaison with aircraft Type Certificate holders, etc.);
- Advising of the GOC on airworthiness matters (i.e. new equipment/tender specifications, civil aviation regulations impacting IAC aircraft operation, etc.).

A synoptic overview of the IAC airworthiness management construct is illustrated in Figure 1.

[6] "Air Corps Fleet", Irish Defence Forces, Last modified July 10, 2019. https://www.military.ie/en/who-we-are/air-corps/the-fleet/

[7] "About the Air Corps", Irish Defence Forces, Last modified July 10, 2019. https://www.military.ie/en/who-we-are/air-corps/about-the-air-corps/

[8] Corcoran, David. "Just Flight Safety Culture and the Irish Defence Forces: It's A Question of Law!" Defence Forces Review (2016): 197-216.

[9] Irish Aviation Authority. *Independent review into allegations concerning the certification, qualification and experience of Air Corps Aircraft Inspectors*, by E. Sullivan, N. Butterfield and M. Purcell, December 3, 2015.

[10] Defence Act [1954-1987].

[11] Defence Force, Defence Forces Regulation CS 8 - *Air Corps Military Aviation Regulations and Directives*, July 20, 2012.

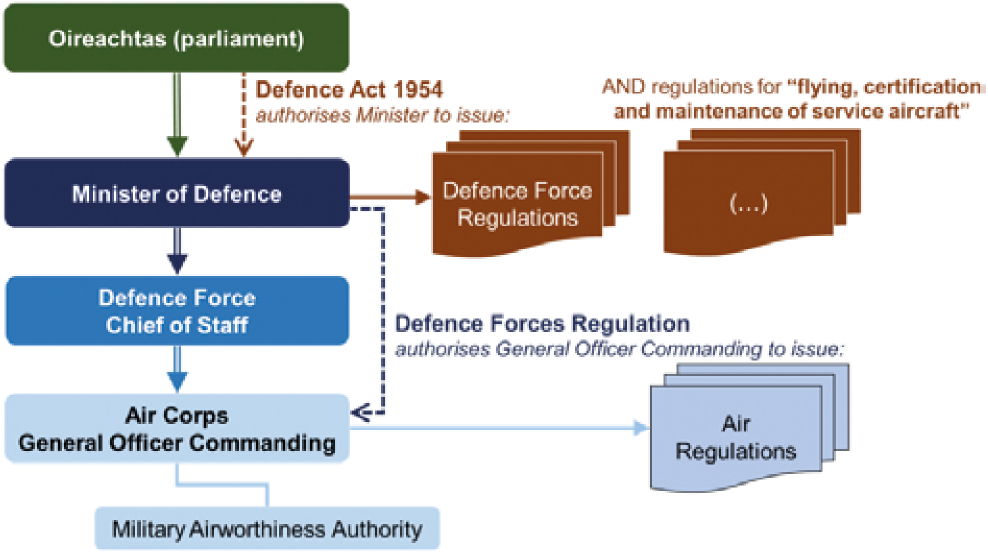

Oireachtas (parliament)
Defence Act 1954
authorises Minister to issue:
AND regulations for "flying, certification and maintenance of service aircraft"
Minister of Defence
Defence Force Regulations
(...)
Defence Force Chief of Staff
Defence Forces Regulation
authorises General Officer Commanding to issue:
Air Corps General Officer Commanding
Air Regulations
Military Airworthiness Authority

Figure 1. Airworthiness Management within the Irish Air Corps (IAC).

A Need for Change in the Irish Air Corps Airworthiness Management

Fragmentation of rules is one of the most common issues identified in military airworthiness systems[4], mainly due to limited standardisation, diversity of the aircraft types, mission profiles, etc., and the progressive erosion of the rules attributed to military management philosophies. The airworthiness framework of the IAC may not be fragmented as that of other, larger, defence forces. However, it is reasonable to assume that the diversity of the fleet, when combined with possible limitations on the availability of (human and material) resources, can pose challenges for the effective and efficient management of airworthiness. Regulatory standardisation, at high level, promotes consistency in the creation, change and implementation of airworthiness rules. This standardisation in airworthiness can be achieved when reverting to practices widely accepted in military and/or civil aviation (with necessary adaptions to account for the military aviation needs).

Another issue one may observe in the airworthiness construct of the IAC, presented in Figure 1, is the lack of **independence** between the airworthiness regulator and the aircraft operator, as both roles are exercised by a single officer (GOC). This is fundamentally inconsistent with the civil aviation practice. Moreover, it is unknown in what extent the IAC regulatory framework is aligned with civil (or other defence) airworthiness regulatory frameworks, apart from a reference to Maintenance Management Organisation Exposition in the ARM and the operation of the Air Corps Technical Training School under the approval by the Irish Aviation Authority (IAA) (as an EASA Part 147 Maintenance Training Organisation)[12].

[12] "Part 147 Approved Training Organisations", Irish Aviation Authority, Last modified July 10, 2019 https://www.iaa.ie/personnel-licensing/maintenance-engineer---amel-licensing/part-147-approved-training-organisations-1

As discussed, **harmonisation** between States' practices in the airworthiness field is one of the main objectives (and deliverables) of the MAWA Forum. The lack of harmonisation with other EU States that have adopted the EMARs is a limiting factor for expanding and improving the interactions with these States but also with the Irish aviation industry. Closer interactions are especially important for a defence aircraft operator of the size of the IAC, as the level of commonality of an airworthiness system with other civil/military systems is a positive contributor to achieving economy of scale.

To summarise, reducing regulatory fragmentation, establishing an independence in the airworthiness management roles and responsibilities and promoting harmonisation are considered some of the main reasons to initiate changes in the IAC airworthiness system. Moreover, these reasons will have to be assessed in conjunction with the benefits that an EMAR-based airworthiness system can offer to the IAC (discussed in the next section).

Nevertheless, as with every change, especially of this magnitude, one would need to examine the challenges associated. The implementation of the EMARs requires the establishment of a suitable legal instrument, which, in the case of the IAC, would be a new Defence Regulation, issued by the Minister (as per the provisions of the Defence Act 1954). This new Defence Regulation is necessary to provide the Basic Regulation as the framework (basis) for the EMARs-derived set of airworthiness regulations. This Basic Regulation would reflect the EASA Basic Regulation, with adaptions, similarly to the approach followed by the Australian Defence Force in their adoption of the EMARs[13].

Benefits of the EMARs for the Irish Air Corps and the Irish Aviation Industry

An effective and efficient airworthiness system can be an enabler for the Irish Defence Force. Moreover, linkage of the IAC with the vibrant aviation industry is an opportunity offered by adopting a civil-based airworthiness system. In line with the aforementioned reasons for a change in the existing IAC airworthiness system, the adoption of the EMARs can offer substantial benefits.

Aviation safety can be enhanced by following best regulatory practice from civil aviation. Namely, the EASA system (mirrored by the EMARs) can be a positive contributor to safety. In a report accompanying the 2015 Defence Forces Climate[14] a number of safety concerns were reported in connection to organisational matters, i.e.:

- "*We can't do things safely. We need to say no to outputs.*", indicating possible discrepancies in the airworthiness decision making processes;
- "*It keeps us up at night.. 'is this safe'... we are signing off on people who don't have experience*", implying a lack of confidence in the maintenance staff certification process;
- "*We are double and triple jobbing. That would be illegal in the private sector*", illustrating a low esteem for the defence regulations.

[13] "Defence Aviation Safety Regulation", Australian Defence Force, Last modified July 10, 2019 http://www.defence.gov.au/DASP/Docs/Manuals/8000-011/DASRWeb/index.htm#8797.htm

[14] "Workplace Climate in the Defence Forces" Phase 2: Results of the Focus Group Research, Last modified July 14, 2019 https://www.defence.ie/system/files/media/file-uploads/2017-12/workplace-climate-defence-forces.pdf

However, it is noted these claims, and the assumption that the EMAR-based system can improve the safety record, cannot be fully substantiated due to the unavailability of safety performance indicators for the IAC.

Standardisation in the airworthiness standards, specifications and processes can be achieved through the adoption of EMARs and the associated/supporting documents. The benefit of standardisation can be witnessed in some recent examples of specifications published for new aircraft procurement purposes. In particular, in the Request for Tenders (RfT) for a new fixed wing utility aircraft[15] and the Request for Proposals (RfP) for a new maritime patrol aircraft[16] issued by the Irish Department of Defence, one can find references to EASA certification specifications, combined with requirements reflecting in practice certification specifications (examples of such references are provided in Table 1). This can be considered as a reflection of limited standardisation, which may have an impact on the accurate capture and definition of the certification specifications. Most importantly, under an EMARs-based system, the certification basis of new aircraft can be defined in an accurate way and tailored, where necessary, to the needs, operating environment and available budget of the Irish Defence Force.

Document	Section of Document	Reference to Airworthiness Requirements
Request for Tenders (RfT) for a new fixed wing utility aircraft[15]	Appendix 1: Requirements and Specifications: 1. Specification 1.4 Applicable Documents	*All configurations and equipment must be Type Certified or Supplemental Type Certified (STC), or another standard, which meets the requirements of the Irish Air Corps Military Airworthiness Authority (MAA).*
	Appendix 1: Requirements and Specifications: 2. Scope of Work/Aircraft Configuration 2.1 General Aircraft Requirements	*The contractor must design, build, install, test and certify the proposed aircraft to the requirements of EASA CS23.*
Request for Proposals (RfP) for a new maritime patrol aircraft[16]	4. Qualification Criteria	*b. The aircraft must be built to EASA CS25 or equivalent standard. All additional items fitted to the aircraft must have manufacturers' Supplemental Type Certification (STC).*
		t. The aircraft must have extensive, evidence based Corrosion Prevention measures, including paint schemes, airframe and engine-wash programmes, panel sealing, internal cavity liquid protection, and corrosion inspection programmes.

Table 1. Examples of references to airworthiness requirements from Request for Tenders (RfT) and Request for Proposal (RfP) documents issued by the Irish Department of Defence.

[15] Department of Defence, Request for Tenders for the Supply of Fixed Wing Utility Aircraft for the Irish Air Corps, Reference CON/0013/2017, May 4, 2017.

[16] Department of Defence, Request for Proposals for the Supply of Maritime Patrol Aircraft (MPA) to the Irish Defence Forces, Reference CON/001/2018, May 11, 2018.

Linkage with the **Irish civil aviation sector** can be facilitated by adopting the (EASA-based) EMARs. Examples of such interactions include:

- Outsourcing of IAC maintenance work to Irish-based EASA Part 145 Aircraft Maintenance Organisations where and as necessary;
- Outsourcing of IAC engineering design and production work to Irish-based EASA Part 21J Design and Part 21G Production Organisations;
- Outsourcing of IAC fleet management to EASA Part M Continuing Airworthiness Management Organisations (CAMOs);
- Inward and outward mobility of EASA Part 66/EMAR 66 civilian/IAC licenced aircraft maintenance technicians and mechanics, enabling the quick filling of skills/man-hour gaps in the Irish civil and military aviation industry;
- Offering of helicopter basic and type training by the IAC EASA Part 147/EMAR 147 Maintenance Training Organisation to the Irish, EU and international civil aviation industry (currently no EASA Part 147 Maintenance Organisation in Ireland offers such training courses).

Work satisfaction of the IAC staff can be improved by working within a modern civil-based airworthiness management system. As identified in the 2015 Defence Forces Climate survey[17], the measured level of organisational procedural justice (perceptions of staff around the organisation's fairness in terms of procedures and policies) suggest dissatisfaction. Moreover, the acquisition of globally recognised qualifications (i.e. EASA/EMAR 66 maintenance licences) is also expected to contribute positively to the morale of the IAC staff, both in terms of the appreciation exhibited to them from their organisation and future career prospects. This can have a positive effect in retaining talent in the IAC.

Interoperability can be improved, since servicing of IAC aircraft, pooling and sharing of human resources and equipment, common training, etc. can be served better by a common regulatory framework. The EMARs can offer that both at EU and international level (due to their increasing use by non-EU States). A cross-state operation of IAC can be not only a force multiplier for the Irish Defence Force (where and as necessary) but also an opportunity for closer interaction with other military aircraft operators employing advanced operational practices.

The EMARs as an Enabler for Irish Air Corps Capabilities

The airworthiness of a military aircraft fleet can sometimes be perceived by the commanding officers (at the various levels of military hierarchy) as a de-facto condition. However, airworthiness, by definition, does not simply imply safe to operate aircraft but also aircraft ready to accomplish their intended mission. In the military world, airworthiness is maintained via a continuous balancing act between safety and operational readiness, which involves risk management. Thus, one should pay close attention to the relation that exists between efficient and effective military airworthiness management and force capabilities.

[17] "Wellbeing in the Defence Forces", Report on the Defence Forces 'Your Say' Climate Survey 2015, Last modified July 14, 2019 https://www.defence.ie/en/press/publications/report-defence-forces-your-say-climate-survey-2015

Assuring the technical integrity of the aircraft (defence capability platform) is what an airworthiness framework covers. Technical integrity comprises of all those norms, regulations and practices covering Product, Behaviour and Process (PBP) integrity[18] for initial airworthiness (design and construction of aircraft) and continuing airworthiness (maintenance and operation of aircraft) assurance. The Product element corresponds to the technical system (aircraft), while Behaviour covers the human requirements' element (training, certification, competency of staff), with the Process element covering all process/procedural requirements and implementation across the board. The EMARs, as discussed in the previous section, are able to contribute positively in enhancing aviation safety, standardisation, work satisfaction and interoperability in the IAC. In effect, these contributions can ensure, in different ways each, the PBP integrity and enable the short, medium and long-term capabilities of the IAC. The interactions and the overall relationship between capabilities and the EMARs, as a comprehensive system for military airworthiness management, are illustrated schematically in Figure 2.

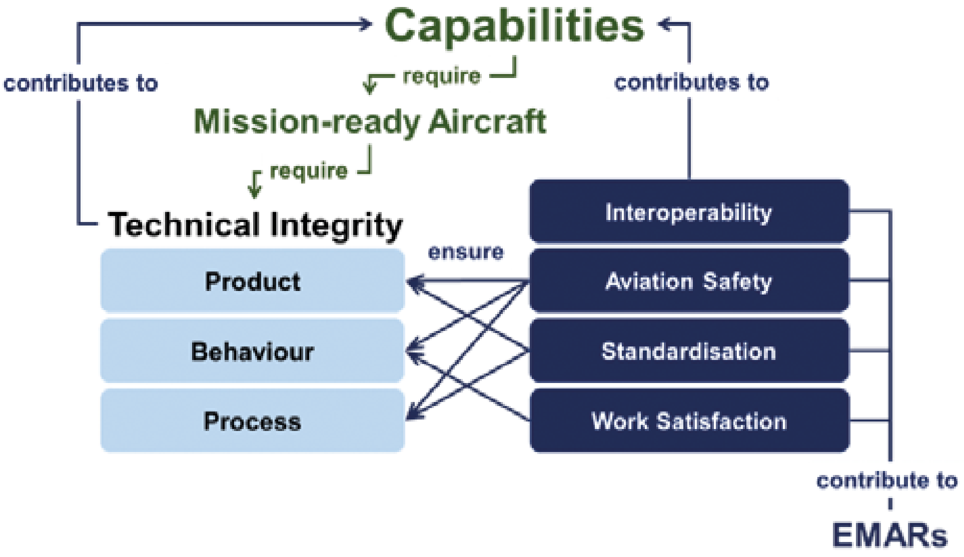


Figure 2. The interaction and relationship between the European Military Airworthiness Requirements (EMARs) and the Irish Air Corps (IAC) capabilities.

Conclusion

In summary, an EMARs-based systems approach to airworthiness management can:

- Offer a modern military-tailored framework for the airworthiness management of the diverse fleet and mission profile of the IAC;
- Promote standardisation across the initial and continuing airworthiness functions of the IAC, including the definition of procurement requirements;
- Enhance the work satisfaction of the IAC staff, with a positive effect in retaining talent;

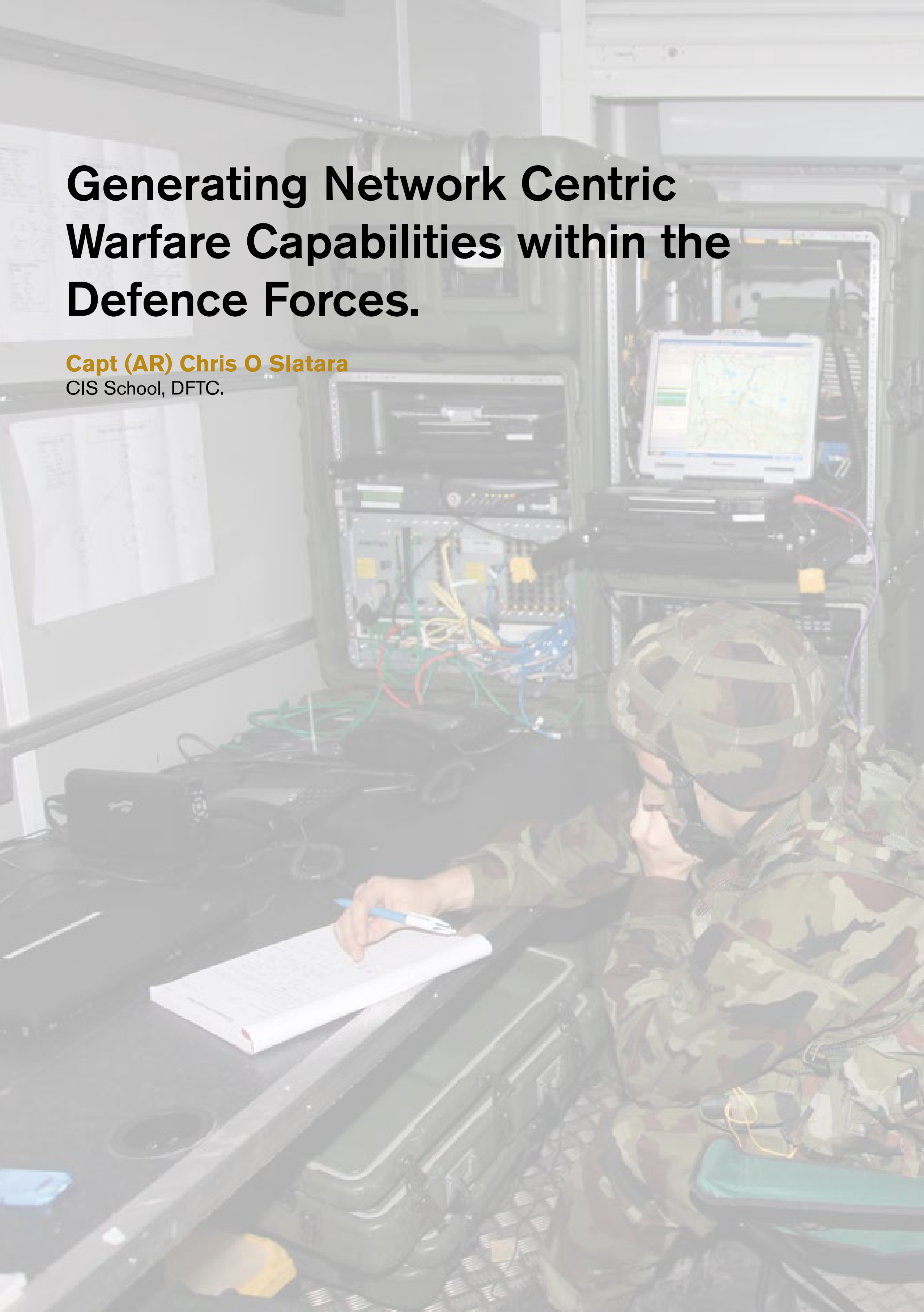
[18] Purton, Leon; Clothier, Reece and Kourousis, Kyriakos. "Assessment of Technical Airworthiness in Military Aviation: Implementation and Further advancement of the Bow-Tie Model". Procedia Engineering 80 (2014): 529-544. https://doi.org/10.1016/j.proeng.2014.09.110

- Link the vibrant civil aviation industry in Ireland with the IAC;
- Improve interoperability in EU and international level;
- Offer a comprehensive solution for the assurance of technical integrity;
- Enable the current and future Irish Defence Force capabilities by providing safe and mission-ready aircraft to the IAC GOC.

The adoption of the EMARs by the IAC is believed to be towards a positive direction, both for achieving a more effective and efficient airworthiness system. This paper, through its analysis, hopes to have provided enough details to stimulate further discussion on this matter within the Irish Defence Force organisation. A full justification and planning of the implementation of the associated change would be the logical next steps, similarly to several defence forces in the EU (and internationally) that have decided to transform their airworthiness management systems.

Generating Network Centric Warfare Capabilities within the Defence Forces.

Capt (AR) Chris O Slatara
CIS School, DFTC.



Abstract

This paper looks at Mission Command and Network Centric warfare, what advantages they might bring to the Defence Forces, and how those advantages might be realised. Mission Command and Network Centric warfare are popular topics. In the modern military of today it is necessary to practice both in order to operate within, and excel, in the coalition/battlegroup format espoused by the US Army and NATO. In this paper it is argued that the Defence Forces can excel in this area with a far lesser expenditure and effort than might be thought.

What is Mission Command

Mission Command is a style of command. There are many others, from micromanagement, to laissez-faire. From a military point of view, the tribunes of the Roman Empire would have been well-versed in mission command, when the Senate and Caesar despatched them to Gaul. Mission Command can be summarized in short as “tell your subordinates what a good end looks like – and let them get on with it”. This allows for initiative and much more to be exercised. As we know it today, Mission Command was first seen in the revived Wehrmacht in the 1930s - German doctrine stated that ‘the emptiness of the battlefield requires fighters who think and act on their own and can analyse any situation and exploit it decisively and boldly’ (W.Murray, 2001). In battle, commanders are told what success should look like. In most cases, as well, they are told what their limits will be, for example “You will proceed no further than Phase Line X-Ray” This style of Command was evident all through WW2, the Wehrmacht‘s decentralization doctrine meant commanders were told what the end state and limits of exploitation were, and told then to get on with it. Even farther back, we can look at WW1. The German word for this style of command is known as ‘Auftragstaktik’ or ‘Mission Command’. So, what are the key factors of mission command – what distinguishes it? It is loose, flexible, and decentralized. It is accepted doctrine that the Defence Forces must use it, as it is the philosophy and system of how we train and how we should fight.

Mission Command is characterized by a much stronger attraction to duty than anything – in a sense, contracts of trust. Much of this is normal to military life in any event but what is new here is the utter reliance and trust that both commander and subordinate understand each other – that the commander will issue orders that the subordinate can achieve, and provide the right support to do so, and in addition that the subordinate will act within the intent of the commander. A key difference here between Mission Command and inflexible orders with no room for interpretation is that on the battlefield, unknown circumstances may likely arise – the commander and subordinate know that the subordinate will take the best action s/he could have taken, without needing to refer back to the commander.

In addition, the contract of trust also results in a much-minimized set of orders, with only an end state and limits of exploitation; this can open the battlefield as it allows for initiative and seizing of opportunities as they arise. With production of reduced orders comes a reduction in misunderstanding, and so an improvement in tempo, as there is no requirement in most cases to refer to higher command for guidance.

However, mission command is not without its drawbacks. With forces that are not trained to a high standard, or commanders that are not sure of their subordinates, then detailed orders may be necessary, thus resulting in a lack of flexibility. The US Army refers to Mission Command as an "*approach*" (Army, 2019)(Army, 2014) "The Army's approach to command and control that empowers subordinate decision making and decentralized execution appropriate to the situation" is guided by the principles of:

1. Building cohesive teams through mutual trust,
2. Creating shared understanding,
3. Providing a clear commander's intent,
4. Exercising disciplined initiative,
5. Using Mission Orders,
6. Accepting Prudent Risk.

In the above discussion we have mentioned trust, intent, initiative and mission orders. This concept of shared understanding will be revisited as it will recur again and again. Risk is also an important factor – no military option is without risk, but the prudent acceptance and a decision to proceed is one of the factors that characterizes a commander using Mission Command. We now mention Shared Understanding – here, what is required is the creation of a shared understanding of the operational environment, the problems and approaches of solving those problems and the reasons the operation exists in the first place. This is no easy task – information management require time and effort to create the shared understanding – it is rarely done via email and always requires some type of contact to do so. This, then, begins our journey into Network centric warfare, and we consider again the tribune leaving Rome to conquer a foreign land, who– he would have understood Mission Command.

What is Network Centric Warfare

Here we attempt to present Network Centric Warfare (NCW), firstly as a definition, but then placing it in context. "It is characterized by the ability of geographically dispersed forces (consisting of entities) to create a high level of shared battlespace awareness that can be exploited via self-synchronization and other network-centric operations to achieve commanders' intent" Network Centric warfare was reallywas first defined in a seminal paper from 1998 in the U.S. Naval Institute by Vice Admiral Cebrowski and John Garska. In order to place it in context, we must understand the massive change in how we perceive technology in the last 20 years; the rise of the Internet and World Wide Web has revolutionized how we store and process information. Just as importantly is how we can now form networks in an ad-hoc fashion (Facebook, Tinder, WhatsApp, Boards.ie are all obvious examples) to carry out a pastime or purpose. They are all enabled by this ability to create networks – without the capability to form networks, Facebook and the other sites would not exist. What Network Centric warfare does is attempt to translate this ability to create networks into a military advantage. Cebrowski' s and Garska paper attempted to visualise what effects the Internet and more specifically the formation of networks might have on war. It lays out the principles and how a fighting advantage may be gained.

The Principles of Network Centric Warfare

A Robustly networked force improves information sharing

Exploring this statement is important - robust networks are difficult to achieve. Consider the use of tactical radios in the Defence Forces. Unless all kit is working properly with a trained operator, communications tends to be difficult at best and other forms of communications are used as fallback. Proper PACE (Primary, Alternate, Contingency, Emergency) planning is vital to ensure communications are maintained, and robust, and users are trained. Without these, the networks cannot be said to be robust. Robust in this context also means secure – although no radio is completely proof against jamming, blocking or interference, it does mean comparatively, a robust network is difficult to jam and difficult to intercept. 'Networks' in this instance also mean primarily data networks – able to exchange messages and data.

Information Sharing enhances the quality of information and shared situational awareness

The next point to mention is that Information Sharing can now take place over the robust networks between staffs and troops on the ground, or between troops on the ground. The very fact that they are networked means that maps, positions, pictures, information, text, chat messages can now be sent across the network, rather than writing information down from a message copied over radio (and as everyone knows, this can be extremely prone to error). This enhances the quality of information. This sharing of information translates into a shared situational awareness – i.e. knowing what is happening on the battlefield OR alternatively, knowledge of the battlespace is available, critically, in the network. You must also have applications/software that can display this information in a manner that you, the user, have been trained to use and fight with

Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command

When mentioning the sharing of information, it must be remembered that even though the information is shared, it may not have been processed or acted on by the users. This is the important point here – self-synchronization now becomes possible. This means that the users can make use of the information themselves, without having being directed to do so The shared environment thus allows for self-synchronization without being directed to do so - the implication is that a user is trained and empowered to collaborate and pick up what information they need from the shared situational picture Thus, speed of command is increased – because we self-synchronize and collaborate, the end result is better than what went before

These in turn dramatically increase mission effectiveness.

So, the last point of Network Centric warfare is the increased effectiveness from self-synchronization; if we can see what others are doing we can reinforce our allies and disrupt our enemies, all in a faster and better cycle than our enemies, most especially if they have not decided to fight with a Network Centric Warfare tool and approach - and by association lack the aforementioned trust in their field commanders, staff and troops. As we can see, there are many tenets of Network Centric Warfare and Mission Command that reinforce and complement one another. We will now examine these, and the requirements to enable them.

Network Centric Warfare and Mission Command from the Irish Point of View

The Irish situation can be explained by looking at the current global trend and identifying the position in respect to that, and looking at ways to harmonize operational art along those lines. The politics of the modern defence arena show that operations by the US Military in the Middle East for the last 20 years (and more) have been focused on coalition operations. As nearly always the largest provider to said coalition operations, it has been a tenet of their coalition dealings that partner nations must be able to interoperate with them - and, of course, this means 'Robust Networks' as meant in the context of Network Centric warfare, quite apart from the nature of staff duties and following NATO Standard Agreements (STANAG)s. This has followed the practice from NATO, where considerable standardization and networking meant that forces could interoperate easily and work together to achieve their aims. Ireland's participation in European Union Battlegroups practices this from a limited point of view – we deploy with force packages of Mechanized Infantry Companies which slot into the host nations force package.

From the point of network centric warfare however, it leaves a lot to be desired as the package, while networked to some extent, does not accept and build the robust networks in order to fully exercise the principles of Network Centric Warfare. Participation in exercises such as VIKING18 shows that considerable effort on several fronts needs more work in order to fully embrace the concepts and approach of Network Centric warfare. As discussed above, robust networks and information sharing improves mission effectiveness. In order to gain the benefits to our forces the correct doctrine, tools and training must be in place. This training must exist in the HQ - training the staff function. It must exist with the troops on the ground, afloat, or in the air; it must exist with the IT soldiers keeping these systems running. Unless all three capabilities (Staff, troops and IT support) are practiced individually, and collectively, Network Centric Warfare Capability cannot be generated or maintained. The US Army recognizes this – They have established several centres of excellence, and created troop grades specifically to assist with this process (Digital Master Gunner), and established several digital ranges to practice. In addition, all of the training tables to certify and qualify are publicly available, giving any military personnel wishing to bootstrap themselves a huge leg up.

From the Irish Point of View, the Staff Process remains largely overlay/paper-based when teaching MDMP (Military Decision-Making Process). There are arguments made strongly on both sides of this debate, as a very strong case can be made that the nature of the MDMP process requires that it be able to operate when communications or power has been disabled, and the Brigade/Formation must still be able to operate, and so commanders at all levels must be able to revert to doing without computers, if forced to do so.

Separately, participation in any overseas role now requires collaboration, usually with some type of network centric warfare -enabled platform. This places a very strong drive on staffs to be able to operate at an exceptionally high level in these roles. Arguably, indeed, they should operate 'as native' in a digital context and therefore Staff Officers from the Defence Forces should be able to execute MDMP via these networks and using those appropriate tools. Furthermore, in order to gain the most benefit for troops, they should not just be 'able' they should excel. Long and painful experience teaching these toolsets and networking shows that a huge benefit occurs when highly trained staffs at these toolsets are working as they should with the correct tools and technology. The training required is comparatively small to get this kind of benefit. This can best be achieved within the Defence Forces by the formation of Centres of Excellence.

Much the same benefit can be had by troops on the ground. The main difference is that staffs are normally located in Formation Headquarters, or tactical operations centres (TOCs), while troops are normally located in vehicles, ships or aircraft. The networks and tools themselves are normally heavily integrated with the vehicle – for example some platforms can pick up and relay turret positioning from Armoured Fighting Vehicles (AFVs) - in addition the vehicles are nearly always highly mobile. This produces a much greater training requirement as the soldier must be able to keep their vehicle and integrated communication network running, AND learn how to do TLPP (Troop Leadership) on the ground using these robustly networked systems and tools. Much of this can be dealt with by the establishment of digital ranges within a Centre of Excellence framework but the proper exercise of vehicles requires practice in the field with individual and collective training to properly learn to fight the formation.

The next part of the training need is that for the communications soldiers, both in the planning and in the operation of the networks. Paradoxically, this is usually easier, as they are normally the introducers of the networks and applications. However, they do need the collective training in high-tempo operations, as the very nature of combat means tools need support, and systems need repair, and the practice in doing this is vital, as is establishment of communications. One important point to make is that it is NOT the responsibility of the communications soldiers to operate these systems – as mentioned above this is the responsibility of the staff and troops on the Ground.

The next point to be addressed is that of the Applications themselves that are used for Information Sharing and Situational Awareness. Historically, militaries paid software vendors very large amounts of money to deliver custom solutions to address the needs of the military at that point in time. However, this ran into problems almost from the start because the computers available evolved rapidly as did the capability of the vehicles in which the hardware was carried. In addition, military capability (for example, precision strike capability and UAVs to take just a couple of examples, arrived in modern warfare, as did the need to operate in loose coalitions of nations. These reasons, coupled with a lack of detailed requirements and little headroom in the systems to expand to meet these needs, resulted in the delivery of systems typically years overdue and obsolete or with very limited capability almost at delivery military at that time. The net result was a huge mistrust of custom applications to deliver network centric warfare capabilities.

Therefore, the current approach is not to use custom applications, but instead to use Commercial Off The Shelf (COTS) applications to generate Network Centric Warfare capabilities. Advances in standards, security, and enhancements to the products which benefit all, can be easily taken on by installing the latest version. The Irish Defence Forces have settled on using the Sitaware family of products, from the Danish company Systematic.

These products are used in the Staff Roles “Sitaware Headquarters” and in the Vehicle “Sitaware Frontline” and on the commander on the ground “Sitaware Edge (on a battle vest)”. This is the same product used by a number of military establishments. The US Army uses Sitaware Headquarters in its new Command Post of the Future programme (CPOF), where it is known as the Command Post Computing Environment (CPCE). Similarly, the US Army are planning on the use of Frontline in the Vehicle Role where it is known as the Mounted Computing Environment (MCE).

The Sitaware product suite is, at its, heart, dedicated to enabling Mission Command and Network Centric Warfare. It does this via enabling information be shared, received and transmitted via Compliance with a large and diverse set of technical standards and protocols - for example VMF, MIP, JREAP, LINK16, ACO, NATO STANAGs. This ensures that it can talk to other nations in the air, sea, and land domains. In addition, it provides Blue Force Tracking display capability, integrating friendly force tracking for both air, sea, vehicle and individual soldiers. It also provides chat message capability, which is fast becoming the preferred communication method in modern Command and Control systems. In addition, detailed Military planning tools to enable the military decision-making process (a standard process, usually just called MDMP) are available to enable doctrine-led operations planning. It enables a Common Operating Picture via advanced mapping and GIS capability, and NATO standard symbology.

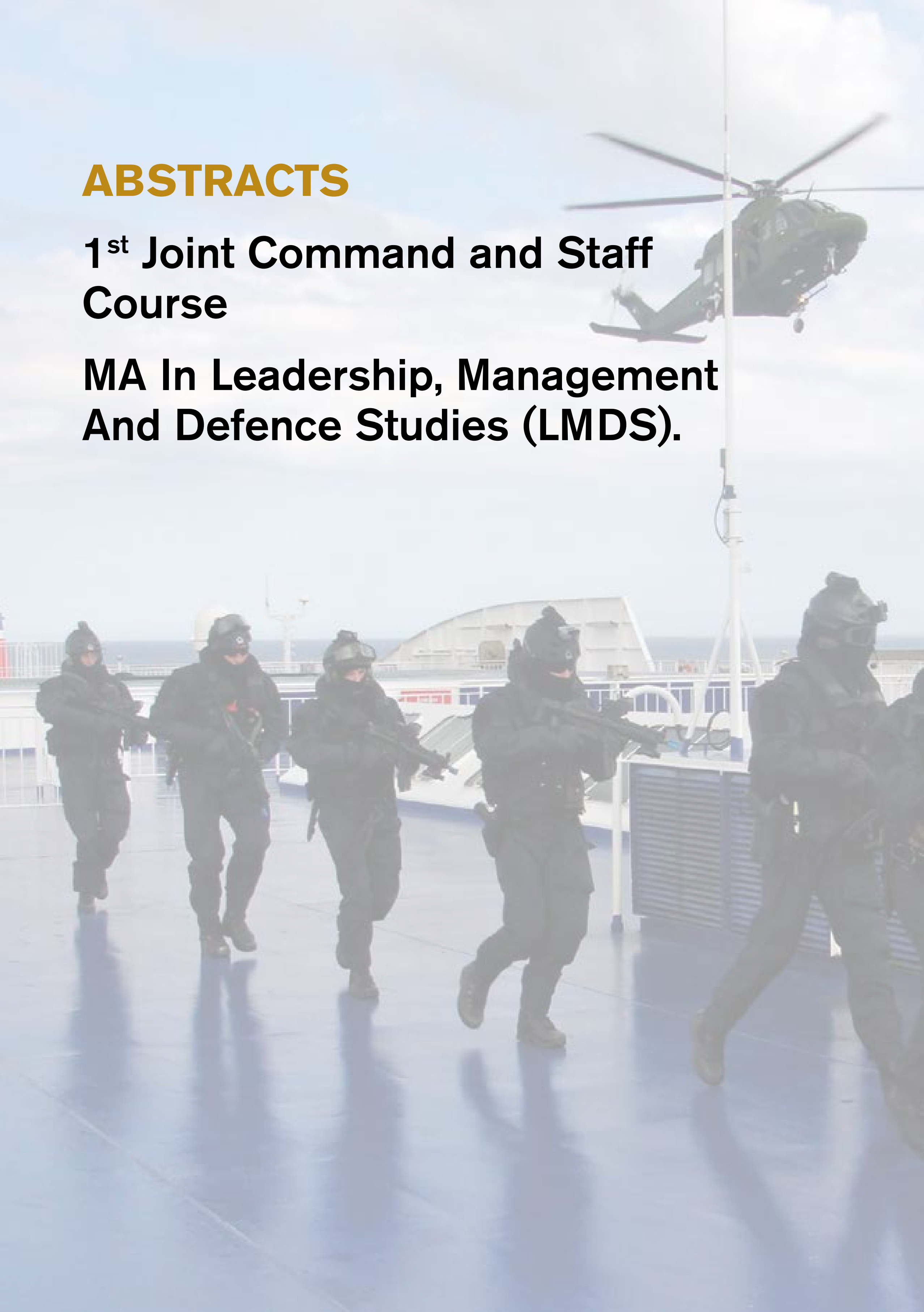
One vital part to note is that it – importantly – is able to work with the concept of resilience. Any military network can and will get disrupted – importantly with Sitaware, if networks are disrupted messages will reroute or hold until they can be delivered, thus making the network self-healing, and validating the PACE concept (having alternate means of communication) so vital to the operation of network centric warfare. In addition, networks may be disrupted by radio silence for operational reasons – in these cases, again, the network will automatically heal itself once radio contact is re-established. The network can also cope with bandwidth limitations – for example the SINCGAR radio has extremely limited bandwidth compared to 3G/4G networks, but can be used by Sitaware by prioritising traffic.

It has been shown above that robust networking and enabling information sharing can strongly improve effectiveness – these are the keys that enable Network Centric Warfare. The Naval Service, in its creation of the Recognised Maritime Picture (the first uses of Sitaware in the Defence Forces), has led the way in the Defence Forces and now it is the turn of the other arms of the Defence Forces. As discussed above, the doctrine, training and equipment must be in place to gain the benefits of Network Centric warfare. Other nations farther along the transformation process have formed, based Centres of Excellence to enable the training of the NCW approach and tools to end users and enable feedback to doctrine. This can happen immediately and at relatively little cost and without waiting for expensive technologies. The creation of Centres of Excellence, designed to provide the Defence Forces with the necessary capabilities to empower the future force is a critical first step to a broader and more effective application of these cutting-edge principles. In addition, for example, other technical advances may be possible – as the openness of the tools make it straightforward to plug in such current-generation approaches like Machine Learning or Artificial intelligence. Within the context of the Defence Forces and their participation in coalition operations, the benefits to be gained are clear and the embrace of Network Centric Warfare something that should happen fully across all the arms of the Force

ABSTRACTS

1st Joint Command and Staff Course

MA In Leadership, Management And Defence Studies (LMDS).



AN ASSESSMENT OF THE IRISH DEFENCE FORCES' INFORMATION AND KNOWLEDGE MANAGEMENT PROGRAMME: STAKEHOLDER PERCEPTIONS

By Comdt Barry Byrne

This thesis examined an internationally recognised programme carried out by the Irish Defence Forces (DF) between 2012 and 2016. This programme was aimed at improving Information and Knowledge Management (IKM) across the organisation. A Return On Expectations (ROE) methodology was selected as the most suitable assessment methodology in this instance (Kirkpatrick and Kirkpatrick, 2010). A multi-methodological approach was used for conducting this assessment across multiple stakeholder groups. Semi-structured interviews were conducted with senior leadership of the DF who were key stakeholders in this programme. These were compared and contrasted against a survey conducted with 130 respondents. The use of a case study further strengthened the validity of this research. This was supported by the introduction of an international perspective from interviews with eight experts in the field. These results were measured against the original objectives of the IKM programme and the standards set out in the new International Standards Organisation (ISO) global knowledge management system standard: ISO 3041. The analysis revealed that while the programme was successful in the early stages, there are clear capability gaps. These gaps challenge the IKM programme's resilience and its continued viability. Key recommendations were made, which are internationally relevant.

"I usually go training to relieve stress…" But what if you can't train?: THE APPLICABILITY OF THE JOB DEMANDS RESOURCES MODEL IN THE IRISH DEFENCE FORCES

By Comdt Andrew Burke

In today's world stress is omnipresent. While personnel across the Irish Defence Forces understand that stress exists, their ability to deal with it is self-taught and superficial in terms of understanding its causes and what can help to ameliorate stress.

The Job Demands Resources (JD-R) Model is an occupational stress model that sets job demands against job resources. Job demands are those aspects of the job that require sustained physical and/ or psychological effort and are associated with physiological and/ or psychological costs. Job resources are those aspects of the job that reduce job demands and the associated physiological and psychological costs.

The research showed that service in the Irish Defence Forces is stressful and that the organisations understanding of stress is limited. While serving personnel accept this, their ability to deal with stress is self- taught and based on the need to get 'space' by carrying out recreational activities. While the model was introduced to research participants summarily, they all acknowledged its relevance and suitability.

The findings demonstrate the need for a better understanding of stress in the Irish Defence Forces. It is also recommended that the Job Demands- Resources model is adopted as the occupational stress model of choice across the Defence Forces to better understand job demands and resources.

HOW CAN THE DEFENCE FORCES MITIGATE THE RISKS POSED BY NON-STATE ACTORS IN THE INFORMATION ENVIRONMENT?

By Comdt Greg Burns

British MOD (2018) have stated "that information is no longer just and enabler, it is a fully-fledged national level of power, a critical enabler to understanding, decision making and tempo, and a weapon to be used from strategic to tactical level for advantage". The significance of this evidence indicates that the Irish Defence Forces cannot operate in a vacuum when it comes to the threats posed by hybrid warfare in the information domain.

The literature highlights the growing weaponisation of the internet and its application by non-state actors to conduct hybrid warfare in the information environment. The application of these hybrid methods by ISIS and Al-Shabaab have demonstrated the significant capabilities provided by the internet as a platform to manipulate perception and radicalise followers. This thesis explores these challenges and investigates the methods employed by nation states to counter these hybrid threats.

The research of this thesis adopted a qualitative phenomenological research methodology, utilising a combination of semi-structured interviews and case studies. As part of this process, experienced DF personnel were consulted to provide an organisational perspective and subject matter experts from outside the organisation provided an in-depth look at the global challenges at the strategic level.

The research indicates the substantial security risks that exist in the information domain to the force protection of DF soldiers serving overseas. The key findings proposes that the platform provided by social media permits non-sate actors to express or exploit anger setting off additional torrents of rage. Recommendations from this study determine that the DF needs the capability to decipher reality from perception in the information domain particularly in the context of an overseas deployment

MANAGER BEHAVIOUR IN THE DEFENCE FORCES AND THE FREEDOM OF INFORMATION ACT 2014 – PERCEPTIONS OF SENIOR STAFF

By Comdt Cathal English

"Never write if you can speak; never speak if you can nod; never nod if you can wink" is a quote attributed to attributed to an old New York Democratic boss (Smyth, 2003, p. 86).

In a modern democracy where openness and transparency is rightly expected, a military organisation must find the balance between its responsibilities for security and its obligations to the institutions of civil society. This thesis sets out to explore how manager behaviour in the Irish Defence Forces has been effected by the enactment of the Freedom of Information Act 2014 and the perceptions of senior military staff around those impacts.

The research adopted a post-positivist qualitative methodology and phenomenological perspective and utilised a combination of a case study, a focus group, and semi-structured interviews with senior executives of the Irish Defence Forces.

The research results indicated that a culture of openness, an increase in transparency, and an increase in accountability have resulted from the enactment of the Freedom of Information Act 2014 in the Irish Defence Forces. The results also indicate that, after initial wariness around Freedom of Information within the military context, military management are positively disposed to the impacts that the Freedom of Information Act produced.

This thesis concludes that the culture of openness, the increase in transparency, and the increase in accountability have led to better decision making and an increased level of trust with both external and internal audiences. Finally, a number of recommendations were reached which include the release of routine military processes that would negate the necessity for Freedom of Information requests, targeted rank-appropriate education in the Freedom of Information area, specialised training in the area of 'big-data' and the consideration of.

PLACES, SPACES, AND PEDAGOGIES: IS THE DEFENCE FORCES' LEARNING ENVIRONMENT SUPPORTING THE NEEDS OF ITS LEARNERS?

By Comdt Colin Lawlor

This thesis aims to answer the central research question: is the Defence Forces' learning environment supporting the needs of its learners? A theoretical framework based on the three components of places, spaces, and pedagogies that comprise the military learning environment is employed to guide this inquiry. This research is informed by workplace learning theory, learning spaces design, and adult learning theory.

A mixed methods approach was adopted for this research. Initially, data was collected through documentary analysis of key Defence Forces' education policy documents. This was followed by the creation of a 'military learning environment survey' using 'Survey Monkey' to assess military learner's perceptions of the military learning environment. The survey was administered to members of the current Junior Command and Staff Course and Joint Command and Staff Course at the Military College. The final stage of data collection was the conduct of semi-structured elite interviews with strategic leaders responsible for officer education in the Defence Forces.

Analysis of Defence Forces education policies highlight the value placed upon education by the Defence Forces, however, some difficulties with delivering on the ambitions for education have emerged. These include inadequate funding; the absence of a coordinated Capability Development Plan with a supporting Infrastructure Development Plan, and the dilution of infrastructure responsibilities across directorates and command boundaries. Results from the survey indicate that learners are motivated to learn so they qualify for promotion and also to enhance their professional knowledge. Barriers to learning in the military workplace include inadequate time to complete tasks, heavy course workloads, and learning infrastructure problems. Findings also point to widespread dissatisfaction with the infrastructure of the Military College, accommodation facilities, learning facilities, and internet connectivity. Facilitators of learning include teaching quality, the Military College link to Maynooth University, and peer knowledge and experience sharing.

It can be inferred from these results that military learners have similar pedagogic and proxemic needs to other adult learners. Military learners also experience similar barriers and enablers of learning to other workplace learners, confirming that workplace learning theory is a useful theoretical lens for understanding learning in the military workplace.

CAN RESILIENCE ENGINEERING THEORY BE USED TO IMPROVE RESILIENT PERFORMANCE (INCLUDING SAFETY PERFORMANCE) IN COMPLEX SOCIOTECHNICAL SYSTEMS?

By Comdt David Browne

This thesis seeks to explore whether resilience engineering theory can be used in practice to improve resilient performance (including safety performance) in complex sociotechnical systems. In order to answer the question, the practical application of the theory was applied to a real complex sociotechnical system, namely the Irish Air Corps' Emergency Aeromedical Service. The research addresses a gap in academic literature within the field of organisational resilience, in that to date no research has been conducted into the practical application of resilience engineering's recently developed Resilience Analysis Grid (RAG) model in an organisation that engages in complex flying operations.

The study required a background understanding of psychological and ecological resilience theory in order to develop a sufficiently deep understanding of the existing theories that led to resilience engineering. Resilience engineering emerged in response to the lack of satisfactory performance of traditional safety management systems over the last three decades, especially in professional aviation organisations. It aims to use the knowledge that has already been gained through psychology and ecology and apply it to sociotechnical systems.

The theory proposes that successfully performing sociotechnical systems must be able to monitor the critical, respond to the actual, anticipate the potential, and learn from the factual. The RAG model, on which this theory is based, was created to assist in the practical assessment of organisational resilience and to identify where improvements in resilient performance could be made. An adapted form of this model was therefore used to assess organisational resilience in the Air Corps' EAS operation, and identify where improvement interventions could be made.

A pragmatic mixed-methods iterative approach was adapted through the use of focus groups and semi-structured interviews, with the quantitative element providing the basis for the graphic presentation of results, and the qualitative element providing the basis for a rich understanding of the problems encountered within the system and therefore allowing the opportunity to propose effective and valuable interventions for improvement.

Following data collection and analysis, it was found that the EAS operation performs reasonably well in the system's ability to monitor and respond, but considerable effort is required to improve resilient performance with respect to learning and anticipation. These improvements would create conditions for improved performance (including safety performance) and would ultimately result in the Air Corps providing greater safety for crews, improved patient care, a more efficient operation and the confidence to be prepared for the unexpected. The study demonstrated that resilience engineering theory can be used to assess organisational resilience in a complex sociotechnical system, and identify where improvements to resilient performance could be targeted.

PROTECTION OF CIVILIANS: HUMANITARIAN INTERVENTION OR POLITICAL INTERFERENCE?

By Comdt David Duff

The 2011 NATO-led intervention into Libya was predicated under a protection of civilians mandate and was the first instance of the UNSC authorising intervention into a nation without that nation's consent. Libya therefore, affords an opportunity to further the debate on the subject of both humanitarian intervention and the protection of civilians. Moreover, Libya offers a contextual platform from which to analyse the development of NATO's protection of civilians (POC) framework and may help determine the efficacy and practicality of the POC policy or indeed of intervention for humanitarian purposes itself. As primarily a defence alliance, with its raison d'être being the principle of collective defence, NATO has demonstrated its willingness to conduct humanitarian interventions in order to protect civilians. However, the current instability in Libya since the 2011 NATO-led intervention and the subsequent second order effects of that intervention give cause to question the efficacy of the intervention.

These second-order effects include but are not limited to, lack of central government control, ongoing violations of human rights and the proliferation of armed groups, in particular the rise of Islamic State in parts of Libya. This has also had the consequence of contributing to regional instability through spill over from Libya into Mali and Egypt.

At the 2016 NATO summit in Warsaw, NATO nations endorsed a specific POC policy, with its stated aim being to "instil a coherent, consistent and integrated approach to POC" (NATO 2016: 2). Can NATO's POC policy be operationalised to ensure that humanitarian intervention remains impartial and that a post-intervention Libya does not reoccur in the future? Moreover, against this background, can genuine humanitarian intervention be separated from the politics of national interest? The aim of this thesis is to examine NATO's POC policy in the context of the broader interpretation of POC and to determine if NATO is best suited to carry forward the developing political and normative assumptions of POC. It additionally evaluates the efficacy of NATO as an intervening agent on behalf of the UN and assesses the effect that the Libyan intervention has had on the development of the POC policy endorsed at NATO's 2016 Warsaw Summit.

The findings from this research suggest that NATO's POC policy itself provides nothing new and presents no further obligation to its members. As such, the policy in essence represents the bringing together of all current POC obligations of NATO nations under one policy document. Additional findings indicate that the separation of humanitarian intervention and national interest is nigh impossible and that although NATO is in itself not an altruistic organisation, it nonetheless may represent the only response option in instances of grave violations of human rights.

NEGOTIATION, A SKILL WORTH FIGHTING FOR: IS CURRENT IRISH DEFENCE FORCES NEGOTIATION TRAINING SUFFICIENT FOR OVERSEAS DEPLOYMENTS?

By Comdt Dermot Earley

Irish Defence Force officers will find themselves negotiating in conflict regions, between warring parties, on complex issues, where an alternative to peace is possible injury or loss of life. At all levels, Irish officers should be fully prepared to navigate any negotiation process successfully.

In order to identify shortcomings in the area of negotiation training, this study explores how the Irish Defence Forces train and develop the negotiation skills of its officers. It further examines avenues for professional development and competency to ensure our officers are fully prepared to negotiate effectively at home and more specifically, overseas.

A qualitative phenomenological study was accompanied by interviewing serving and retired officers who were centrally involved in overseas negotiations at varying levels. Their knowledge and experiences provided a rich description of the challenges they faced negotiating overseas and the training, or lack of, they received in preparation for such appointments. Content analysis revealed a close alignment with the literature reviewed and the research findings.

The research findings indicate that current negotiation training in the Irish Defence Forces is not adequate. It is further posited that due to our innate ability to interact and adapt with people and situations when required, negotiation training in the Irish Defence Forces has never received the focus it necessitates and therefore should become part of Defence Force formal training.

In light of these findings, a number of conclusions and recommendations are made. This thesis proposes the requirement for a modularised crisis negotiation course, for officers serving overseas in appointments that necessitate negotiation, and should be conducted in the pre-deployment phase of training. It further describes a model for crisis negotiation training, which is recommended for officer education within the Defence Forces. The adoption of such a model will meet the Defence Forces requirement to advance our current knowledge and skills in negotiations.

DESTRUCTIVE INNOVATION: AN EXAMINATION OF INNOVATION BY IRREGULAR FORCES

By Comdt Enda Moynihan

This thesis examines the nature of innovation by irregular forces such as terrorists and insurgents in order to address the following questions: 1. What drives and/or enables innovation for irregular forces? and 2. What are the most appropriate responses by conventional forces when faced with disruptive innovation from irregular forces?

In addition to examining scholarly work in the defence and security field, this work also draws on sources from the fields of business management, public policy and sociology in order to gain as holistic a view of the phenomenon as possible. The research took the form of semi-structured interviews with subject matter experts both with Counter IED experience and specialist knowledge on innovation. The relevance to the Defence Forces, as a whole, is that a better understanding of such innovations could lead to improvements in how we approach C-IED.

The key findings of the study on the question of innovation by irregular forces are that it is driven by many factors from cost, emulation, practicality and overcoming countermeasures. These factors additionally are influenced by a group's relationship with other groups and the nature of the environment in which the irregular force can operate.

Concerning the response by conventional forces, it is found that the employment of certain types of technological countermeasures and proactive measures against threat networks are limited in their effectiveness. Great value can be extracted from improved tactics techniques and procedures. The effect of organisational culture for a conventional force is significant and the degree of inertia that is inherent in large organisations is clearly an obstacle which needs to be addressed.

A REVIEW OF THE DEFENCE FORCES EMPLOYMENT SUPPORT SCHEME: DOES IT CONTRIBUTE TO POSITIVE SOCIAL IMPACT

By Comdt Eoghan O'Sullivan

As Ireland's economy approaches full employment, the rate of youth unemployment is well above the levels during the height of the Celtic Tiger. The Defence Forces Employment Support Scheme aims to provide participants between the ages of 18-24, with the knowledge and skills that will enhance their capacity to pursue employment, work experience or further educational opportunities.

The aim of this research was to review the Defence Forces Employment Support Scheme from a social impact perspective, as outlined in the White Paper on Defence (2015). In conducting the research, the relevant literature was reviewed in detail, along with qualitative analysis involving a number of key individuals who have been instrumental in developing and overseeing the scheme since its inception.

The key findings of this research were that the scheme has a positive social impact. All of the research participants spoke highly of their involvement with the scheme. An unexpected finding related to the positive effect, which the scheme has had for the Defence Forces. This is positive in an era where the Defence Forces can struggle to justify its relevance.

In conclusion, the Defence Forces Employment Support Scheme is a success. Further study may be required to evaluate the progress of the participants after the completion of the course in order to fully assess if they are in full employment, education or on the live register.

PROCUREMENT EFFICIENCY IN THE DEFENCE FORCES: BALANCING EXPERT OPINION

By Comdt James Hourigan

Procurement is a critical function for any large modern organisation. Many large modern organisations, with a wide globally-distributed structure, function optimally under centre-led procurement as they can take advantage of a number of factors that enhance efficiency. The aim of this research was to elicit consensus of expert opinion on the current state of procurement within the Defence Forces, how it might be improved, whether centre-led procurement would improve procurement efficiency and effectiveness, whether there was any appetite for change at the senior management level and to what extent change to centre led procurement was desirable or feasible for senior management in the Defence Forces.

Semi-structured interviews were carried out in order to ascertain the data in a qualitative approach. Four interviews were carried out with experts within the Defence Forces and the Department of Defence at the senior management level and one with a senior representative of the Office of Government Procurement, to provide an external unbiased perspective. Each interview was prefaced by the provision of a case study on centre led procurement to contextualise the area of research. Interviews were recorded and transcribed, and thematic coding used to identify recurring themes.

The results showed a significant degree of consensus from interviewees within the Defence Forces/Department of Defence in that there was no requirement or utility for change, except in special cases, as procurement was currently working well. The Office of Government Procurement interviewee demurred, expressing the need to constantly refine process and practice to maximise efficiency and effectiveness.

Challenges such as the cash accounting system and lack of multi-annual budgets were identified as significant impediments, in addition to skills fade due to the constant turnover of personnel and the unique nature of military service. There was a large variation in the appetite for change. Ultimately, centre led procurement was recognised as the way ahead with regards to complex and bespoke procurement, but there was no clear vision or roadmap identified by senior management as to how it should be achieved.

This thesis identified a natural tension between the need for compliance and the need for innovation and evolution of processes and practices. This should provide a platform for future research into the harmonisation of both approaches to exploit the positives from each viewpoint.

MOTHERHOOD AND THE MILITARY- APPOSING FORCES A FEMALE PERSPECTIVE

By Comdt Orla Jennings

Becoming a mother is a life altering experience on its own. When women who serve in the military become mothers for the first time their cover as conceptual men is broken. Motherhood ultimately alters the playing field.

The review of the literature focused on the institutions of work and family and examined the intersection between these two opposing arenas. Both institutions have been termed "greedy" within the literature. Role conflict emerged as a theme in two guises, first as a result of involvement in two competing systems and second from having a range of competing duties to perform. One of the major obstacles put forward for women in pursuing a career is that of balancing the new roles associated with motherhood and their previous existing work related roles. The literature points to the construct of masculinity as an emergent theme when considering women in an organisation such as the Defence Forces where they are a minority grouping. The literature also ranks organisations maturity in respect of work life balance polices and supports provided to women and the perception of these supports within both the organisation and by the recipients of these supports.

The research employed a post-positivist, qualitative research methodology utilising semi-structured interviews with senior HR managers both internal and external to the Defence Forces. Focus groups with participants drawn from all three services, Army, Air Corps and Naval Service and including both commissioned and non-commissioned officers were also exploited. This provided a broad range of views. The unique experiences of women as mothers and soldiers was captured.

This study confirmed that women re-evaluate their future careers when children arrive and based on current requirements for career progression within the Defence Forces are self-selecting not to progress. It also confirmed that the current career obstacles for many to overcome require a clear choice between family and work. This research drew attention to the fact that women are disadvantaged by common practices of performance appraisal when absent for maternity leave. This research has also demonstrated that women are highly committed to the Defence Forces and deeply appreciated of the statutory entitlements they receive.

In conclusion for the Defence Forces to recruit, retain, promote and increase the number of women within the organisation it is essential that it acknowledges that the current practices do not fit with the way women work. Failure to do so will continue to result in a loss of capability which the Defence Forces cannot afford.

SHOULD THE IRISH DEFENCE FORCES DEVELOP AN ADAPTATION PLAN FOR CLIMATE CHANGE?

Comdt Louise Fitzsimons

Ireland's climate is changing in terms of sea level rise, increases in average temperature, changes in precipitation patterns and weather extremes. The observed scale and rate of change is consistent with European and global trends. The Irish Defence Forces has been requested by local authorities throughout the country to supply defence aid for every adverse weather event since 2010. Notwithstanding supplying defence aid, defence infrastructure is experiencing the effects of climate change during these extreme weather events with increased demand for heating and cooling of buildings. This is similar to what other militaries experienced and who have since developed adaptation plans for climate change. This difference between the Irish Defence Forces and other militaries who have developed adaptation plans for climate change is that they were legislated to do so by their government.

This research found that there is a level of concern for the impact of climate change by Government, Department of Defence and Defence Forces. The Government are producing the All Government Climate Action Plan, the publication of which keeps being postponed. The Department of Defence had input into this document, yet the Defence Forces say they did not. Production of after-action review of aid to the civil authority callouts for extreme weather events vary but where produced they consistently fault equipment available to use and the suitability of military equipment for civilian use.

While the Government, Department of Defence and the Defence Forces are interested in addressing climate change they have not come together to address the issues being faced. It is therefore essential that the Defence Forces develop an adaptation plan to climate change with the support of Department of Defence and Government to have a unified approach to becoming climate resilient.

THE COMMAND STRUCTURE OF THE IRISH DEFENCE FORCES: IS IT FIT FOR PURPOSE?

By Comdt Michael Parsons

Is the Command Structure of the Defence Forces Fit for Purpose? This thesis examines the Command Structure of the Defence Forces and whether it is fit for purpose. The history of the Command Structure of Óglaigh na hÉirean is examined in detail in order to establish why the Defence Forces has the command structure it currently has, if it is suitable or are there more suitable options available.

It explores the militaries of several other nations who are in the process of changing or have already changed their Command Structures in response to the evolving security and defence arena as well as changing strategic threats. It contrasts that which caused these other nations to change their C2 against the unchanging structure of the Defence Forces. The thesis also explores various change theories, asks what the best change model for the Irish Defence Forces would be and how the Defence Forces could change were the political will to do so present.

The study revealed several findings including the fact that Jointness, in some form at the strategic level at least, may be a solution to command and control issues bearing in mind that the small scale of the Defence Forces makes this difficult to achieve. The subject matter experts interviewed in Chapter Four all agree that the Command Structure needs to change to some extent or another. It also became apparent that the Chief of Staff needs more autonomy, both from a legal and command perspective.

As a result of these findings a number of recommendations were made including changes to the establishment of the Defence Forces, the introduction of Jointness in some form tailored specifically for Irish military tasking's, the need for new branches such as cyber- warfare to deal with evolving strategic threats and the creation of a land component commander.

PREPAREDNESS FOR NATIONAL EMERGENCIES IRELAND'S APPROACH TO EMERGENCY PREPAREDNESS: A GAP ANALYSIS

By Comdt Paul Connolly

The aim of this research is to examine the national approach to emergency preparedness and to determine how prepared Ireland is for an emergency that would require the activation of the National Emergency Coordination Group. The research applies the Clark and Estes' (2008) Gap Analysis Model to identify the existence and causes of the gaps in national emergency preparedness.

The research first establishes the national high-level goals for emergency preparedness and through document analysis and interviews attempts to define the current levels of preparedness. Then by applying the Gap Analysis Model, the research examines three areas, namely Knowledge, Motivation, and Organisation, to determine the root causes of the gaps. By then comparing the gaps to the desired end state, a road map to a better level of preparedness is proposed.

Through this research I have found that Ireland is moving towards improved preparedness for national level emergencies. Policy and guidance documents exist, and key individuals recognise the need for a developed emergency management system. However, gaps also exist and will need coordination and collaboration amongst all members of the Government Task Force for Emergency Planning along with leadership and guidance from the Lead Government Departments and the Office of Emergency Planning if those gaps are to be resolved.

THE IRISH DEFENCE FORCES' APPROACH TO CONTEMPORARY CIMIC OPERATIONS IN UNIFIL: IS THE DEFENCE FORCES DEVELOPING THE NECESSARY CAPABILITY TO MEET THE OPERATIONAL REQUIREMENTS OF ITS UN CIMIC ROLES?

By Comdt Rory Esler

The thesis will examine the Irish DF's approach to contemporary CIMIC operations in UNIFIL. The question that provides direction for this thesis is: *Is the DF developing the necessary capability to meet the operational requirements of its UN CIMIC roles?* Essentially, this research examines how the DF selects and trains personnel for this operational task to ensure the organisation can meet the UN's requirements.

Selection for overseas service is generally conducted in a structured way within the Defence Forces to ensure a fair system is available to all personnel. This research examines whether there is a link between individuals selected for operational roles overseas and the suitability of such individuals.

Pre-deployment training of personnel selected for tactical CIMIC appointments in UNIFIL is the main focus of the research. International military best practice is considered, as well as published literature regarding areas of importance for pre-deployment training. In particular, training in cultural awareness, negotiation and language skills is examined to establish what level of training in these softer military skills is available to military personnel, pre and post-deployment.

Interviews conducted with the selection and training authorities within the DF reveal how the organisation deals with these areas. Focused semi-structured interviews with officers with a combined total of five years' experience in tactical CIMIC appointments in UNIFIL provide detail of the lack of formal training in these skills. However, the Irish DF still manage to meet all operational requirements assigned by the UN.

There is no doubt that the Irish DF is meeting the operational requirements of its UN CIMIC tasks, but it may be doing so by consequence of its soldiers' collective attitudes and behaviour, rather than by design. The empathetic nature of Irish soldiers and their ability to apply an 'Irish approach' to any and all scenarios they encounter during deployment positively influences the attitude of the local population towards the deployed force. The intricacies of peace-keeping appear to come naturally to Irish soldiers.

MOTIVATIONAL CLIMATE IN THE CADET SCHOOL: THE INFLUENCE OF CLIMATE IN A PHYSICAL TRAINING ENVIRONMENT

By Comdt Ross Dunphy

This thesis examines if the motivational climate in the Cadet School of the Irish Defence Forces facilitates individuals to reach their physical fitness potential. It examines specifically the impact of organisational climate and outlines the current understanding of how climate influences motivation. The conceptual framework draws from the existent literature in organisational climate, motivation, sensemaking, social comparison and goal setting and situates these in the context of inductees in this military training environment.

A mixed methods research approach was employed. This comprised of questionnaires, previous fitness test results, focus groups and semi-structured interviews with both newly commissioned officers and cadets, and key influencers in the Cadet School. The key findings indicate that section commanders, platoon sergeants and platoon commanders are the main architects of climate within the Cadet School. Climate plays a significant role in restricting certain cadets from achieving their full physical training potential, and this has knock-on effect on the other areas of their training. The findings also indicated a gendered nature to this phenomenon. A physical training regime that incorporates a realistically high level of personal challenge and which also includes the possibility of both ability-based individual and group elements of physical training increases motivation to succeed. Approaches to the recognition of injury on the part of key influencers have serious implications for psychological well-being for feelings of efficacy in relation to other areas of cadet preparation.

Recommendations include a comprehensive approach to human performance, development of an educational framework for both staff and students and a physical training environment centred on a team-based military ethos incorporating individual and group-based goals.

THE IRISH DEFENCE FORCES: APPLICATION OF FORCE PROTECTION ACROSS UN MISSIONS

By Comdt Shane Phelan

As soldiers, it is expected that we will be placed, at times, in harm's way. We do after all deploy soldiers to assist our public services in on-island operations, including tasks such as flood relief and firefighting. We conduct live fire training exercises and deploy our soldiers on overseas missions suffering injury and loss of life. This aim of this research is to determine best practice when assessing risks and their application to Force Protection measures adopted on UN missions from an Irish military perspective.

Combining semi-structured interviews of highly competent individuals with some pre-existing textual data, the study found that many factors at the tactical, operational and strategic level influence a mission's, country's or an individual's appreciation and application of force protection. The adoption of a Force Protection doctrine and its implementation will mitigate those risks which soldiers can be subjected to on overseas missions to as low as is reasonably possible while also fulfilling the mission those troops were sent to achieve.

The main findings of this study are that NATO Force Protection doctrine is the best approach to Force Protection and should be implemented and espoused by the Irish Defence Forces on-island and overseas. National and individual approaches to force protection significantly affect a mission's approach to force protection. In general, culture changes slowly, with the possible exception being shocks to systems which can generate a more rapid rate of change. Ireland's significant contribution to peacekeeping can be further enhanced by being a positive influence for change in the area of force protection and the safety of all soldiers on overseas missions.

MAKING A CASE FOR IRELAND TO ADOPT A NATIONAL MARITIME SECURITY STRATEGY.

By Lt Cdr Bernard Heffernan

Ireland, as an island nation, is heavily dependent on the seas for social, political and economic deliverables and requires that this maritime domain is secure for its survivability. Despite this requirement for security, Ireland has not developed a maritime security strategy.

The aim of this thesis is to make a case for Ireland to adopt a national maritime security strategy as the literature review highlighted that island nations with a heavy dependency on the oceans should implement a maritime security strategy. The literature review also highlighted that the creation of a maritime security strategy can be utilised to define the maritime governance of a state and that the methods to complete this requirements requires states to conduct maritime security sector reform.

This research adopted a qualitative research design with a social constructivist approach. Data was collected utilizing a focus group to form the questions for the conduct of semi-structured interviews of the senior command of the Naval Service and of a leading Irish academic expert.

The findings of this research indicate that a maritime security strategy is required as it would resolve the current siloed approach in Ireland towards maritime national security. This is due to the disperse allocation of maritime responsibility across all government departments that has no central coordinator with authority. The findings of the research further reflect that a maritime security strategy is a key enabler to economic development of the maritime sector, however, maritime sector reform is required.

The key finding of this research is that a case does exist for Ireland to adopt a maritime security strategy.

THE FUTURE MODEL OF JOINTNESS WITHIN THE IRISH DEFENCE FORCES: HOW DO WE GET THERE?

By Lt Cdr David Memery

Irish Government policy expresses the intent that the Defence Forces should operate 'Jointly', that is to deliver effects in a coordinated and cohesive manner. Building on previous research, the aim of this study is to identify, analysis and ultimately recommend what model of 'Jointness' is best suited for application within the Defence Forces.

As part of this analysis, it is important to take cognizance of the prevailing cultures within the component services that constitute the Defence Forces and how such cultures will impact upon the transition to achieving joint effects, with particular emphasis upon the level of understanding that exists within the Defence Forces as to a 'Joint' concept and the application of various levels and models of joint organizational structures that can be employed.

This study initially examines a broad swathe of academic literature, determining that although a significant proportion of this literature is focused upon the implications of Joint structural dynamics in larger, more kinetic, military structures, there exists utility in its employment in the context of establishing an analysis of Jointness within the Irish context.

This study also adopts a Realist, Post-Positive ethnographic approach to examine the individual service culture, the overall organisation Defence Forces culture, and how they interact in the context of organisational change.

Findings from this research indicate that the Defence Forces has developed to become increasingly Joint and that a broad, yet diverse, understanding of the utility of a joint concept exists. Findings also determine that the organisational cultural dynamics have reduced in severity, despite the existence of cultural barriers.

This shift in the cultural organisational dynamic provides a window of opportunity for the Defence Forces to further develop a Joint concept; however, the window of opportunity is finite and may close if the Defence Forces does not take advantage of its current position.

"THE NEW COLD WAR"

By Lt Col Daniel Wicke

After the end of the Cold War NATO's old adversary, the Soviet Union had fallen apart and its successor, Russia, sank into insignificance. NATO faced other conflicts and concentrated its efforts on fighting international terrorism and other threats for the international community. But fighting insurgents and terrorists worldwide influenced NATO Forces on both sides of the Atlantic Ocean, in their structure as well as in their ideology and mindset. In Europe, former Warsaw Pact members decided to join NATO and took shelter under the umbrella of NATO. Consequently, military forces were adjusted to the new security environment and were reduced dramatically throughout Europe.

With NATO expanding its area of responsibility to the East, Russian sphere of influence has been decreased and Russia expressed – more than once – its unwillingness to accept this new situation of being surrounded by its previous enemy. In March 2014 the Russian bear roared again and reminded Europe that the old and well-known adversary of the west is back on stage. The Chief of the Russian General Staff, General Waleri Gerasimov used a new strategic concept of expanding Russian influence through all possible means. This approach was later described as the so-called "Gerasimov Doctrine" and illustrated the idea of hybrid warfare.

Acknowledging the problematic history of the German – Russian relations, this thesis describes the development of the German Army, after Russian illegal annexation of the Crimean Peninsula and its aggression in Eastern Ukraine. It assesses the development of NATO towards a higher status of readiness and responsiveness and describes the political framework in which German forces are set.

This thesis is aimed to provide an impression of the capabilities modern Land Forces must provide to withstand a hybrid adversary on a more and more digitalised battlefield. They are derived from the lessons learned from current conflicts, a possible path of development for the German Army described, as well as several individual actions are recommended.

TRANSFORMATIONAL VERSUS TRANSACTIONAL LEADERSHIP IN US ARMY LOGISTICS LEADERS

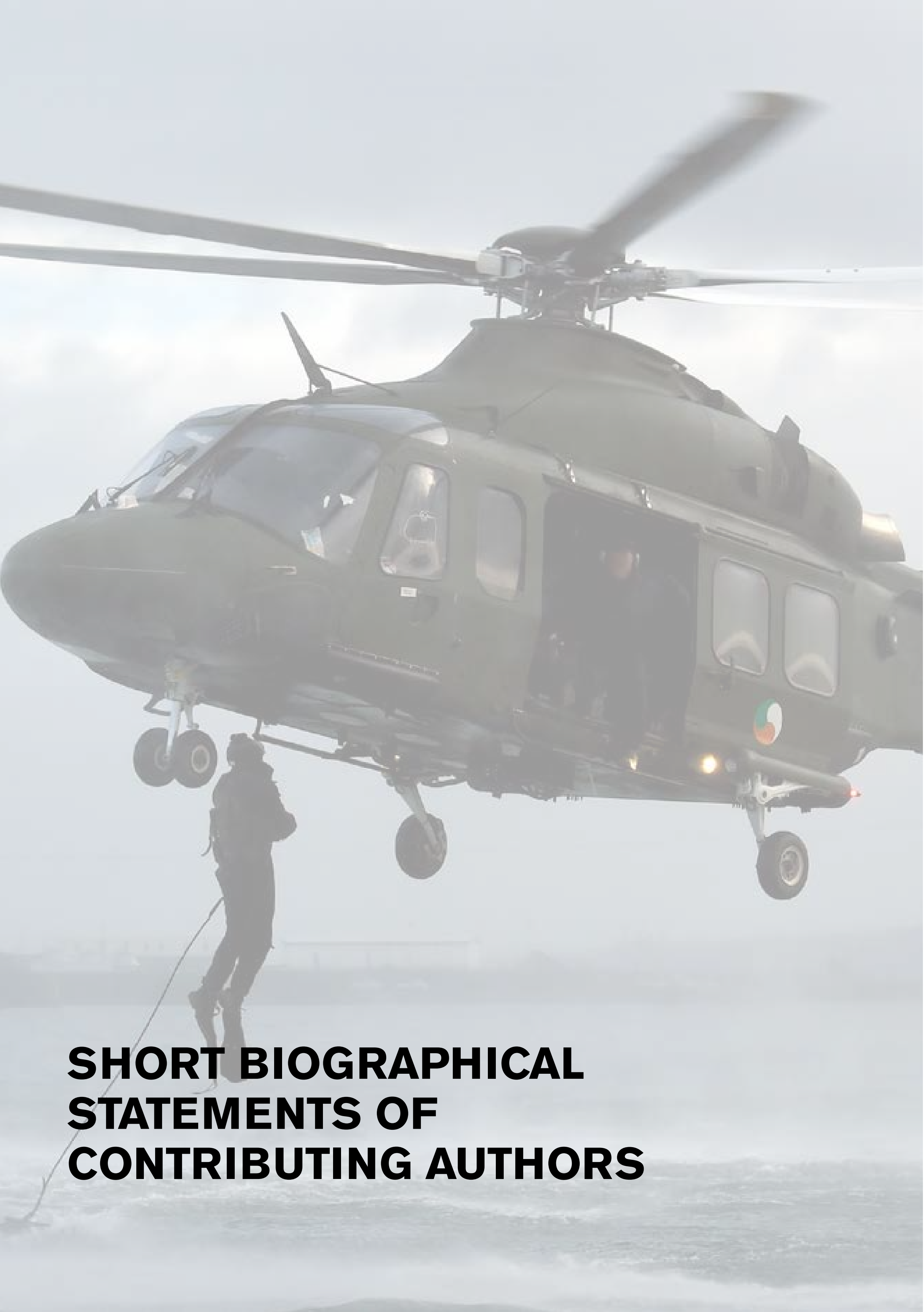
By Major Samantha Smay

The US Army is a global network that would not be effective without a good logistics network. A good logistics network needs effective Logistics Officers to be effective. The purpose of this research paper is to examine which leadership style is more effective, transformational or transactional for US Army logistics officer.

This study aims to determine the effective leadership style for US Army Logistics Officers in order to gain a better understanding of the current leadership styles used and when to use them to be more effective. After analysing the current literature, the research revealed that past studies used the Multi-factor Leadership Questionnaire (MLQ) as a basis for research, and there is a gap in styles of leadership used in logistics. While the MLQ is a sound model, it does not reveal the human aspects of leadership. Therefore, the study used a qualitative method of research using authoritative knowledge, subjective epistemology, relativist ontology, naturalist methodology and balanced axiology to conduct the research.

The study was conducted through semi-structured interviews analysed using reoccurring themes by coding the data into smaller packets. Ultimately the study confirmed five characteristics of an effective logistics officer in explaining the why, communication, building the team, trust, and accomplishing tasks based in current literature.

The study revealed three factors in choosing which leadership styles is more effective based on situation-based, position-based and environment-based. The findings of the study demonstrate that further research is needed using qualitative methods and a larger sample to examine using a blend of two leadership styles based on the three factors.



SHORT BIOGRAPHICAL STATEMENTS OF CONTRIBUTING AUTHORS

Dr. Donna O'Shea is Head of Department of Computer Science at Cork Institute of Technology, Funded Investigator at the SFI research centres CONNECT and ENABLE and group lead of Ríomh – Intelligent Secure Systems research group and member of Nimbus Research Centre. Donna's research expertise lies in the area of enterprise security (i.e. SDN and NFV security) and network and service management with a specific focus on the design, analysis and optimisation of wired and wireless communication systems, networks and services.

Dr. Mubashir Husain Rehmani received a B.Eng. Degree in computer systems engineering from Mehran University of Engineering and Technology, Jamshoro, Pakistan, in 2004, the M.S. degree from the University of Paris XI, Paris, France, in 2008, and the Ph.D. degree from the University Pierre and Marie Curie, Paris, in 2011. He is currently working as Assistant Lecturer in the Department of Computer Science, Cork Institute of Technology, Ireland. Prior to this, he worked as Post Doctoral Researcher at the Telecommunications Software and Systems Group (TSSG), Waterford Institute of Technology (WIT), Waterford, Ireland. He also served for five years as an Assistant Professor at COMSATS Institute of Information Technology, Wah Cantt., Pakistan. He is currently serving as an Area Editor of the IEEE Communications Surveys and Tutorials. He is also serving as Column Editor for Book Reviews in IEEE Communications Magazine.

Dr. Brendan Flynn is a lecturer at the School of Political Science and Sociology, NUI, Galway. His current research interests include maritime security and defence and security studies more broadly. He teaches European politics and Ocean and Marine politics and has lectured at the Joint Senior Command and Staff Course. He was a co-editor of the 2018 Defence Forces Review. Recent publications include: Flynn, Brendan (2019) "From hand-me-down navies to niche players? Comparing the navies of (very) small European states", pp. 51-70 in McCabe, Robert, Deborah Sanders and Ian Speller (eds.) Europe, Small Navies and Maritime Security Balancing Traditional Roles and Emergent Threats in the 21st Century. London: Routledge; Flynn, Brendan (2018) 'PESCO and the Challenges of Multilateral Defence Cooperation for Ireland: More of the Same or Sea Change?'. Irish Studies In International Affairs, 29 :1-23.

Jonathan Carroll, a graduate of Maynooth University with a Degree in Civil Law and a Master's in Military History and Strategic Studies, is currently a PhD student in Military History at Texas A&M University, a United States Senior Military College. Jonathan's research focus is on military operations other than war (MOOTW). He is currently working on a project examining the multinational military interventions in Somalia from 1992-1995. Previously, Jonathan was an adjunct lecturer with the Center for Military History and Strategic Studies at Maynooth University, providing academic instruction to Defence Forces cadets, potential-officer, and officer progression career courses. Jonathan also served in the Army Reserve as an NCO, and subsequently a commissioned officer, with units in Dublin, Athlone and the Defence Forces Training Center

Capt Kevin Fitzgerald works as a helicopter pilot in No. 3 Operations Wing in the Air Corps, and as a press and public relations officer. He has a background in aeromedical flying and police flying, and works primarily as a flight instructor in the helicopter school. Kevin has a particular interest in development of the Special Operations Forces rotary capability in the Defence Forces.

Capt James Northover
BSc In Management and Aeronautical Studies, DIT
BSc Honours Aviation Technology with Pilot Studies. University of Leeds.
BSc Honours Management and Aeronautical Studies

Lt David Finnegan is a pilot with the Maritime Surveillance and Airlift Squadron of the Irish Air Corps. He is also a founding member of the Defence Forces RPAS school who provide education, training and flight safety information to all members of the organisation in all matters pertaining to RPAS operations both at home and overseas

Dr. Sharon Feeney is Head of Learning Development, College of Business, Technological University, Dublin. She is a board member of the Higher Education Authority (in the role of Deputy Chair from 2016 – 2020) and is Chair of the Audit and Risk Committee (2016 – 2021). Her research interests focus on higher education policy at the institutional, national and international levels, with particular emphasis on gender equality, teaching and learning enhancement in higher education, quality systems, and qualifications and awards frameworks

Dr. Daniel Fiott is Security and Defence Editor at the EU Institute for Security Studies (EUISS). At the EUISS, Daniel analyses European defence policy, CSDP, defence capability and industrial issues and hybrid threats. Daniel was educated at the University of Cambridge and he holds a PhD from the Free University of Brussels (VUB). He is the author of Defence Industrial Cooperation in the European Union: The State, the Firm and Europe (Routledge, 2019).

Eoin Micheál McNamara is currently in the completing stages of a PhD in political science at the University of Tartu in Estonia. His monograph is focused on NATO stabilisation strategy in Afghanistan. Since 2013, McNamara has taught extensively at Tartu's Johan Skytte Institute of Political Studies, convening courses in: foreign policy analysis; transatlantic relations; EU security policy; alliances in international politics; and power in international politics. His research interests include: NATO transformation; comparative security policy in Central and Eastern Europe; Nordic-Baltic security; and the strategies of war in the contemporary world. McNamara's academic and policy publications have appeared in the NATO Review, the Revue Militaire Suisse, New Eastern Europe and Irish Studies in International Affairs, as well as with research institutes including the Finnish Institute of International Affairs (Helsinki) and the Foreign Policy Research Institute (Philadelphia). His commentary on security and defence affairs has been quoted in many international media outlets; these include the New York Times, the Irish Times and the Estonian Public Broadcasting Service (ERR). In July and August 2019 he was awarded the Think Visegrád Fellowship at the Institute of International

Relations (IIR) in Prague, Czech Republic to undertake research on the Visegrád states and the development of collective security along NATO's 'Eastern flank'. He holds an MSc in security studies from University College London; an MA in European Union – Russia studies from the University of Tartu; and a BA (Hons.) in history and politics from University College Dublin.

Comdt Gavin Egerton is a professional Army officer with 17 years' service in the Infantry Corps. He was commissioned in 2004 and commenced his career with 3 Infantry Battalion. He later served in 1 Mechanised Infantry Company; 4 Infantry Battalion; 1 Brigade Training Centre; Officer Training Wing, Infantry School; and Strategic Planning Branch, DFHQ. His most recent appointment was as Officer-in-Charge and Chief Instructor of the NCO Training Wing, Infantry School. He has served overseas on three previous occasions: as a CIMIC officer with 101 Infantry Battalion MINURCAT, as Company 2IC with 108 Infantry Battalion UNIFIL, and as battalion operations officer with 110 Infantry Battalion UNIFIL. Comdt Egerton holds a Bachelor of Business degree from GMIT; a Higher Diploma in Leadership, Defence, and Contemporary Security from Maynooth University; as well as a first class honours Master's degree in Political Communication from Dublin City University. He is currently deployed to EUTM Mali where he is serving as the Deputy Chief Instructor in the Education and Training Task Force.

Dr. David Reindorp is a member of Vedette Consulting Limited's Battle Staff Coaching Cadre. He is currently working with the UK's 2* Maritime Battlestaff and Standing Joint Force HQ as they develop the decision making skills and processes necessary for warfighting in today's uncertain and ambiguous operating environment. David has a PhD in Strategic Studies and an MPhil in International Relations. In a previous career he commanded warships for the Royal Navy and developed military and defence strategy for the MOD.

Pte (AR) Eoin O'Shea serves as a reservist in 7 Inf Bn but is currently seconded to the PSS for research taskings. His civilian professional career involves working as a counselling psychologist and CBT therapist. He is additionally qualified in both CISM (IT Carlow) and Psychological First Aid (International Federation of Red Cross, Copenhagen). Areas of experience and interest include: Psychological therapies (primarily cognitive behavioural therapy/CBT), occupational stress, psychological trauma and PTSD, online mental health support, and training/lecturing. He currently works for the Irish Red Cross where he provides psychosocial support for Syrian refugees settling in Ireland, as well as training and support for staff and volunteers at the organisation. Previous employment has included the post of Senior Psychologist at 'Combat Stress', a UK mental health charity for veterans and reservists affected by PTSD as a result of their service.

Capt (AR) Mathew McCauley is a commissioned army officer and the first consultant clinical psychologist to serve in the Irish Army Reserve. He is assigned to DF Headquarters as consultant advisor in the Office of Director, Medical Branch. Capt McCauley completed his doctoral residency at the UK's Royal Centre for Defence Medicine, followed by training at Britain's Defence School of Healthcare Education and the US Centre for Deployment Psychology. Prior clinical psychology appointments include six years with the US Department of Defense as part of a Global War on Terror assignment, where he was based with the USAF's

48th Medical Group, 48th Fighter Wing and 423rd Medical Squadron, 501st Combat Support Wing. His background also involves seven years with Defence Medical Services, Joint Forces Command, UK Ministry of Defence (MOD), where he was lead MOD consultant clinical psychologist in Scotland and Northern Ireland. Capt McCauley has served as an observer controller on Operation Bushmaster with the US Uniformed Services University of the Health Sciences. He is currently assigned to NATO's Science and Technology Organisation and he remains active in military psychology research as an academic at Trinity College, University of Dublin. Capt McCauley was the guest editor and co-author of the 2019 Special Issue on Military Psychology for the Journal of the Royal Army Medical Corps. He is furthermore a co-founder and committee officer for the Section on Psychology in Defence and Security within the British Psychological Society; and is also a member of the executive committee of the Reserve Defence Forces Representative Association.

Comdt Dorota O'Brien is a commissioned army officer and is the first fulltime clinical psychologist to serve with the Irish Permanent Defence Forces (PDF). She has held this clinical appointment for over 12 years and is currently the manager of the PDF clinical psychology service, which operates as part of the DF Central Medical Unit. Comdt O'Brien oversees the clinical management and provision of psychological care to personnel who serve within the Irish army, air corps, and naval service. She supports serving personnel on main overseas deployments to UNIFIL and UNDOF as well as on smaller tours of duty to KFOR, UNTSO and MINUSMA. As a member of various working groups and boards, she is responsible for creating and delivering Defence Forces Mental Health and Wellbeing Policy and Defence Forces Transgender Strategy. On an international level Comdt O'Brien represents Ireland on the Military Mental Health Expert Panel for NATO and PfP. She remains an active member on an international panel with her most recent involvement in drafting the consensus of fitness to deploy for all nations.

Comdt Ken Sheehan is a Communications and Information Services (CIS) Officer with 17 years service. He has served in a wide variety of appointments and units throughout the Defence Forces, including 1 BTC, 1 Bde HQ, 1 Bde CIS and 2 Bde CIS. Comdt Sheehan has just completed a two year appointment as OC 1 Bde CIS Coy, where the main effort of the unit was the roll out of the Virtual Desktop Architecture system. He has served overseas with UNMIL, EUFOR Chad, KFOR and UNTSO. Comdt Sheehan holds a MA in International Relations from DCU, a HDip in Leadership, Management and Contemporary Security from NUIM and a BSc in Computer Science from UCC. He is currently serving overseas with the 115 Inf Bn, UNIFIL.

Lt (NS) Shane Mulcahy is an Operations branch officer with 15 years' experience in the Naval Service. He qualified as a Naval Diving Officer in 2010, and was the first DF member to complete the Royal Canadian Navy's Mine Warfare and Clearance Diving course in 2013 and was awarded best student. He deployed to the Mediterranean in 2015 as the Search and Rescue officer for the first NS overseas humanitarian mission, OPERATION PONTUS. He has served in various appointments ashore and afloat, deploying on diving operations across the country as a member and officer in charge of the Naval Service Diving Section (NSDS). He holds a BSc Hons in Nautical Sciences, and is currently completing a LLB in Law while serving as staff officer in the Naval Operations Command Centre.

Comdt Mike Hosback was commissioned in 2003 as an Infantry Officer. He has served in a variety of command, staff and training appointments in 2 Bde, the Defence Forces Training Centre and Defence Forces Head Quarters. His overseas postings include tours of duty with the United Nations in Liberia and Democratic Republic of Congo, NATO in Kosovo and the European Union in Somalia. He holds a BA and MEconSc from University College Dublin, an MA in History and Strategic Studies from NUI Maynooth and an MMAS from the United States Army Command and General Staff College, Fort Leavenworth, Kansas. Comdt. Hosback is currently posted as a member of the instructional staff at the Command and Staff School, Military College.

Caitríona Heinl is Director of The Azure Forum for Contemporary Security Strategy, Ireland. With over ten years experience in think tank and academic environments, she continues her work on issues that include international cyber policy, cyber diplomacy/military cyber stability and the implications of other emerging and disruptive technology security challenges for state behaviour and international stability as well as the EU and Asia Pacific regional security architectures. She publishes policy reports, academic articles, and government reports, contributing to research projects for government and corporate clients. She frequently lectures and addresses audiences globally, including at forums such as ASEAN/ARF, OSCE, UN, NATO and Track 1.5/Track 2 government events.

Steven Harland is a strategic advisor currently working with the UK Ministry of Defence on Information Manoeuvre and Full Spectrum Joint Effects, with a particular emphasis on operations below the threshold of armed conflict. He has worked on future conflict, Network Centric Warfare, intelligence fusion for counter terrorism, and the application of cyber and information operations. Steven was formerly Intelligence and Cyber Programme Lead at MOD Niteworks and is an Associate Fellow of the British Psychological Society.

Dick Hemsley is a former soldier and airman, who established Vedette Consulting in 2010. His private passions include the study of military history, whilst his professional interests are centred around the command and control of integrated operations, and the innovative exploitation of digitally-shared information and intelligence in their support. The practical application of strategic theory in the new era of ‘persistent competition’ is a current focus.

Matthew G O'Neill is a Leverhulme Interdisciplinary Network on Cybersecurity and Society (LINCS) postgraduate research student in Political Science at the Senator George J. Mitchell Institute for Global Peace, Security and Justice at Queen’s University Belfast. His research explores the European Union Digital Single Market.

Mark Williams is a Leverhulme Interdisciplinary Network on Cybersecurity and Society (LINCS) postgraduate research student at the Senator George J. Mitchell Institute for Global Peace, Security and Justice at Queen's University Belfast. His research explores the interface between the social sciences and electronic engineering and computer science focussing primarily on the criminal use of social media. In his project, he is looking at ways of detecting and preventing inappropriate and criminal behaviour in social media, with particular emphasis on the mitigation, policing and prosecution of offensive online expressions.

Lt (NS) Stephen Ryan is an Operations Branch officer in the Naval Service, commissioned in 2016 with the 54th Naval Cadet Class. He holds a BSc in Zoology from UCC, a BSc in Nautical Science from CIT and an MSc in Conservation and Land Management from Bangor University. His interests include reading, photography, and hiking. He is currently serving as the Gunnery Officer on LÉ William Butler Yeats.

Lt Col Timothy O'Brien is OIC Planning and Capabilities Section in Defence Forces Headquarters Directorate of Operations and Planning. Commissioned in 1990 an infantry officer he has served in a variety of command, staff and training appointments throughout the Defence Forces, most recently as School Commandant of United Nations Training School Ireland. His overseas deployments include tours of duty with the United Nations and NATO in Lebanon, East Timor, Afghanistan, DR Congo and Syria. A graduate of UCG, DCU, NUI Maynooth and the Institute of Public Administration, Lt Col O'Brien's academic qualifications include a Masters in International Relation Relations and a Diploma in European Union Studies.

Wesley Bourke is the Chief Executive Officer (CEO) of The Irish Military Heritage Foundation. He holds a Bachelor's Degree (Hons) in War and Security Studies from the University of Hull; a Master's Degree in War in the Modern World from King's College London; and a Master's Degree in Military History and Strategic Studies from NUI Maynooth. He is currently involved in an extensive project exploring identity, culture, and reconciliation in modern Ireland. He has been invited to participate in The Institute of International and European Affairs (IIEA) defence series entitled: The Security and Defence of Small European States: Challenges, Options and Strategies in the European Union.

Dr. Kyriakos I. Kourousis is a Senior Lecturer (Associate Professor) in the School of Engineering of the University of Limerick. He is the Director of the undergraduate and postgraduate programmes in airworthiness. Dr Kourousis also leads the establishment of the University's new 3D Printing Hub, following the recent award of a Metal 3D printer from General Electric. Dr Kourousis holds a BSc (Hons) in Aeronautical Engineering, from the Hellenic Air Force Academy, and an MSc and PhD in solid mechanics and metal plasticity, both from the National Technical University of Athens. He has 19+ years of professional and research experience in the fields of airworthiness, metal plasticity and additive manufacturing, as both an aeronautical engineer and a University academic in Ireland and Australia. He has extensive experience on fighter aircraft maintenance, airworthiness and structural integrity management, earned from his 12 years' career in the Hellenic Air Force as an Aeronautical Engineering Officer, where he specialised on the Mirage 2000. He is currently a Major of the reserve force. To date, Dr Kourousis has authored 72 peer reviewed journal and conference papers and more than 30 technical and engineering reports in the fields of his research and professional expertise. His research work has been recognised internationally, has attracted funding from various civil, and defence organisations and companies. Dr Kourousis has led research, consultancy and training projects on military airworthiness, funded by the Australian Defence Force technical airworthiness authority and other defence clients. His work on aerospace metals has been primarily focused on the development and implementation of plasticity models for military aircraft fatigue life predictions, for application in life extension and airworthiness sustainment. Dr Kourousis is a Chartered Engineer, registered with the United Kingdom Engineering Council, and a Fellow of the Royal Aeronautical Society. He is also a member of the Royal Aeronautical Society's Airworthiness and Maintenance Specialist Group and a Professional Member of the International Federation of Airworthiness.

Capt (AR) Chris O Slatara enlisted FCA 1986 Griffith Barracks . Commissioned 2001 into 20 Inf Bn Rathmines , then served 62 Inf Bn, 1 Mech Coy, and transferred to CIS in 2016, serving as instructor in CIS School, DFTC. Work as Principal Consultant for Version 1 Software in Dublin, largely in database, integration and cloud areas. Experiences with European Union Battlegroups and Viking led to authoring the End User training syllabi for Sitaware, the selected Common Operating Picture for the Defence Forces.

Printed by the Defence Forces Printing Press Jn15741/Nov2019/2000