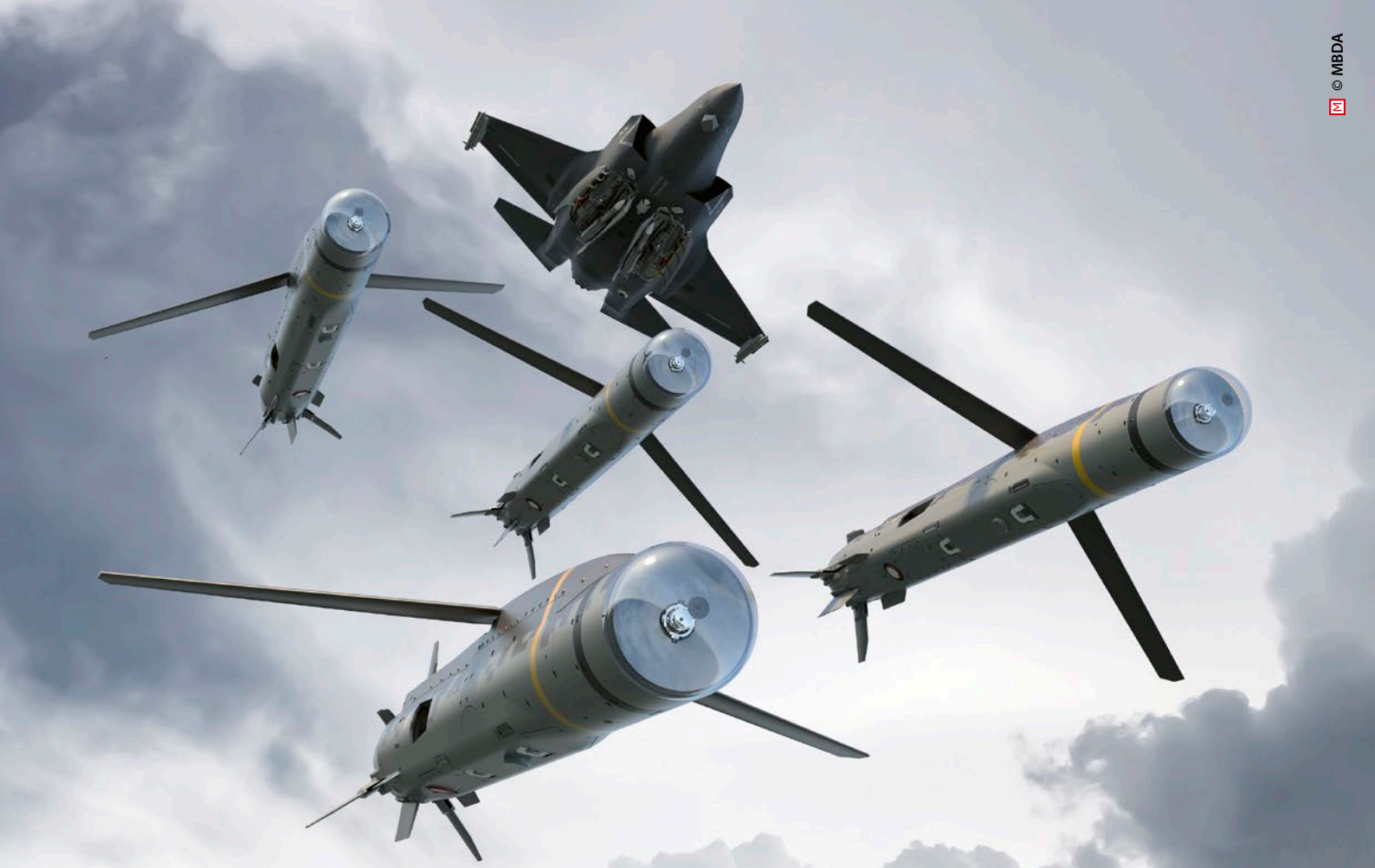


Good News or Bad News?

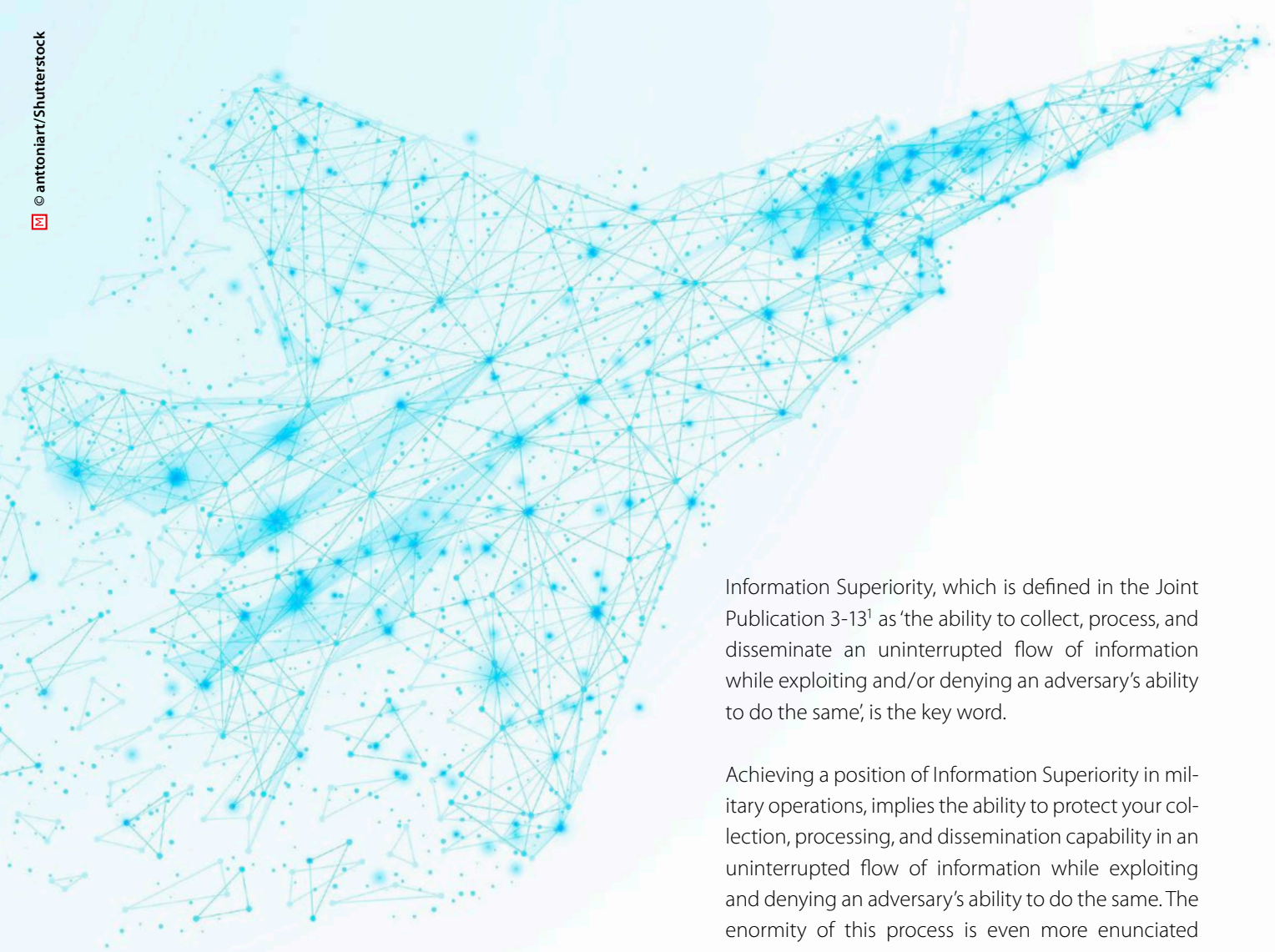
Embryonic Development of Network Enabled Weapons

By Lieutenant Colonel Francesco Esposito, IT AF, JAPCC
By Mr Adam T. Jux, BA, Civilian Targeting Consultant

In the past few decades, the way we have understood conflict and war has seen a tremendous change. War had traditionally been understood as armed physical violence. Today, global security challenges are changing faster than in the past. Adversaries are more adaptive and able to counter their opponents from the five recognized domains: air, sea, space, land, and cyber.

All modern forces involved in military operations are now more interconnected, mutually dependent, and challenged. The ability to operate is questioned by the rapid proliferation of advanced and emerging technologies. These technological innovations, and the ever-growing dependence on the electromagnetic spectrum are affecting military operations, which requires an ever more careful examination on how forces will sense, plan, decide, and act coordinated across all domains in the future.

The purpose of this article is to frame the new generation of Network Enabled Weapons (NEWs) into a present-day multi-domain conflict, identifying strengths and weaknesses, and providing conclusions and recommendations. To achieve this aim it is essential to briefly introduce the concepts of Information Superiority, Multi-Domain Operations (MDO), and Command and Control (C2) networks in modern warfare.



Definition of Information Superiority

All elements of intelligence involved in a conflict or operation collect vast quantities of information.

The advances in Information Technologies (IT) and the ability of modern military forces to take advantage of these opportunities, are significantly altering the nature of the conflict in which we expect to be involved in the future.

Specifically, IT changes the nature of our mission, the battlespace in which we operate, our adversaries' capabilities, our ability to sense and understand the battlespace, the capability of our weapons, and, perhaps most importantly, our ability to conduct C2.

Developing and analysing such a large quantity of data is a challenge, especially when taking into account the multiple levels of security at which these systems operate.

Information Superiority, which is defined in the Joint Publication 3-13[1] as 'the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting and/or denying an adversary's ability to do the same', is the key word.

Achieving a position of Information Superiority in military operations, implies the ability to protect your collection, processing, and dissemination capability in an uninterrupted flow of information while exploiting and denying an adversary's ability to do the same. The enormity of this process is even more enunciated when, with the advancements in technology, the information being collected still exceeds the physical processing capability. Every asset has a sensor and this will only increase exponentially.

Multi-Domain Operations

The relationship between Information Superiority, the high level of shared battlespace awareness, and the necessity to operate jointly in all domains brings together a new warfighting concept known as MDO. By synchronizing global and local systems and crucial data sources with innovative simplicity, MDO presents a complete picture of the battlespace allowing warfighters to take fast decisions to steer actions. The ability to do it quicker than your opponent will allow NATO to achieve information superiority, leading to increased battlespace awareness to gain the initiative.

The new MDO contribution to the battlespace is a combination of physical and electromagnetic common operational pictures, enhanced by exploited

cognitive applications and artificial intelligence. It is designed to detect [sic war] emissions, optimize Intelligence, Surveillance, and Reconnaissance (ISR) sensor collection, and autonomously update aircraft and weapons routes based on threats.[2]

New C2 Network

Understandably, a new operating concept needs a new joint C2 structure.

The new C2 framework requires secure, reliable, and affordable communication structures in order to integrate platform sensors, data, and operators (including weapon systems and decision-makers) in a contested, lethal or non-lethal electronic warfare environment. It will require a more complex Data Exchange system than the current formatted messages and, therefore, there is a need to devise a brand new network or improve an existing one. We must be mindful that many of the communications systems that we utilize today as a coalition are particularly dated. Nations must embrace a mindset of flexible procurement to ensure connectivity with our partners.

Network-Enabled Weapons

The need to ensure that all single systems are well integrated to benefit from this concept is shifting, more than ever, with military investments focusing towards increased network integration, data fusion, and NEWs.

NEWs represent an emerging class of Precision-Guided Munitions (PGM), which are able to integrate and share information between platforms and systems. They differ from the standard operational weapons by their enhanced post-launch C2 facilitating attacks on fixed, moving, and time-sensitive targets within moments of their detection and under any weather condition.

The ability to find, track, and engage a target will become faster in the future, as will reports on damage assessment. This helps to reduce the potential for fratricide and increase interoperability in targeting. These weapons will be fully integrated into the new network, exchanging information between themselves and the nodes linked to the network itself. The result is a weapon that collaboratively interfaces with systems, potentially acts as an ISR platform en route to its target, adjusts its trajectory in-flight to optimize effort, and provides real-time impact assessment (when equipped with Electro-Optical/Infra-Red (EO/IR)).

Current technology allows NEWs to contribute to a network with 2-way communications. This means that the weapon is able to coordinate attack, coordinate sensor use, and provide ISR.

Strengths and Weaknesses of NEWs

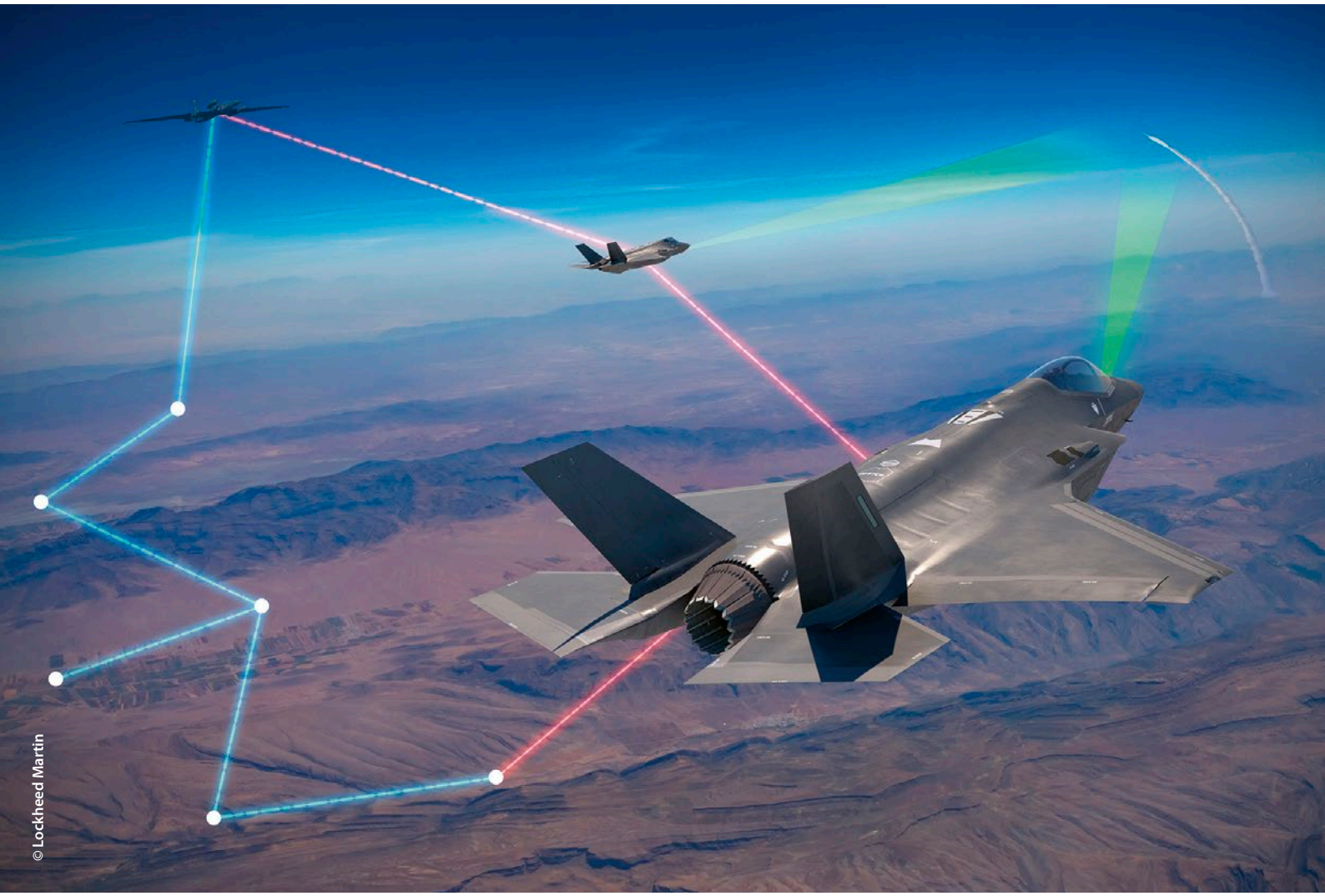
Strengths

1. Acquisition of Fixed and Moving Targets at Long Ranges Using Existing Intelligence, Surveillance, Target Acquisition, and Reconnaissance (ISTAR) Assets

ISTAR system data, imagery, and information are often crucial elements in the successful detection, identification, and engagement of opposing forces across the area of responsibility. Components of the network-enabled ISTAR system include sensor platforms (i.e. satellites, fixed and rotary wing, manned and unmanned aircraft, ground and sea-based sensors), their associated ground and exploitation workstations, as well as network-enabled remote workstations and Command and Control Information Systems (C2IS) that are not directly associated with an ISTAR system or sensor.[3] A weapon fully integrated in this network-enabled ISTAR system is able to acquire and engage fixed and moving targets at long ranges.

2. Operations in a Global Positioning System (GPS) Jammed Environment

Military uses of GPS include navigation and timing applications; therefore, interference in the GPS frequency bands makes them particularly vulnerable. Without a high-quality GPS signal, network-centric systems establish communication nodes linking NEWs with



the most accurate information available by the most timely and accurate source available without being limited to the delivery platform or GPS signal.[4]

3. Battle Damage Assessment (BDA)

Most of the time, initial BDA reports must rely on visual observation of the target and are usually based on a single source.[5] With weapons fully integrated into the network, the BDA is based on data provided through a combination of weapons system video, aircraft cockpit video, and varied visual and electronic reports from multiple other sensors, all in real time. This information will be relayed to the Joint Force Air Component (JFAC) to be incorporated in their overall assessment. It would not necessarily inform re-attack options, but an assumption of success, having confirmed a hit on the target as planned, would remain until follow on BDA reporting confirmed the outcome.

4. Advancements in Weaponry

Advancements in weaponry are not necessarily limited to being network enabled. Future weapons also fall into the bracket of hypersonic capabilities. While much of this is still under development, allied forces also have the ability to influence additional features of these weapons. Since modern day adversaries have layered and formidable defensive postures, it is reasonable to expect that stand-off weaponry is the

foremost capability under development. Stand-off weaponry, developed to be sensor nodes by themselves with programmable loiter time for network-enabled programme changes as well as EO/IR capability for Positive Identification (PID) and BDA, will provide a significant advantage.

5. Shortening the Kill Chain

The advent of advanced weaponry forces us to revisit the targeting cycle's standing procedures to shorten the 'kill chain', i.e. to do it better or quicker. This will aid our commanders in defeating the enemy before they can react and counter our actions, thus enacting battlefield superiority, which is achieved by entering their OODA (Observe, Orient, Decide, Act) loop. The shortening of a procedure that currently works well and is already efficient may include, for example, delegation of engagement authority to lower levels or trusting sensors to ensure PID, CDE (Collateral Damage Estimation), as opposed to human visual acuity.

Weaknesses

1. Bandwidth and Net Design

Bandwidth is the primary driver of a network's speed. Unavailable or limited connectivity due to low or unstable bandwidth results in a slower exchange of information, thus failing to reach the required Information Superiority and impacting weapons' engagement. The closer the NEW is to the target area, the less available and reliable the bandwidth. Data prioritization is required to send only the essential data at the correct phase of the mission and reduce load on the network.

2. Ethics and Legal Aspects

The legal aspects of weapons employment is of paramount importance. They define the means by which we conduct ourselves and are accountable for our actions. It is not an argument whether a military force can kill people; it is legally doing so for military advantage that is proportional, distinctive, necessary and with regard for human life. Whenever we delegate responsibility, we must ensure that the legal aspects that define the way we operate are met. The delegation of PID to sensors is a perfect example, but if debated and accepted as meeting our principles, it will considerably shorten the ability to meet the approval criteria to strike the enemy.

3. Operational Procedures

Considering the multiple options that NEWs offer, the sharing or allocation of responsibility among stakeholders will have to be reviewed and updated, acknowledging all associated risks and consequences. Updated or new terminology will be required to be clear on how delegated engagement authority is disseminated for dynamic targets during post-launch execution. Joint Targeting is a process to engage the right target with the right weapon, but ammunition redirection requires a new framework for strategic decision-making.

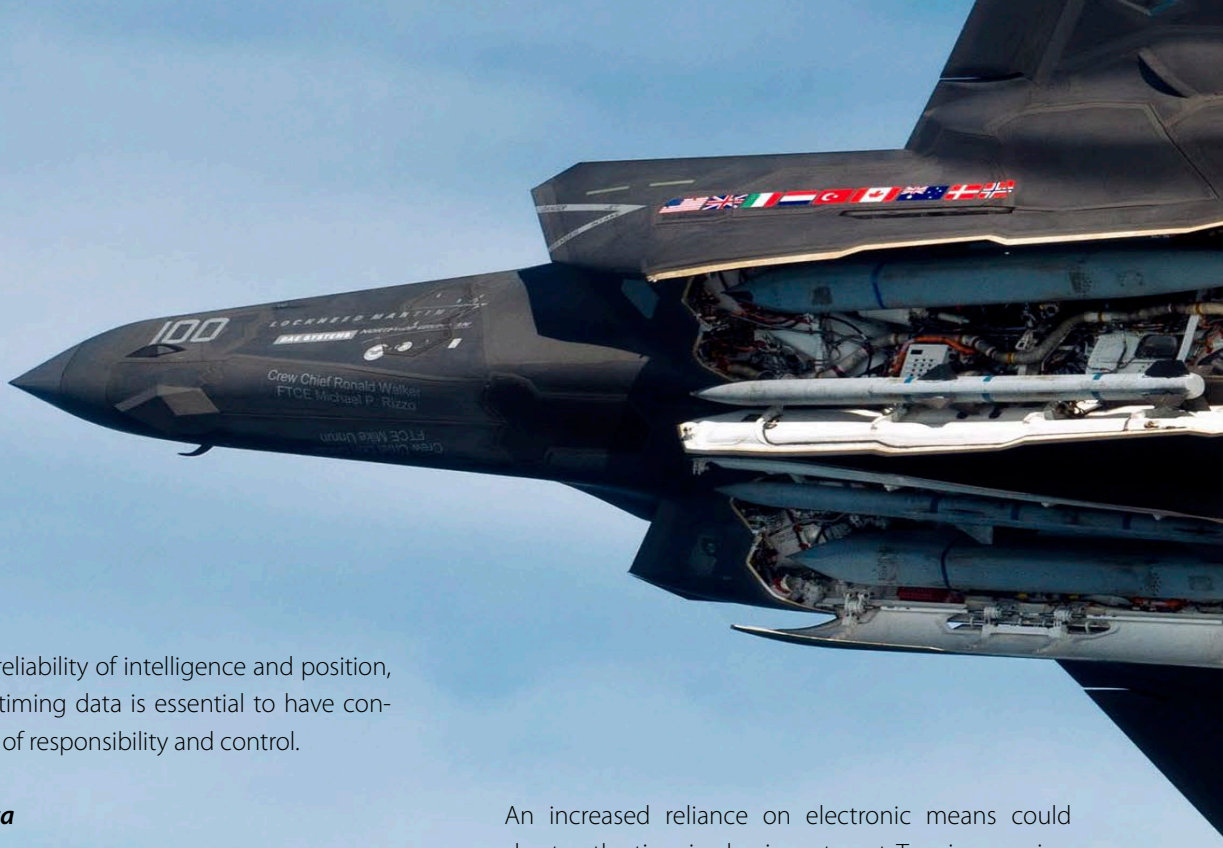
4. Overlapping C2 and Effective Engagement Aspects

One clear aspect of modern weaponry is that it is under the ownership and control of specific groups. Whether it is a component weapon (e.g. ATACMS) or a national-owned weapon used within a coalition (e.g. TLAM), there is always the threat of loss of control over the assigned weapons. The disposition to forego weapon ownership, for the greater good of quickly striking the enemy with the best available asset, is a difficult threshold to overcome. Identifying where the weapon employment decision-making and control delegation sits will be key.

5. Methodology

A speeding up of the targeting process is not necessarily where the benefits would lie, as opposed to speeding up CDE approval, faster transmission of mission details, or delegation of engagement authority based on Situational Awareness. The Find, Fix, Track, Target, Engage, Assess (F2T2EA) targeting cycle should not be disrupted as such, as it is a proven set of repeatable processes to legally prosecute a target.

What will enable an enhanced methodology are connectivity developments, particularly regarding handover phases, authentication, and engagement authority



delegation. The reliability of intelligence and position, navigation, and timing data is essential to have consistent transition of responsibility and control.

6. Weapons Data

Releasability of weapons data that are covered by National Security Regulations may limit the inclusion of specific capabilities allocated to NATO within future modelling and simulation activities, exercises, research and development, etc. Sharing national sensitive information, e.g. weapon ranges for planning purposes, is challenging in the best of times. There will need to be an agreed means of working these issues within the coalition.

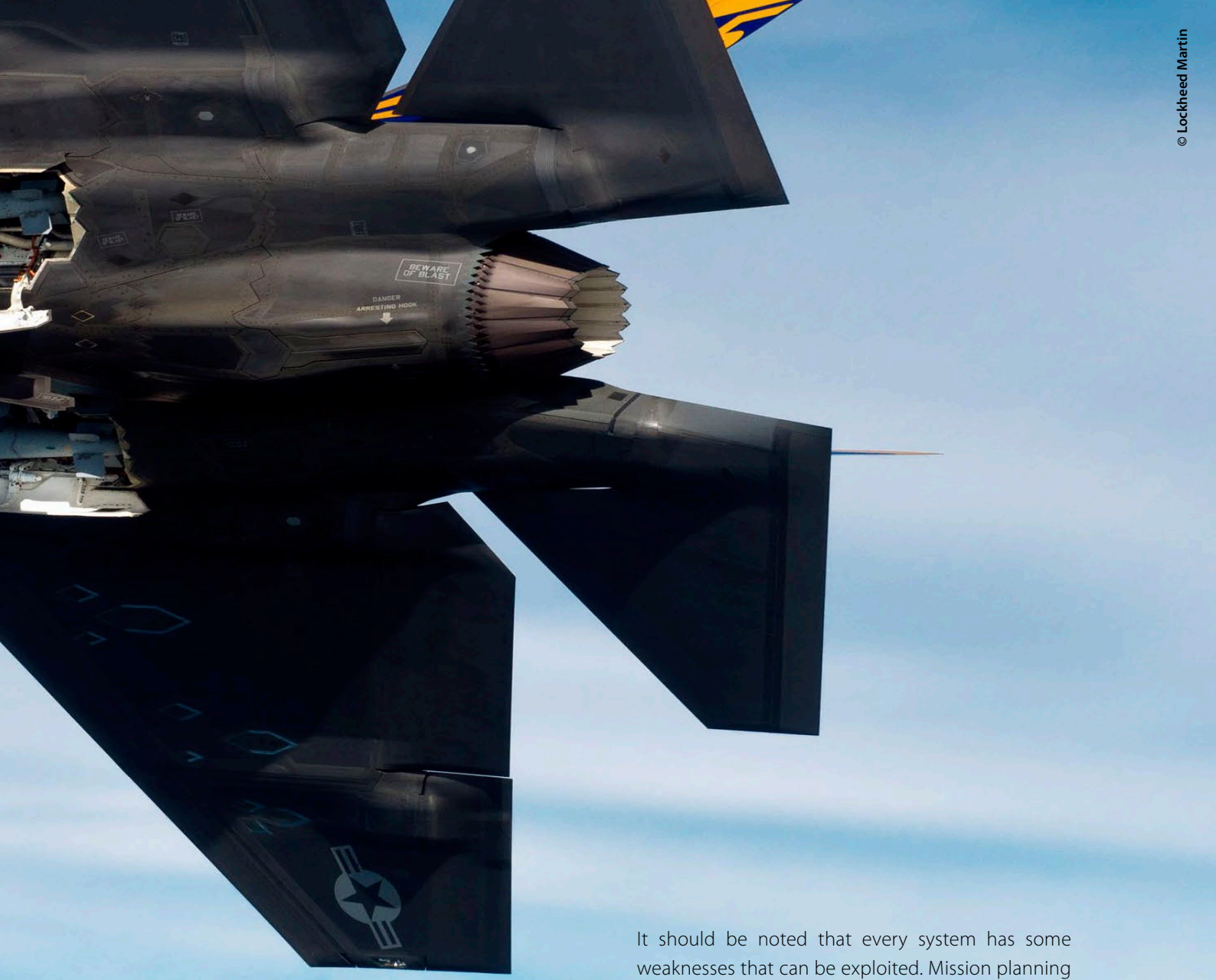
Future Targeting Cycles

Deliberate or dynamic, the targeting cycle can be very different and must be approached separately. The targeting cycle describes the deliberate means of allocating weapons to task for fixed structures that are planned through a cycle within the JFAC. This encompasses target development and authorizing of targets, with prioritization and execution to meet the commander's intent.

The same applies for dynamic targets, although they are mobile by nature and cannot be guaranteed to be struck through the normal cycle. The clearance of a dynamic target goes through a similar cycle to ensure all authorizations for legal, military, planning, etc. are met.

The challenge is how to improve both systems, without compromising procedures or legal obligations. An increased reliance on electronic means could shorten the time in clearing a target. Terrain mapping is not new, nor is the electronic capture of imagery. A visual clearance for all strikes, not necessarily for PID, but for CDE purposes is the norm. Should electronic means become acceptable to recognize change to imagery and clear a target for CDE purposes, then the potential to carry out a strike without waiting for visual confirmation could significantly shorten the time to strike. This would only be applicable to fixed targets.

Stand-off weaponry is becoming more common coupled with the problem of visual confirmation. Dynamic targeting is traditionally a rapid process to acquire a target and ensure it is legal, authorized, and tasked without compromising other priority tasking. Making it quicker is not necessarily better; however, with the development of NEWs, the ability to fire and forget from a stand-off position and then hand over programmed tasking of the weapon to another aircraft or ground unit is now under development. This will require a change in procedures for rapid planning to launch of a stand-off weapon and hand over the programming of the coordinates, enabling in place requirements to be more easily acted upon, e.g. a visual CDE clearance from a team with eyes on target, which afterwards conducts the appropriate programming. This would mean utilizing the best available weapon, from an increased arsenal, considering that many modern weapon systems would not be selected due to risk to aircraft or aircrews while establishing those visual confirmations.



Vulnerabilities and Mitigations

The risk of vulnerabilities is extensive, especially considering the connectivity links needed by the NEWs. Sophisticated electronic attack and cyber warfare highlight NEWs' vulnerabilities associated with the increased system connectivity, from which 'stand-alone' weapons were essentially impervious.

Sensors/seekers could be susceptible to electronic attack, which could affect the weapon by feeding insufficient data and reducing effectiveness. Consequently, a network's vulnerability could lead to a complete loss of its services from jamming or from a lethal attack, data corruption from a cyber-attack, or increased latency which affects guidance, navigation, and control of weapons in flight.

It should be noted that every system has some weaknesses that can be exploited. Mission planning and logistical chain protection must be secured, so that NEWs vulnerabilities to cyber-attacks are mitigated from corrupted environments. Additionally, appropriate electronic protection measures are paramount to ensure maintenance of sensor and seeker data. Hardening of locations and protection of access points with encrypted software are potential protection solutions against electronic attacks, together with the creation of new algorithms and systems redundancies to counter attacks and protect them from latency.

Recommendations

- Robust joint investment in networked communications through partnerships with coalition members will ensure commonality and connectivity for future joint operations.

- The immediate challenge for a new C2 structure is a reliable, secure, and affordable communications system within a modern military construct. Investment in these areas will be paramount, especially for contested and forward deployed locations.

- Whilst mentioned only briefly, a new concept for C2 structures and target methodology implies a review of current Tactics, Techniques, and Procedures (TTPs), Standing Operating Procedures (SOPs) and doctrines to accept NEWs as normal.

- Establish a framework for strategic decision-making as part of the Joint Targeting process and, more specifically, on the delegation of authorities as part of the targeting cycle.

- NATO Defence Planning Process is invited to consider these issues in projecting future procurement, specifically with the integrated ISR technology on future NEWs.

Conclusion

Advancements in technology are a coming of age in modern warfare, where we are seeing a generational leap in connectivity, data management, and C2 challenges. The ability to master these challenges before our peers will define our future military advantages. This is a crossroads of major changes to modern warfighting when network enabling will become the new norm. As a coalition, there is a profound need to be on the same path of modernization where new partnerships in agile procurement and research in this field are a must. ●

1. 'Information Operations', United States Joint Publication 3-13, 2014. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf (accessed 5 April 2022).
2. Kahn, M., 'Integrated Joint All-Domain Operations Collaboration Strategy', Lockheed Martin, 2020.
3. 'Coalition Interoperable ISTAR system concept of employment', NC3A, 2007.
4. Koudelka, B., 'Network-enabled Precision Guided Munitions', 2005.
5. Joint Targeting School Student Guide, Dam Neck, VA: Joint Targeting School, 2017. https://www.jcs.mil/Portals/36/Documents/Doctrine/training/jts/jts_studentguide.pdf?ver=2017-12-29-171316-067 (accessed 27 January 2022).

Lieutenant Colonel Francesco Esposito

joined the Italian Air Force in 1990. He was trained with the US Air Force SUNT programme at Randolph AFB, Texas, and in 1996 graduated as a Tornado Navigator/Weapon System Operator in Cottesmore, UK. As an aircrew with 156° Tornado Sqn and as an instructor with 102° Tornado OCU Sqn he participated in the flying operations in Bosnia and Kosovo. Between 2008 and 2012, he served as ATO Coordinator and Chief Strike cell in the Combined Air Operation Centre in Uedem, Germany, contributing also to the Operation Unified Protector in Libya. Currently, he serves as JAPCC Precision-Guided Munition Expert.

Mr Adam T. Jux

is a retired Royal Air Force Officer who also served in the Royal Australian Air Force and the Australian Army over his 27 years of military experience. He is a qualified targeteer and has worked in the discipline for the last 14 years, including on operations. He has instructed in targeting, collateral damage estimation and has mentored targeting at the Joint and Component levels. He has published a number of articles and contributed to white paper research regarding targeting in general and its interaction with intelligence and other disciplines. He is currently working as a civilian targeting consultant for NATO's Joint Warfare Centre in Stavanger, Norway under contract for CALIAN EUROPE AS.