Volume No. 2 | November 2023

IAMD CoE's ANNUAL JOURNAL

Integrated Air and Missile Defence: A valuable pillar in NATO's Deterrence and Defence.

LETTER FROM THE DIRECTOR

Dear reader,

As Director of the Integrated Air & Missile Defence Centre of Excellence, it is a great pleasure and privilege to present to you all the 2nd Annual IAMD COE Journal.

After gaining valuable experience from our first two conferences, the boost from the latest joined of France, as a sponsor Nation, and the successful Periodic Assessment from ACT/CPD, I strongly believe that this Journal will also have the same success as the previous one and would be beneficial for the whole Integrated Air & Missile Defence community.

The Centre has managed to develop skills in all important fields of IAMD, with an active role and dedication to its mission, and to provide training and best practices, doctrines, analysis, and lessons learned in the demanding IAMD Domain.

This comes together with our motto "Act Knowing'', a phrase of Pittacus (640 -568 b.C), a Mytilenean General and one of the seven wise men of ancient Greece, which means to be fully aware of the situation before acting.

This effort is continuing in our second Journal named:

'' Integrated Air and Missile Defence: a valuable pillar in NATO's Deterrence and Defence''

Within the aforementioned document, we intend to draw a picture of the current Geostrategic Military Situation for Euro-Atlantic Partners. This will lead us to describe the new era of Threats for the Euro Atlantic area, focusing mainly on Hypersonic Weapons and Remotely Piloted Aircraft Systems (RPAS) developments, the way NATO will meet today's and tomorrow's IAMD challenges, and how training, modeling, and simulation could support deterrence and defence from an IAMD perspective.

It is commonly agreed that sharing of knowledge and experience among specialists in IAMD enhances Air and Missile Defense operations by building common understanding and that is what we are focused on.

Sharing knowledge with our distinguished authors, their capacity, and expertise is valuable to all of us.

Sincerely,

Brig. General (OF-6)
Nikolaos KOKKONIS GRC (AF)
IAMD COE DIRECTOR

Table of Contents

NATO IAMD Role in the Overall Deterrence & Defence

By Mr. Bogusz Madej

INTRO

The security paradigm we're living in is shifting dramatically. There is number of unknowns that makes it hard to predict where this change will take us. Results of the war in Ukraine and developments in the Indo-Pacific in the light of the rising China are some of the most prominent among them. I will try to describe how NATO is answering to this new reality in terms of adaptation of the deterrence and defence posture, including NATO Integrated Air and Missile Defence (IAMD).

To this end, first, I would like to focus on the major milestones and steps taken so far to adapt NATO's deterrence and defence posture, main decisions have been taken at the Summit in Vilnius, and the most pressing and probable next steps that should be taken to complete the adaptation. In the second part, I will briefly account for the role played by the NATO IAMD in this adaptation.

Together, it should provide us with a good background and introduction to fruitful discussions. However, before doing that, to set the scene, please let me say few words about the security environment we are operating in.

SECURITY ENVIRONMENT

NATO's Strategic Concept, which was adopted last year in Madrid states that the security environment has deteriorated significantly and the Euro-Atlantic area is no longer at peace. The Strategic Concept further underlines that Russia is the most significant and direct threat to the Allies' security and to the peace and stability in the Euro-Atlantic area, while terrorism, in all its forms and manifestations, is the most direct asymmetric threat to the security of our citizens and to the international peace and prosperity.

Beside these two directs threats, NATO also recognizes and addresses challenges posed by other actors. We especially continue to monitor rising China in the context of the overall strategic situation in the Indo-Pacific region and its growing military cooperation with Russia. In the longer-run, Chinese military build-up, including in the nuclear and air and missile domain, may create significant challenges for individual Allies and the Alliance as a whole. Other countries requiring our particular attention are Iran and DPRK. Their continuous military build-up and aggressive rhetoric, aimed at challenging the current rules based order, create potential threats to the Euro-Atlantic security.

Finally, the Alliance continues to assess challenges and opportunities stemming from emerging technologies. For our community, hypersonic weapons are of course the most relevant, especially in the context of Russian and Chinese capabilities. Nevertheless, we must not ignore developments in other spheres, especially AI and quantum technologies. In the longer-run, they may have significant implications on our

deterrence and defence, including air and missile defence.

It all adds up to a highly complex and unpredictable environment, with multiple stakeholders and interconnected issues. Still, please let me zoom in on Russia, and make few quick points on it.

First, we must remember that Russian irresponsible, aggressive and escalatory behavior and rhetoric started way before the last year's full-scale aggression against Ukraine. Attack on Georgia, annexation of Crimea, occupation of large parts of Donbas and Lugansk Oblasts, and the breach of the INF treaty, together with the continuous military build-up, also in the air and missile domain, are only some, prominent examples of that behavior. Russian military integration with Minsk, including the planned deployment of Russian tactical nuclear weapons in Belarus, must also be closely assessed. It provides Moscow with additional military options and create new strategic dilemmas for us.

Second, we must not get complacent with our adaptation efforts in light of Russian failures in Ukraine and its shrinking resources, including missile arsenals. Instead, we should assume that, on the one hand, Moscow will draw lessons from these failures and adapt, and on the other hand, that it will rebuild its potential, also thanks to the international support.

It leads me to my third point, the need to pay close attention to the growing military cooperation between Russia and China and Iran, also in the air and missile domain. If continued, it can lead to even more complex, unpredictable and dangerous security environment.

Fourth, we should be more active in our outreach to the Global South to counter Russian and Chinese propaganda, and to ensure that our message is well heard and understood. To that end, we should enhance cooperation with our partners, including the EU, and strive to use all possible instruments and international forums to convey our message.

Fifth and final, although the war is probably far from being over, we should already think about future relations with Ukraine. Ukrainian role in the Western community should be defined. Kiev expressed its European and Euro-Atlantic ambitions, we must respond to them in one way or another. Some decisions in this regard are expected to be taken in Vilnius. However, we should assume it will be a long-term process.

ADAPTATION OF THE DETERRENCE AND DEFENSE POSTURE

With this picture in mind, please let me now turn to the adaptation of the Alliance's deterrence and defence posture. I will not be try to give you a full history. Instead, I will pinpoint the major milestones and key principles in this regard.

First of all, adaptation is a continuous and long-term process. Throughout its history, NATO adapted successfully to changing security paradigms. The most prominent examples of that are: the post-Cold War reality, when NATO needed to find its way in the world without the second superpower, and the post 9/11, when the Alliance faced terrorist threats and needed to focus on the out-of-area operations. An adaptation is also happening now.

Second, the current adaptation did not start on 24th February 2022, but at least as early as in 2014. Yes, last year's Russian

aggression on Ukraine accelerated some processes, and probably made some Allies to do more than some initially expected, but the whole process hasn't started then. The first war in Ukraine was the real wake-up call. Since then, Allies realized that Russia may or actually is posing a real threat, which needs to be addressed.

The next major step was taken during the Summit in Wales in 2014, when Allies enhanced readiness of forces, mainly through the Readiness Action Plan. It included establishment of Very High Readiness Joint Task Force and commitment to increase defence spending through the new Defence Investment Pledge.

Following that, during the Summit in Warsaw in 2016, Allies announced the decision on enhancing deterrence and defence on the Eastern and South-Eastern flank to signal unity, solidarity and resolve. To that end, four battle groups (BGs), in Baltic States and Poland, were established and military presence in the Black Sea region was increased. Allies also agreed to deliver "heavier, high end forces, at higher readiness". Decisions taken in Warsaw represented the biggest reinforcement of the Alliance's collective defence in a generation.

The adoption of NATO's Military Strategy in 2019, followed by the Concept for Deterrence and Defence of the Euro-Atlantic Area (DDA) and NATO Warfighting Capstone Concept (NWCC) in 2021, constituted another major milestones. It enabled development of the new planning construct for deterrence and defence for the whole spectrum of peacetime, crisis and conflict.

I will focus on the DDA and its family of plans. In short, DDA and its family of plans should enable to cohere deterrence activities in peacetime, enable swift transition to crisis and conflict, and allow for efficient deterrence and defence in crisis and conflict against both main threats. DDA will be implemented though a set of new, domain-specific and region-specific plans, especially in crisis and conflict. Together, this family of plans should enable active management of posture, i.e. thanks to a multi-domain and multi-functional integration across the AOR. These plans will build on the enhanced Allied presence and vigilance activities on the Eastern and South-Eastern flank. It includes measures introduced in response to the 2022 Russian attack on Ukraine, in particular:

- significant increase of land, air and maritime presence throughout the whole Eastern and South-Eastern flank, including deployment of SBAMD units and further enhancement of the Air Policing mission;
- establishment of four additional BGs in Bulgaria, Romania, Slovakia and Hungary, doubling the size of Allied deployed troops on the Eastern flank;
- commitment to enhance the BGs from battalions up to brigade size, where and when required;
- agreement that the current posture on the Eastern and South Eastern flank, also in the air and missile defence, should become the new baseline, continuing the move from the tripwire defence concept to forward defence.

This year the whole DDA family of plans should be in place. However, in order to ensure executability of these plans and complete this major step in modernization of our collective defence, they should be supported by:

- forces, with an appropriate level of readiness, with proper balance between homeland defence, in-place forces and reinforcements;

- efficient command and control, maximizing the use of existing NATO's and national structures, together with efficient alert and response system, allowing for timely decision-making, with appropriate level of political control;

- enablement, including IAMD and long-fires, together with efficient and sustainable logistics, also in terms of pre-positioning of equipment and ensuring swift movement of forces across the whole area of responsibility (AOR).

It all should be underpinned by robust training and exercises, to demonstrate our resolve (for both deterrence and reassurance), but also ensure interoperability of our forces. Exercises should also help in further refinement of plans. Allies should also strive to cohere their national exercise activities with DDA in peacetime and offer sufficient visibility of such activities to NATO, and SACEUR is particular. It should allow for more efficient use of resources and STRATCOM.

Finally, to ensure the posture is sustainable in the long-run, it must be properly resourced. To that end, Allies are considering a new Defence Investment Pledge, potentially with 2% of GDP spending as the floor, not the ceiling, and more efficient ways of using common funding.

By the way of spending, another significant questions ahead of us are:

- how to balance our support to Ukraine, with the necessity to replenish our stocks and ensure sustainability of our posture, and in general how to establish and sustain the industrial base responding to the current needs;

- what should be the right balance between developing "numbers" and maintaining technological edge (the war in Ukraine proved that quantity, not only quality, matters);

- are our decision-making processes adequate to the current security environment, and what should be the right balance between the political control and the military responsiveness?

Last, but definitely not least, last year in Madrid, Allies adopted the new Strategic Concept. The Concept highlights that the security environment has deteriorated significantly, with Russia and terrorist groups as the main threats to the Alliance. This clear reference to Russia and terrorist groups marks a significant change comparing to the 2010 Concept. Moreover, the Concept reaffirms that NATO's key purpose is to ensure collective defence of its members, based on a 360-degree approach. To this end, deterrence and defence posture needs to be further strengthened. Furthermore, the document reaffirms that deterrence and defence is based on forward defence and credible reinforcement, but that the balance must be changed towards the former. The Concept also recalls the three essential core tasks of the Alliance – deterrence and defence, crisis prevention and management, as well as cooperative security.

As a final addition, please let me stress that simultaneously to this adaptation on the conventional side, Allies continue to adapt NATO's nuclear deterrence. The Strategic Concept reaffirms the key role of nuclear deterrence, as an element of appropriate mix of conventional, nuclear and missile

defence capabilities, complemented by cyber and space capabilities. Addition of space and cyber capabilities to "the mix" is another significant change, comparing to the 2010 Concept. Efforts concerning NATO's nuclear deterrence are focused on ensuring its long-term credibility, effectiveness, safety and security, as well as "enhancing nuclear IQ" on all levels of decision-making. Allies also strive to enhance coherence between nuclear and conventional deterrence, while maintaining unique and distinct role of nuclear deterrence.

Role of IAMD in the adaptation of NATO's Deterrence and Defence posture

Moving to NATO IAMD, again please let me highlight only few brief points, as a lot more will be said later today and tomorrow.

First, from the outset, NATO IAMD was considered as a part of adaptation of the Alliance's deterrence and defence posture.

Second, the real wake-up call for Allies in the air and missile domain was the breach of the INF treaty by Russia and the development of SSC-8. It resulted in the recognition of the so-called whole suite of Russian missiles as s potential threat to the Alliance. Consequently, as a part of a broader response, Allies decided to answer to this threat by enhancing readiness and responsiveness of NATO IAMD, to ensure the right capabilities, at the right place, at the right time. These were mainly peacetime measures, aimed at enabling seamless transition to crisis and conflict. Moreover, in 2021, in the Brussel's Summit Communique, Allies publicly acknowledged, for the first time in years, importance of NATO IAMD in the context of potential threats posed by Russian air and missile capabilities.

Third, this adaptation is ongoing as we speak. I have already mentioned that steps taken by NATO and individual Allies in direct response to the 2022 Russian aggression against Ukraine included deployment of SBAMD units on the Eastern flank and enhancing of Air Policing. Allies are also exploring ways of enhancing its peacetime air and missile defence posture on the Eastern flank, though rotational deployments for training purposes. It should enhance responsiveness and interoperability of our forces. Beyond that, we continue adaptation of our plans, including the IAMD Standing Defence Plan, to ensure proper integration of NATO IAMD within the DDA family of plans.

Moreover, Allies continue development of IAMD capabilities. Over the last few years a significant number of Allies acquired or announced plans to develop or acquire IAMD capabilities. Commitments in this regard were recently confirmed i.a. in the Political Guidance for the next cycle of the NATO Defence Planning Process. On top of that, we also continue implementation of the commonly funded air command and control system and prepare the future of air command and control. In the context of capabilities' development, it is important to remember about the necessity of striking the right balance between offensive and defensive capabilities, such as IAMD and deep-precision strike. For years, many Allies were reluctant to develop some offensive capabilities, and to talk about it, basing it on the principle of NATO being a defensive Alliance or because of the sensitivity of such capabilities.

Forth, following the 360-degrees approach to NATO IAMD, we also respond or monitor other actual and potential threats and challenges in air and missile domain. NATO BMD is operational and soon it will be expanded with the second Aegis Ashore site in Poland. With that, full coverage of NATO Europe against ballistic missile threats emanating from outside the Euro-Atlantic area will be ensured. NATO BMD is still relevant given the continuous proliferation of ballistic missiles, especially the growing arsenal of Iranian ballistic missiles. Enhanced Russian-Iranian defence cooperation further amplifies this threat. We cannot exclude a scenario that in time of crisis or conflict between NATO and Russia, Iran will threaten to target our critical infrastructure with its ballistic missiles. In the NATO BMD context, we are also exploring ways of ensuring greater coherence between missions conducted under NATO IAMD. Eventually, it should increase missions' effectiveness and allow for better use of available resources.

Moreover, we closely monitor potential air and missile threats posed by other state and non-state actors, especially China and DPRK. We assess that currently neither of them poses a direct threat to the Alliance. However, their ongoing nuclear and missile programs, including hypersonic, are of concern, also in terms of the broader security challenges in the Indo-Pacific.

We are also looking at other air breathing threats, especially UAVs and loitering munition, from both politico-military and capabilities' development perspective. Initially, these threats were considered in a hybrid, terrorist scenario. The war against Ukraine proved, however, that we should also include them in the crisis and conflict scenarios against state actors, including Russia.

To conclude, please let me stress that although during the Summit in Vilnius some important decisions were taken on enhancing our deterrence and defence, it was just another milestone, not the end of our journey.

Further steps will still need to be taken, especially in terms of ensuring:

- executability of plans and that they are properly translated to the tactical level;
- assignment of forces, at appropriate level of readiness, and enablement;
- coherence between nuclear and conventional deterrence;
- efficient decision-making, with a balance between political control and military effectiveness;
- proper STRATCOM concerning our main activities.

With regard to NATO IAMD, the further adaptation should especially cover refinement of policies and plans, capabilities development, including command and control, as well as training and exercises.

Before I finish, I would like to leave you with few points on NATO IAMD, I believe we should consider in the context of further adaptation.

First, what would be the appropriate IAMD posture on the Eastern and South-Eastern flank, and how to ensure its long-term sustainability?

Second, how should we demonstrate this posture, for deterrence and reassurance purposes?

Third, how should we define the "appropriate mix" of conventional, nuclear and missile defence capabilities, especially missile defence role therein, and how to strike balance between offensive and defensive capabilities?

Forth, how to balance the 360-approach with the need to enhance deterrence and defence of the Eastern and South-Eastern flank, given the persistent lack of IAMD capabilities? •

Geostrategic Military Situation for Euro-Atlantic Partners

By Dr. Kostantinos IFANTIS

The presentation attempts to sketch out the day after the war in Ukraine is over by addressing three issues. First, to what extent has the war resulted in broad shifts when it comes to the European and global economic, political, and military power distribution. Second, what are the vulnerabilities and shortcomings the war has exposed in the unity and strategic coherence of the transatlantic community and to what extent have they been overcome. Finally, can we imagine the post-war global order, and what are its main strategic features and policy challenges. •

The Russian Military Strategy in Ukraine and IAMD Lessons

By Dr Emmanuel KARAGIANNIS

Dr Emmanuel Karagiannis is a Reader in International Security at King's College London's Department of Defence Studies.

Introduction

Following the overthrow of Russian-leaning President Viktor Yanukovych in February 2014, Russia occupied Crimea and organized a referendum for its annexation. In April 2014, the Ukrainian army clashed with pro-Kremlin separatists in the Russian-speaking region of Donbass. The fighting continued throughout the summer of 2014. On September 5, representatives from Russia, Ukraine, and the self-declared People's Republics of Donetsk and Luhansk signed the Minsk Protocol, establishing a ceasefire. For eight years, Donbass became another frozen conflict with occasional skirmishes.

In July 2022, relations between Russia and Ukraine escalated dramatically. Putin published an essay titled 'On the Historical Unity of Russians and Ukrainians,' claiming that the Ukrainian nation did not exist because Ukrainians were part of a triune Russian nation (*triedinyi Russkii narod)* along with Russians and Belarusians (Putin, 2021). The Russian leader embraced a pseudo-historical narrative to construct the geo-identity of a greater Russian nation. The Kremlin presented itself as the savior of Russian speakers, supposedly facing discrimination and hostility. Meanwhile, it portrayed the Ukrainian government as a 'nationalist, neo-Nazi regime' that seized power by force in 2014 before instigating conflict in Donbass' (Tass Russian News Agency, 2022). The Russian invasion of Ukraine started on 24 February 2023. After more than a year of war, it is possible to assess the Russian military strategy in the country and draw valuable lessons for the future.

The Russian military strategy

The Kremlin initially applied the art of deception (*maskirovka*) at the strategic level, claiming that it was not going to attack Ukraine (Keating, 1981). For several months, Russian officials fiercely dismissed reports by Western intelligence agencies openly predicting an invasion. Operationally, the invasion began with an advance of motorized troops that attacked from three directions simultaneously: north, east and south. The Russian Air Force destroyed critical infrastructure (e.g., power stations) to plunge the country into chaos. In addition, the Black Sea fleet blockaded Ukrainian ports to stop any supplies from third countries. At the tactical level, Russian special forces attempted to create bridgeheads by seizing airports and carrying out acts of sabotage within cities. In effect, the Kremlin launched a blitzkrieg against Ukraine.

The strong resistance of the Ukrainians caught the Kremlin by surprise. Moscow underestimated the Ukrainian military doctrine, which calls for the mass mobilization of the population in the event of a foreign invasion. The Ukrainian leadership initially moved the war into and around populated areas, where the defender has the tactical advantage. Within the urban environment, small groups can easily set up ambushes and hit enemy targets with anti-tank missiles. In fact, urban warfare is the nightmare of all regular armies. The Ukrainian side was well aware that Moscow is still haunted by the "Grozny syndrome". The first war in Chechnya (1994-1996) resulted in a humiliating defeat for the Russian army. Small groups of determined fighters destroyed entire columns of Russian tanks that had entered the centre and suburbs of the Chechen capital.

Yet, the Russian forces was expected to overwhelm the Ukrainian positions within less than a week. Putin's battle-hardened army did enjoy numerical and technological superiority. Following the 2008 Georgian war, minister of defence Anatoly Serdyukov's military reforms changed the force structure of the Russian army. The creation of the battalion tactical group (BTG) was intended to increase the firepower and speed of the Russian forces. Indeed, each BTG has a motorized infantry battalion together with tank and artillery elements; a total of 600-800 officers and men. However, the main disadvantage of BTGs is the relatively small number of light infantry troops (around 200 men) which makes BTG vulnerable to ambushes. During the first three months of the invasion, the Russian BTGs became an easy target for the Ukrainian fighters.

Apparently, the Russian military were not prepared for such a large-scale invasion. Due to poor military planning, the Putin's army has failed to conduct combined arms operations. This should have come as no surprise. In the 2008 war against Georgia, the involvement of the Russian army was limited in time and geography. Yet, its performance was assessed by analysts as rather poor. Six years later, the annexation of Crimea took place with a hybrid and bloodless operation. In the Syrian civil war, the Kremlin has mainly used its air power, special forces, and mercenaries to support the Assad regime. In other words, it is the first time since the 1979 invasion of Afghanistan that the Russian military has been called upon to subdue a large country with a hostile population. It should be noted that there was an insurgency in western Ukraine after the end of the Second World War that lasted ten years.

During spring and summer 2022, the Russian military used indirect artillery fire and ballistic missiles to defeat the Ukrainians. This is not the first time in recent history that Moscow resorted to such tactics. During the Second Chechen war (2000-2002), the Kremlin bombed Grozny

to the ground without any concern for the international law of armed conflicts. The Russian leadership chose the same siege warfare in certain parts of Ukraine.

The siege of Mariupol began on 24 February 2022 and finished three months later. The city was erased to the ground due to Russian massive bombardment. According to the UN, up to 90 percent of residential buildings have damaged or destroyed and at least 350,000 people (around 70 percent of the pre-war population) were forced to leave the city (OHCHR, 2022). While estimates vary, it is clear that thousands of civilians were killed during the siege.

However, the invaders failed to capture Kyiv and Kharkiv, which are the two largest cities of Ukraine. According to Professor Louis DiMarco (2012) two factors could play a decisive role in attacking urban centres: the size of the population and the size of the area. The larger the population and the area, the more forces must be devoted to occupying a city. The American professor has challenged the 3:1 rule in favour of the attacker and advocated a 6:1 ratio for launching an attack in urban areas.

What has come, perhaps, as a surprise is the outsourcing of the Russian military operations to mercenaries. Since the summer of 2022, an unknown number of Russian and foreign mercenaries have joined the regular Russian army in fighting the Ukrainian army in Donbass. The partial "privatization" of the war is an innovation in itself. During the tsarist period, the army was under strict surveillance because officers were the only ones who could challenge the regime. In the Soviet era, the role of the political commissar was to enforce political control over the military through his presence at the strategic and operational levels. The use of private military companies, such as the infamous Wagner, runs counter to Russian military culture that prioritizes political control of the military. However, mass mobilization is neither desirable nor feasible in a middle-class country like Russia. The use of mercenaries allows Moscow to hide casualties from the Russian public opinion that does not massively support the war in Ukraine. The Wagner's force functions as a small army capable of operational and tactical support when is needed.

The war has entered a new phase since September 2022. The Ukrainian counter-offensive succeeded in recapturing territories in the southern and eastern parts of the country. Yet, the Russian forces managed to stop the Ukrainian offensive before Christmas. Currently, there is a stalemate on the eastern front because of the trench warfare. The Kremlin has mobilised human and material resources for a new Spring offensive in Donbass. Europe and the United States must do whatever is necessary to stop it before it begins.

The IAMD lessons

The Russian army has historically understood victory as the product of human spirit and psychology. Hence, material factors such as technology are not decisive for victory. In a way, this reflects the influence of Carl von Clausewitz on the Russian military thinking. The Prussian theorist, who served in the Russian army for two years, stressed the importance of "moral forces" (e.g., motivation, patriotism, will) in the final outcome of the war. Consequently, it has been argued that the "Russian view of modern warfare is based on the idea that the main battlespace is the mind" (Berzins, 2014, p. 5).

Since the beginning of the war, the Russian military has used short-range ballistic missiles, cruise missiles, and UAVs to defeat the Ukrainians. Although this is not the first time in recent history that Moscow resorted to such tactics (e.g., Second

Chechen war 2000-2002), the extent of the use of missiles is alarming. Russian missiles have targeted the country's critical energy infrastructure and population centres.

Moreover, the Russian armed forces have used extensively drones against Ukrainian targets. Simultaneously, the Ukrainian army has developed its own capabilities to counter the this Russian threat (see below).

While it is perhaps to early to draw conclusions about the utility of IAMD systems, a preliminary assessment could provide some important lessons for NATO and its members.

- IAMD systems must be acquired in sufficient quantity and be well dispersed before a conflict begins.
- Rather than shooting down individual missiles, it will be more effective to destroy launch sites, launchers, and associated equipment (e.g., radars)
- Protection of IAMD assets can include passive defences measures, such as shelters and Camouflage, Concealment and Deception. •

References

Adamsky, D., *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US and Israel* (Stanford: Stanford University Press, 2010)

Berzins, J., "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy", National Defense Academy of Latvia, Policy Paper no. 2, April 2014

Braw, E., "Russia's Conscription Conundrum: The Obstacles to Modernizing the Country's Armed Forces", *Foreign Affairs*, August 25, 2015, https://www.foreignaffairs.com/articles/russia-fsu/2015-08-25/russias-conscription-conundrum

DiMarco, L.A., Concrete Hell: Urban Warfare from Stalingrad to Iraq Essential Histories (Osprey, 2012)

Hsu, J., "Ambiguous Warfare Buys Upgrade Time for Russia's Military", *Scientific American*, August 12, 2014, http://www.scientificamerican.com/article/ambiguous-warfare-buys-upgrade-time-for-russia-s-military/

Jonsson, O. and R. Seely, "Russian Full-Spectrum Conflict: An Appraisal After Ukraine", *Journal of Slavic Military Studies*, vol. 28, no. 1, 2015

International Court of Justice, Press Release, 7 October 2022, https://www.icj-cij.org/public/files/case-related/182/182-20221007-PRE-01-00-EN.pdf

Glantz, D.M., *The Evolution of Soviet Operational Art, 1927-1991: The Documentary Basis* (London: Routledge, 1995)

Keating, H.C., *Maskirovka: The Soviet System of Camouflage*, US Army Russian Institute, June 1981

OHCHR, "High Commissioner updates the Human Rights Council on Mariupol, Ukraine", June 16, 2022, https://www.ohchr.org/en/statements/2022/06/high-commissioner-updates-human-rights-council-mariupol-ukraine

Putin, V., "On the Historical Unity of Russians and Ukrainians," July 12, 2021, http://en.kremlin.ru/events/president/news/66181.

TASS Russian News Agency, "Neo-Nazi Regime in Kiev Guilty for Donbass Tragedy, Putin Says," September 5, 2022, https://tass.com/politics/1502775.

The Rise of China and an Emerging Bipolarity

By Dr Harry PAPASOTIRIOU,
Professor of International Relations and Strategy, Panteion University and Chairman of the Scientific Board, Institute of In-

The rise of China has been meteoric. As the Table below shows, at the end of the twentieth century China had the seventh largest GDP (measured by current exchange rates). In the next ten years China overtook Italy, France, Britain, Germany and Japan. By 2014 China was well ahead of the third largest economy, Japan, and moving closer to the United States. The gap has narrowed since.

This development suggests that we have moved away from the unipolar moment of the 1990s and towards a new bipolarity. But it is an asymmetric bipolarity favoring the United States for the following reasons:

a) In the bilateral distribution of power, the United States remains the more powerful actor. Chinese GDP in recent years has no longer maintained high growth rates and seems unlikely to overtake that of the United States soon. Moreover, the United States in far ahead in military power. According to SIPRI, the United States in 2022 had 39% of global defense spending whereas China had only 13%.

b) The United Sates has impressive worldwide alliances, including NATO in Europe and Japan, South Korea, Taiwan, Australia and New Zealand in the Pacific. China has only North Korea and Russia. It could be argued that the Ukraine-Russia war is a proxy confrontation between the West and China whereby the West is weakening one of the two allies that China has.

c) The United States stands for appealing values such as liberty, democracy and the rule of law. Its alliances are not transactional but constitute communities with shared values. China seems to appeal to other states only in the sense of being antiliberal, rather than for any positive values it stands for. China and Iran have in common an antiliberal opposition to the West while having very different ideologies and values.

China has pursued its Belt and Road Initiative (BRI), including an ambitious set of developmental infrastructure projects, on account of its export-led growth policy, which resulted in the accumulation of vast foreign exchange reserves in need of being invested abroad, as well as its excess construction capacity that also needed to be deployed abroad. But its BRI initiatives are

	USA	Japan	Germany	UK	France	Italy	China
1999	9.660	4.432	2.196	1.558	1.500	1.171	1.089
2014	17.419	4.601	3.852	2.941	2.829	2.114	10.360
2021	23.315	4.941	4.260	3.131	2.958	2.108	17.734

GDP (current US$) | Data (worldbank.org)

transactional or even neocolonial (as in Shri Lanka) and have not fostered lasting alliances.

China was instrumental in creating BRICS in 2001, an economic formation that also includes Brazil, Russia, India and South Africa, which has sought to escape the rules of the Western liberal international economic order. But BRICS is not a geopolitical alliance. Indeed, its leading members (by GDP), China and India, are geopolitical rivals.

In Central Asia, Russia has accepted a co-dominion with China, particularly through the Shanghai Cooperation Organization. This was largely the result of Western policy that pushed Russia closer to China. The West before 2014 had two options regarding Russia and Ukraine.

The first option followed from the dictates of Realism. The top external priority of any state is to defend itself against the largest external threat. For the United States in 2013 that would be China. From an American perspective, Ukraine was insignificant for coping with the Chinese threat, or for any other significant national interest. Coming to an arrangement with Moscow, whereby Ukraine would remain in Russia's geopolitical sphere, might have kept Russia away from China's orbit.

The second option followed from the imperative of upholding the rules-based liberal international order that the United States promoted in the post-war era. Ukraine had a right to determine its external orientation and join the West. Any serious Russian retaliatory violations of international law at the expense of Ukraine should be punished, in order to send the message that the West takes the rules of the liberal international order very seriously. In this approach it would be hoped that China will be socialized into the rules-based liberal international order, so that even if it overtakes the United States in power factors, it will not be a strategic threat.

Note, that Great Britain faced the same dilemma regarding the Soviet Union in 1939-1940. Germany was Britain's main threat. But it was both Germany and the Soviet Union that conquered neighboring states. Punishing the Soviet Union would have pushed it into Germany's arms. In that case Realism prevailed over the imperatives of the liberal international order, because the German threat was very menacing and imminent.

Evidently the same was not the case for the United States in 2013-2014 regarding the potential Chinese threat. Pushing Putin's Russia into China's arms was an acceptable cost for Obama's United States, for the sake of upholding the liberal international order. And yet the Western measures against Russia for attacking Ukraine at that time were ineffective. Therefore, American policy resulted in the worst of all possible outcomes. There was no geopolitical deal on Ukraine to satisfy Russia's major national interests and keep it away from China. But the rules of the liberal international order were not really enforced in an effective way either. This led to Russia's miscalculation in 2022 that it could conquer all of Ukraine without serious opposition from the West.

The Ukraine War created a greater sense of unity and purpose in the West than had been witnessed in decades. It thus backfired disastrously on Russia, but also put China on notice not to dismiss the West as a declining force in contemporary world politics.

Nonetheless, the “global South” refused to follow the West in its sanctions against Russia. This means that we now see a trifurcation in global politics. One side is the revied West, united, purposeful and still the leading force in global politics. The second side is China with its few allies, the most important of which, Russia, is decisively weakened. The third side is the global south, which is not an alliance but a group of states that refuse to align themselves firmly with either of the leading blocs. •

The rising increase of importance of unmanned systems across defense lines of effort

By Dr Charles A. Rea, Deng

Intelligent Autonomous Systems are rapidly becoming a critical aspect of modern defense with the increasing prevalence of uncrewed aerial, ground, and maritime systems. Several factors are driving this trend, including the increasing complexity of warfare, the need to reduce risk to personnel, and the ability to conduct missions more efficiently and effectively. This presentation will examine the key drivers behind the rising importance of uncrewed systems, and the challenges / opportunities that arise from their use. •

Hybrid Threats – How they affect Integrated Air and Missile Defence (IAMD)

By Sozon A. LEVENTOPOULOS, MSc, PhD(c)

Introduction

As Heraclitus said almost 2.000 years ago, "War is the father of all and the king of all". For millennia wars were fought mainly on land or at sea, and even though great generals like Alexander the Great would embark on extensive and lengthy campaigns, it was Christopher Columbus' voyage and the subsequent maritime discoveries that led to a global military naval strategy of ocean control, known as "command of the sea". This concept entails that a naval force is so strong that could dominate its surrounding waters (green-water navy) and, in theory, extend far into the oceans (blue-water navy). This concept was dormant from the 16th to the early 20th centuries when the small and fragmented European states could control most of the world and its commerce.

On December 17, 1903, Flyer I, a heavier-than-air motor-operated airplane piloted by Orville Wright[1], made its maiden flight from Kill Devil Hills in North Carolina. A couple of years later (1905) a better – and more practical – model, the Wright Flyer III, was introduced. These pivotal events changed not only the way of travel but and how wars were conducted. Almost a decade later, airplanes found their way onto the battlefields, even before World War I[2]. Like its naval counterpart, the "command of the air" is mostly attributed to Giulio Douhet[3], was introduced. This military concept and strategy entail air superiority or dominance over a territory, where the friendly forces would freely "roam the skies", engaging at will enemy forces. Consequently, this strategy created its "alter ego" in the form of Integrated Air and Missile Defence.

Hybrid threats have emerged as complex and multifaceted challenges in today's interconnected world. Unlike traditional forms of aggression or conflict, hybrid threats combine a wide range of unconventional tactics, blending conventional and unconventional methods to achieve their objectives. These threats can originate from state actors, non-state actors, or a combination of both, making them highly adaptable and difficult to counter. With the increasing reliance on

[1] Orville (* August 19, 1871 - † January 30, 1948) and Wilbur (* April 16, 1867 - † May 30, 1912) Wright (aka "the Wright brothers") were American aviators, engineers and inventors which managed to invent, design, and build the first heavier-than-the-air flying machine (aka Flyer I) with which managed to make the first control flight with a fixed wing airplane.

[2] Reconnaissance missions were flown as early as 1911, with the first war naval co-operation mission taking place in 1913, by the Hellenic Naval Aviation.

[3] General Giulio Douhet (* May 30, 1869 - † February 15, 1930), was an Italian military officer and air power visionary and theorist. Most famous about his book "The Command of the Air"

technology and the interconnectedness of global systems, hybrid threats have the potential to disrupt societies, undermine institutions, and exploit vulnerabilities across various domains, including political, economic, social, and informational realms. Understanding and effectively responding to hybrid threats requires a comprehensive and integrated approach that encompasses diplomacy, military capabilities, intelligence gathering, cybersecurity, and resilience-building measures. As the nature of global security continues to evolve, addressing hybrid threats becomes imperative for nations seeking to safeguard their interests and maintain stability in an ever-changing landscape.

Terms and Definitions

- Cyberspace: For the purposes of this document, we are going to use Kuehl's definition, who defines cyberspace as:
  "A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies."

- War: The mechanism, method, or modality of armed conflict against an enemy**. In short it is "the how" of conducting war.**

- Warfare: An **intense armed conflict** between states, governments, societies, or paramilitary groups such as mercenaries, insurgents, and militias. **In that view, warfare constantly changes, while war remains the same.**

- Information security: Information security is what keeps valuable and sensitive information protected. Its main focus is the protection of the CIA (see figure below). It is not something you can buy (a process rather than a product), it is something you do (needs commitment) and involves people, processes, and technology. Information itself should be considered as an asset, therefore it has a value to the organization and should be protected, irrespective of the form it might take.

Figure 1 - The Confidentiality, Integrity, and Availability (CIA) Triad

- Cybersecurity: It is the art of protecting networks, devices, and data from unauthorized access or criminal use.

Against these new threats IAMD forces are not ready, trained or equipped to defend themselves and their assigned assets.

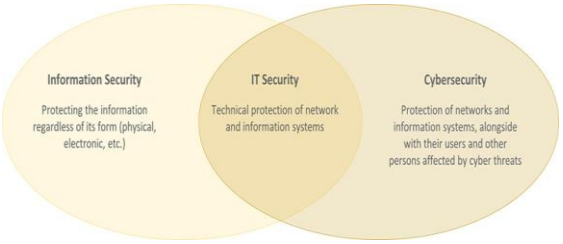


Figure 2 – Information Security, IT Security and Cybersecurity - How they interact.

Overview of the modern IAMD

Integrated Air and Missile Defense (IAMD) is an essential modern approach to strategic defense, bringing together multiple systems and technologies to detect, identify, track, and eliminate aerial and missile threats. The concept of IAMD hinges on the integration of various sensors, weapons, and command and control systems, providing a comprehensive and layered defense structure. The key advantage of IAMD is its ability to counter a wide range of threats, including aircraft, cruise missiles, ballistic missiles, and unmanned aerial systems, utilizing a network-centric warfare approach. The use of advanced radar and other sensor technologies allows for early threat detection and tracking, which is vital in allowing enough time to engage and destroy the incoming threat.

Recent advancements in IAMD technologies focus on improving the speed, accuracy, and reliability of these systems. Multi-domain operations, enabled by improvements in data fusion and AI algorithms, have become a central aspect of modern IAMD, allowing seamless integration and communication between land, sea, air, and space-based systems. Directed energy weapons, such as lasers and high-power microwaves, are also being explored as potential additions to the modern IAMD arsenal due to their potential for speed-of-light response times and lower cost per shot. Cybersecurity has likewise become a critical concern, given the interconnected nature of these systems and the potential for cyber-attacks to disrupt their operation. Finally, the development of hypersonic missiles by potential adversaries has led to an increased emphasis on hypersonic defense, which requires new (or upgraded) sensors and interceptors capable of detecting and tracking these incredibly fast and maneuverable threats.

We can summarize current IAMD characteristics and features in three main pillars:

- **multiple and diverse systems** ("system of systems" approach)
- **a layered approach** (which in turn, is supported by the "system of systems" approach)

- **integration and interoperability** (which supports the “system of systems” approach)

Figure 3 - A USAF F-105G Thunderchief aircraft, armed with AGM-45 and AGM-78 anti-radiation missiles.

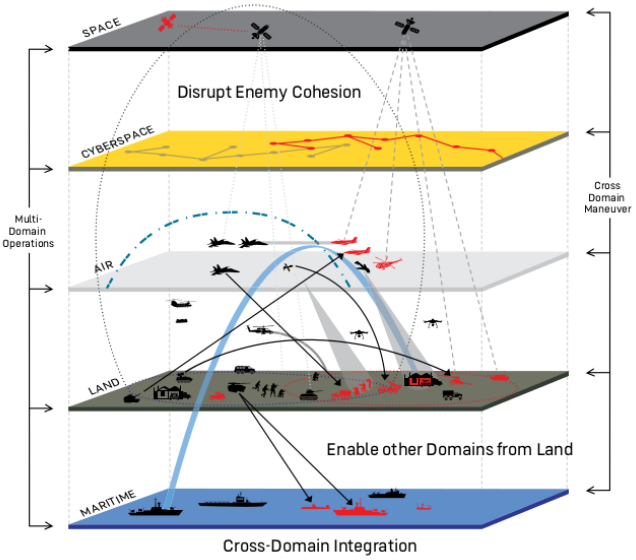


Figure 5 - All domain warfare (Source: Wikipedia - Public Domain)

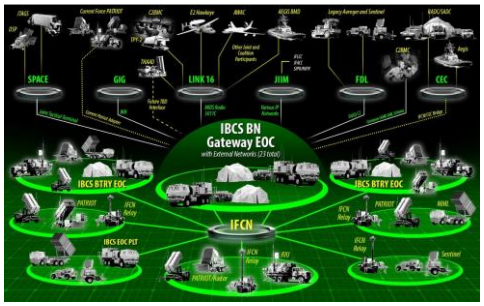


Figure 4 - An overview of a network-centric, extensive "system of systems" (source:

The common factor of the above-mentioned characteristics is that all of them rely on technology, namely computers, networks, and software/algorithms (AI is based on highly capable computers and extremely efficient and effective machine learning models/algorithms). These elements are in the heart of present IAMD systems, and adversaries are shifting their focus in attacking and disrupting their operations and effectiveness. Since the Vietnam war, missions like SEAD/DEAD[4] were the primary means for suppressing or destroying enemy air defenses. Today, cyberattacks and hybrid warfare will not target radars, C2 functions or SAM batteries, but will direct its efforts towards other – more lucrative – targets, that can greatly affect IAMD operations.

Hybrid Warfare

There are two strategies when using military force. The strategy of annihilation and the strategy of erosion. The first one refers to all actions towards the physical destruction of the enemy’s military

[4] **Suppression of Enemy Air Defenses/Destruction of Enemy Air Defenses (SEAD/DEAD)**, also known in the United States as "Wild Weasel" and (initially) "Iron Hand" operations, are military actions to suppress/destroy enemy surface-based air defenses, including not only surface-to-air missiles (SAMs) and anti-aircraft artillery (AAA) but also interrelated systems such as early-warning radar and command, control and communication (C3) functions, while also marking other targets to be destroyed by an air strike. Suppression can be accomplished both by physically destroying the systems or by disrupting and deceiving them through electronic warfare. In modern warfare, SEAD missions can constitute as much as 30% of all sorties launched in the first week of combat and continue at a reduced rate through the rest of a campaign.

capabilities. In that way the enemy becomes helpless, and his ability or will to resist is evaporated. This form has been historically characterized as annihilation or attrition[5]. The second strategy aims to convince the enemy that acceptance of the attacker's terms will lead to less suffering than the continuation of hostilities would. In this case, military power is used as an "erosive substance" against the will of the enemy's leadership and society to continue fighting[6].

The concept of a "revolution in military affairs" first appeared in the Soviet Union (today RF - Russian Federation) in the early 1980s, when Soviet Marshal Nikolai Ogarkov[7], wrote about a "military technical revolution" which could dramatically improve lethality as well as the capabilities of conventional weapons[8]. For years, the Soviet doctrine regarding the military technological enabler, favored mass production over quality[9], while the U.S. and its allies relied on technological advancements, especially in the fields of micro-electronics and communications as their competitive advantage in the battlefield. It is interesting that in a Congressional hearing in 1970 - two years before the invention of the microprocessor - General William Westmoreland testified that "*data links, computer assisted intelligence evaluation, and automated fire control…*" will be used in the future to search for, lock-on, and engage enemy forces.

Information technology is considered a key enabler in RMA and has been materialized in the "system of systems" approach by the U.S. military[10]. To create the required command structures, across all services and authorities, together with the integration of all weapon-delivery platforms it is essential to have a robust, reliable, and effective C4I system. The latter is heavily dependent on information technology advances and efforts. In that view today's military forces' dependance on complex and unreliable systems (e.g., computers, and communication systems) that are prone to attacks or disruption(s), is creating the risk of a complete breakdown, if these attacks being materialized and successful. As a result, the "all-domain warfare" was introduced, where all previously unlinked domains, land, sea, air, space, and cyberspace were now interconnected and interdepended. Currently, several foundational cyberwarfare programs are researching and assessing cyberwarfare capabilities at

[5] World War II is an example of annihilation.
[6] World War I is an example of erosion, when the German Revolution of 1918 - 1919 and the widespread loss of confidence that the war could be won led to the new German government to move towards surrender, even though the German army had not been decisively defeated in the battlefield and no Allied military force had penetrated the German borders.
[7] Nikolai Vasilyevich Ogarkov (Russian: Николай Васильевич Огарков; 30 October 1917 – 23 January 1994) was a prominent Soviet military personality. He was promoted to Marshal of the Soviet Union in 1977. Between 1977 and 1984, he was Chief of the General Staff of the USSR. He became widely known in the West when he became the Soviet military's spokesman following the shootdown of Korean Air Lines Flight 007 near Moneron Island in September 1983. He was dismissed as Chief of the General Staff on 6 September 1984.
[8] https://csbaonline.org/uploads/documents/2002.10.02-Military-Technical-Revolution.pdf
[9] Here it should be noted that poor quality does not necessarily means a lesser product. For example, the Soviet T-34, while would have never passed a German quality control, it introduced innovative design with his slope armor (the first example of what would later become the norm), fuel efficiency, and gun power.
[10] https://www.darpa.mil/program/cyber-assured-systems-engineering

the platform level, like that of kinetic warfare.

The U.S. military had a foul start in the Vietnam War, which had a tremendous cost to human lives. By the end of 1972, however, they had learned from their failures and had adapted their tactics. As a result, the U.S. won every battle they fought during the final years of the war, inflicting heavy losses on their opponents, but ultimately, withdrawing. This result came about, as they had lost both civil and political support in the U.S., along with the "hearts and minds" of the local population. The U.S. was fighting - perhaps without realizing it - a "hybrid warfare". Hybrid warfare as a term was first proposed by Frank Hoffman and describes a combination of conventional warfare, irregular warfare, and cyberwarfare together with information warfare actions, like fake news, disinformation, misinformation, and more. While there is no universally accepted definition, hybrid warfare helps better understand today's military operations and the challenges that have emerged. Various methods of combat encompass conventional and unconventional strategies and arrangements, acts of terrorism encompass selective aggression and manipulation, and criminal chaos is executed by both opposing factions, in addition to a diverse range of non-state entities. In such a form of warfare all efforts, including conventional military operations, are subordinate to an information campaign. It should be considered as a "whole-of-government" activity. As per the NATO definition:

Hybrid threats combine military and non-military, as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, and deployment of irregular armed groups and use of regular forces.

Hybrid warfare is not exactly a new idea; it can be viewed more of an old paradigm (Byzantine emperors used gold to manipulate enemies and avoid wars) exploiting of or adopting to new technologies, like computers, the internet, and the world wide web. For example, during the operation Overlord[11] (the allied cross-channel invasion of German-occupied Western Europe during World War II), the operation Bodyguard[12] successfully managed to mislead the Oberkommando der Wehrmacht (OKW) as to the time and place of the invasion. The success of this umbrella - operation was such that even after the first reports from Normandy, about the landings were received by the OKW, the latter still believed that this was not the main allied operation. Operation Bodyguard employed deception, signal intelligence and manipulation, and electronic warfare.

Hybrid Threats - An enemy you can't see, feel, touch, or hear.

[11] https://en.wikipedia.org/wiki/Operation_Overlord

[12] https://en.wikipedia.org/wiki/Operation_Bodyguard

In the era of information, hybrid threats have gained unprecedented potency due to the rapid advancements in technology and the proliferation of digital platforms. The interconnectedness of our globalized society has created a vast digital landscape where misinformation, propaganda, and cyberattacks can be deployed as potent weapons. State and non-state actors can exploit this landscape to manipulate public opinion, sow discord, and undermine trust in institutions. The ability to wage influence campaigns, spread disinformation, and launch cyberattacks poses significant challenges to governments, organizations, and individuals alike.

Furthermore, hybrid threats are not confined to the virtual realm but can also manifest in the physical world. Covert military operations, economic coercion, proxy warfare, and terrorist activities are just a few examples of the diverse tactics used in hybrid warfare. By blurring the lines between traditional warfare and unconventional methods, hybrid threats capitalize on the vulnerabilities and interdependencies of modern societies. They seek to exploit gaps in governance, exploit ethnic or religious tensions, weaken alliances, and erode societal resilience.

Addressing hybrid threats requires a comprehensive and multidimensional approach that combines intelligence-sharing, international cooperation, strategic communication, and investment in cybersecurity capabilities. It also necessitates enhancing societal resilience, promoting media literacy, and strengthening democratic institutions to counter disinformation and propaganda effectively. As technology continues to advance and new threats emerge, it is crucial for governments, organizations, and individuals to remain vigilant, adapt to the evolving landscape, and collaborate to mitigate the risks posed by hybrid threats.

Elements of Hybrid Threats

Cyberwarfare:

We can define cyberwarfare as the use of digital attacks against a state with the possibility to cause comparable harm to traditional kinetic warfare by the disruption of vital information, communication systems, and infrastructure[13]. While cyberwarfare as a concept is still debatable, most countries have developed active cyber units capable of both offensive and defensive cyber operations. Furthermore, there is debate as to whether cyberwarfare is distinct or not from the term cyber war. It is implied that cyber war typically refers to a long period of time, where multiple offensive and defensive operations or cyberwarfare-related operations are taking place. For the purposes of the current document cyberwarfare and cyber war will be considered as one [in an analogy to the other domains of operations were there is no distinction between air warfare and air

[13] See also: Singer, P.W. and Friedman, A. Cybersecurity and Cyberwar: What everyone needs to know.

war], and only the term cyberwarfare will be used, since it includes within itself, all the methods, actions, and references surrounding actions within the cyberspace domain of operations.

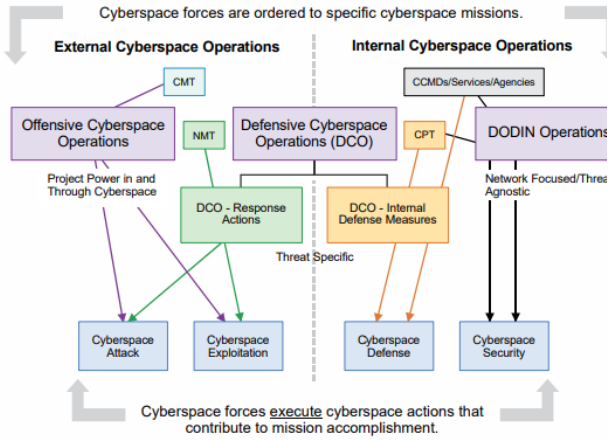


Figure 6 -Cyberspace Operations, missions, actions, and forces (Source: JP 3-12/2018)

In 1995, the United States Air Force published the Cornerstone of Information Warfare, in which the integration of cyberwarfare within the concept of military operations was first introduced. According to U.S. military doctrine, offensive cyberspace operations (OCO) are operations intended to "project power by the application of force in or through cyberspace"[14]. The idea behind the OCO is shaped through the concepts of **defending forward** and **persistent engagement**. These concepts describe ongoing confrontation efforts throughout cyberspace to stop threats materializing, by attacking the enemy's network and computing infrastructure. As a result, it was identified that cyberspace capabilities and, more specifically, OCO could be integrated into the military strategic objectives and plans. In that view, OCO could be used in coordination with other operations across the range of military operations, and even help achieve several military objectives through its implementation. The importance of OCO within the overall concept of military operations will grow as the reliance of military forces on cyberspace increases. Several challenges can be identified by the ever-increasing integration of OCO into the military doctrine. For example, the full integration of OCO, with operations and tools in the physical domain, requires effective synchronization and planning, as to set up the boundaries of OCO exploitation and usage, together with priorities and restrictions on their use.

Critical Infrastructures

Critical infrastructures are these essential systems, facilities, and assets the functioning and welfare of a society and its economy, fundamentally requires. These include sectors such as energy (oil, gas, electric power), water supply, transportation (highways, mass transit, aviation, maritime), telecommunications (broadcasting, internet, satellite), healthcare (hospitals, health information systems), food and agriculture, banking and finance, emergency services, and government functions, among others. These systems not only facilitate our daily lives but also ensure national security, public safety, and economic vitality. The failure or disruption of these

[14] https://www.justsecurity.org/64875/u-s-offensive-cyber-operations-against-economic-cyber-intrusions-an-international-law-analysis-part-i/

infrastructures could have a profound and potentially devastating impact, causing societal and economic instability or loss of life.

Maintaining the security and resilience of critical infrastructure is a shared responsibility among multiple stakeholders, including governments, the private sector, and individuals. Threats to these infrastructures range from natural disasters, like earthquakes or floods, to human-made incidents, such as cyberattacks or terrorism. Therefore, comprehensive strategies for risk management are required that cover physical security, cybersecurity, and organizational resilience. This involves the continuous evaluation of risks, implementation of protective measures, preparation for emergencies, and the ability to rapidly recover and adapt to changing conditions. The digital transformation of many critical infrastructures has also introduced new vulnerabilities and interdependencies, making the task of protecting these assets even more complex and challenging.

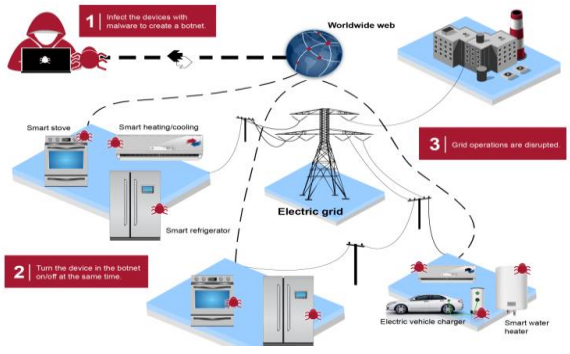


Figure 7 - An example of a cyber-attack against power grid (Source: https://www.gao.gov/assets/gao-21-81.pdf)

As per the **Cybersecurity & Infrastructure Security Agency's (CISA)** definition[15], Critical Infrastructure are those assets, systems, and networks that **provide functions necessary for our way of life**. There are 16 critical infrastructure sectors that are part of a complex, interconnected ecosystem and any threat to these sectors could have potentially debilitating national security, economic, and public health, or safety consequences. CISA identified **16 critical infrastructure sectors:**

Figure 8 - An overview of the critical infrastructure sectors

The **European Program for Critical Infrastructure Protection (EPCIP)** refers to the doctrine and programs created to identify and protect critical infrastructure[16] that, in case of fault, incident or attack, could seriously impact both the country where it is hosted and at least one other European Member State. **Council Directive**

[15] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience

[16] Council Directive 2008/114/EC in its Articles 2 and 3 also provides the definition of the European critical infrastructure (ECI). ECI means an asset, system or part thereof located on EU

2008/114/EC[17] adopted on December 8, 2008, is an integral part of the European Program for critical infrastructure protection, which emerged in the aftermath of the devastating terrorist attacks that shook the US and Europe in the early 2000s. Despite its terrorism-related roots, the EPCIP takes a broad approach regarding causes of threat. While recognizing threats resulting from terrorism as a priority, it embraces an all-hazards approach towards the protection of critical infrastructure, encompassing man-made and technological threats (e.g., industrial incidents, blackouts, terrorism) as well as natural disasters caused for instance by earthquakes, or extreme weather conditions, such as flooding and hurricanes.

In 2009, the European Commission published a communication (COM(2009) 149)[18] in which the protection of the **Critical Information Infrastructures** (CII) was addressed. Specifically, the communication aimed in strengthening the security and resilience of the CII by focusing on the prevention, preparedness, and awareness, and proposed a relevant action plan. The action plan was built upon 5 pillars:

- Preparedness and prevention,
- Detection and response (early warning mechanisms),
- Mitigation and recovery,
- International cooperation, and
- Further support in the implementation of Directive 2008/114/EC.

The directive established a step-by-step procedure for the identification and designation of critical infrastructures located on EU territory that are vital from a European perspective, in the sense that their disruption or loss would have major cross border impacts. In the years following the directive's entry into force, a number of parliamentary questions – for example E-8498/2010[19], E-000720/2012[20], E-002050/2013[21] and E-002999/2013[22] – related to cybersecurity, and in particular to EU plans and measures aiming to protect critical infrastructures against cyber-attacks. It was during this period that the EU shaped its first cyber security strategy (2013) and adopted the NIS Directive.

On December 16, 2020, drawing on the evaluation's findings, the Commission presented a new proposal for a directive on the resilience of critical entities (COM(2020) 829)[23], together with the supporting impact assessment. In view of the

territory, which is essential for the maintenance of vital societal functions, health, safety, security, economic or wellbeing of people, and the disruption or destruction of which would have a significant impact on at least two Member States, as result of the failure to maintain those functions. The significance of the impact is assessed against distinct cross-cutting criteria, which encompass casualties, economic and environmental effects, and public effects.

[17] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN

[18] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

[19] https://www.europarl.europa.eu/doceo/document/E-7-2010-8498_EN.html

[20] https://www.europarl.europa.eu/doceo/document/E-7-2012-000720_EN.html

[21] https://www.europarl.europa.eu/doceo/document/E-7-2013-002050_EN.html

[22] https://www.europarl.europa.eu/doceo/document/E-7-2013-002999_EN.html

[23] https://eur-lex.europa.eu/resource.html?uri=cellar:74d1acf7-3f94-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF

importance of cybersecurity for the resilience of critical entities, the Commission submitted a proposal in parallel for a revised NIS Directive ('NIS 2')[24]. To ensure full coherence, cyber-resilience obligations under NIS 2 would apply also to critical entities identified under the new proposal.

The Undersea Infrastructure Risk

In September 2022, the **Baltic Sea Nord Stream gas pipeline ruptured[25]**, an incident attributed to sabotage, but the origins of the saboteurs (or the methods used) are still unclear (at least openly). That incident laid light into the risk posed to undersea infrastructure, which includes oil and gas pipelines and data and electrical power cables[26]. The following figure depicts an overview of the fibre-optics underwater cables mapping around the world, which supports modern communications efforts. With an overall length of more than half a million miles of fibre-optics this is a huge infrastructure, mostly insecure and unprotected[27]. The undersea data cable network serves as a tangible representation of transnational digital connectivity, with over four hundred active cables spanning a minimum of 1.3 million kilometres worldwide. These undersea cables play a vital role in facilitating communication within Europe and connecting European countries with the rest of the world. In addition to their civilian applications, undersea cables are crucial for national security as they support military operations, diplomatic endeavours, and intelligence gathering. Any disruption in communication, even for a brief period, can result in severe consequences for time-sensitive operations and lead to substantial financial losses. Thus, the impact of any damage to these cables is highly significant[28].

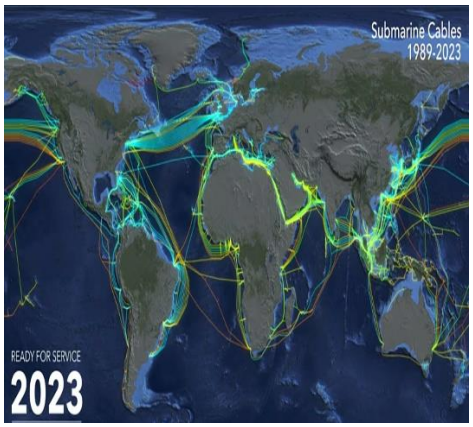


Figure 9 - Map of submarine cables

Today's internet is capable of coping with certain failures in its backbone infrastructure. If these failures would exceed a certain threshold, then global access to the internet would be severely altered and affected. Using every communications satellite[29] available in the Earth's orbit could carry just 7% of the communications currently sent via cable from the United States alone[30]. For years large depths and other constraints have been proven as the best

[24] https://eur-lex.europa.eu/eli/dir/2022/2555
[25] https://www.navalnews.com/naval-news/2023/05/nato-steps-up-response-to-clear-and-present-undersea-infrastructure-risk/
[26] https://www.euroafrica-interconnector.com/
[27] https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf
[28] https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf

[29] It should be stated here that during the 1980s, satellite communication was playing the dominant role for overseas communications. The construction of TAT-8, which is the first trans-Atlantic fiber-optic cable ever laid, tipped the balance back to cabling. [Carter L., Burnett D., Drew S., Marle G., Hagadorn L., Bartlett-McNeil D., and Irvine N. (2009). Submarine Cables and the Oceans - Connecting the World. UNEP-WCMC Biodiversity Series No. 31. ICPC/UNEP/ UNEP-WCMC]
[30] https://www.navylookout.com/the-threat-to-worlds-communications-backbone-the-vulnerability-of-undersea-cables/

Hybrid threats will primarily target societies and communities, not soldiers or military units.

safeguards of this network. Today, advancements in Underwater Unmanned Vehicles (UUVs)[31] have made these safeguards obsolete and inefficient. Since these cables are installed, with a large portion of their length being laid in international water and owned by private companies, they are outside the scope of national governments. As almost every legislative examined so far, the relevant United Nations Convention on the Law of the Sea[32] (UNCLOS) is highly deficient in ensuring the protection of this infrastructure.

Figure 10 - China's Militarized Unmanned Underwater Vehicles

Disinformation/Misinformation

Misinformation and disinformation are significant concerns in today's digitally driven society, as they can severely influence public opinion, distort truths, and create unnecessary panic or fear. Misinformation refers to inaccurate or false information, but crucially, it is spread without malicious intent. The concept of **"intent" is a crucial factor when discussing the handling of information**. It often arises from honest mistakes or misunderstandings and spreads organically through social networks, digital platforms, and traditional media. Misinformation can cause harm by feeding into biases, perpetuating stereotypes, or leading to poorly informed decisions, especially in critical areas such as public health, politics, or environmental issues. This fundamental distinction is significant because it influences the range of possible responses for dealing with unintentional misinformation compared to intentional information manipulation. For instance, when dealing with intentional, coordinated, and systematic manipulation, it may be appropriate to expose the responsible actors.

On the other hand, disinformation refers to the deliberate creation and distribution of false or manipulated information with the intent to deceive or mislead. Disinformation campaigns are often well-coordinated and purposefully designed to create discord, exacerbate divisions, or undermine trust in institutions. The internet, especially social media platforms, has significantly amplified the reach and impact of disinformation due to its ability to distribute content rapidly and widely. It can be used as a tool of influence or warfare by state or non-state actors, aimed at

[31] https://maritime-executive.com/editorials/how-china-is-militarizing-autonomous-underwater-vehicle-technology

[32] https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

destabilizing societies or influencing political processes. The fight against disinformation requires concerted efforts from governments, tech companies, media organizations, and individuals to promote fact-checking, media literacy, and transparency in the digital information ecosystem.

Artificial intelligence (AI) can be exploited for misinformation efforts in several ways, primarily due to its ability to create convincing fake content and to scale the distribution of such content.

Firstly, AI can be used to generate 'deepfakes', which are highly realistic and manipulated images, videos, or audio recordings. Advanced deep learning techniques like Generative Adversarial Networks (GANs)[33][34] can create fake videos or audio that are indistinguishable from real ones. For instance, an individual's face can be superimposed onto another person's body in a video, or their voice can be synthesized saying words they never spoke. These convincing deepfakes can then be used to spread misinformation, impersonate individuals, or create fake news, with potentially serious repercussions for individuals and society.

Figure 11 - Images created by NVIDIA's GAN AI. None of them is a real person!

Secondly, AI algorithms can be leveraged to automate and scale the distribution of misinformation. For example, 'bots'—automated social media accounts—can be programmed to share and amplify misinformation quickly and to large numbers of people. They can also be used to manipulate online discourse by artificially inflating the apparent popularity of a particular viewpoint, creating a false sense of consensus or trending topics.

Lastly, AI can be exploited for microtargeting, where misinformation is tailored to specific individuals or groups based on their online behavior, demographics, or preferences, thereby

[33] Generative Adversarial Networks (GANs) are a class of machine learning models that are designed to generate realistic synthetic data samples. GANs consist of two primary components: a generator network and a discriminator network, which are trained together in a competitive manner. The generator network takes random noise as input and learns to generate synthetic samples, such as images, text, or even audio, which resemble the real data. The discriminator network, on the other hand, acts as a critic that learns to distinguish between real and fake samples. It is trained on a dataset of real samples and the synthetic samples produced by the generator. During the training process, the generator and discriminator are trained in an adversarial manner. The generator tries to generate samples that fool the discriminator, while the discriminator aims to correctly classify real and fake samples. GANs have gained significant attention and achieved impressive results in various domains, including image synthesis, video generation, text generation, and more. They have been used for tasks such as image super-resolution, style transfer, data augmentation, and even generating entirely new and original content.

[34] https://jrodthoughts.medium.com/nvidias-impressive-gan-applications-fdfffeaf3609

increasing the likelihood of the misinformation being believed and shared. While AI has significant potential to benefit society, these challenges underline the importance of developing robust strategies to mitigate its misuse for spreading misinformation.

The significance of cybersecurity in this particular situation cannot be overstated[35]. To begin with, the convergence of cyberattacks and information manipulation in hybrid threats is key to their successful realization. Consequently, a comprehensive examination of interconnected phenomena must encompass the realm of cybersecurity. Additionally, gaining a deep comprehension of the tactics, techniques, and procedures (TTPs) employed by malicious individuals is essential for mounting effective countermeasures against potential threats.

Outer Space

Space, commonly known as outer space, is the vast expanse beyond Earth and its atmosphere, existing between celestial bodies. It should be noted that outer space is not completely devoid of matter; it is a nearly perfect vacuum. The precise boundary where outer space begins is not defined by a specific altitude above the Earth's surface. However, the Kármán line[36]. Throughout most of human history, space exploration was limited to observations made from the Earth's surface, initially with the naked eye and later with telescopes.

Prior to the development of reliable rocket technology, the highest humans had reached in their attempts to reach outer space was through balloon flights. The next significant milestone occurred in 1957 with the launch of the unmanned satellite Sputnik 1 by a Russian R-7 rocket. Subsequently, in 1961, Yuri Gagarin became the first human to venture into space aboard the Vostok 1 spacecraft. The feat of escaping from low Earth orbit, by the Apollo 8 spacecraft. The first spacecraft to achieve escape velocity[37], , was the Soviet Luna 1. The successful 1962 fly-by of Venus by Mariner 2 marked the first accomplished planetary mission. Since then, unmanned spacecraft have effectively investigated all the planets in the Solar System. Notably, in August 2012, Voyager 1 became the first human-made object to depart from the Solar System and enter interstellar space.

<u>The Outer Space Treaty</u>

The Outer Space Treaty, formally the “Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies”, is a multilateral treaty which provides the basis of international space law[38]. It was drafted under the

[35] https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape

[36] The von Kármán line is a proposed conventional boundary between Earth's atmosphere and outer space set by the international record-keeping body FAI (Fédération aéronautique internationale) at an altitude of 100 kilometres (54 nautical miles; 62 miles; 330,000 feet) above mean sea level.

[37] Escape velocity: the speed required to break free from Earth's gravitational pull.

[38] Space law refers to the body of international and national laws and regulations that govern activities in outer space. It encompasses a wide range of legal principles and treaties that aim to

auspices of the United Nations[39] and entered into force on 10 October 1967. Today, 113 countries have signed the treaty (which includes all countries with an active space program), plus another 23 signatories. The Outer Space Treaty was a result of the rapid development of intercontinental ballistic missiles (ICBMS) and:

a. Prohibits the deployment of nuclear weapons (actually weapons of mass destruction) in space. This includes the prohibitions of the establishment of military bases, testing of weapons and conducting military maneuvers on celestial bodies[40].

b. Limits the use of the Moon and all other celestial bodies for peaceful purposes.

c. Precludes any sovereignty claim (outer space = international waters).

Despite its efforts, the Outer Space Treaty is not "bulletproof". For example, it does not expressly and explicitly ban all military activities in space, nor the deployment of conventional weapons in space. As a result, countries around the world have established Military Space Forces and have developed and/or tested various weapons and techniques. Most notable examples are:

a. **Anti-Satellite Weapons (ASAT)**. Weapons (kinetic, or directed energy ones, like lasers) that are designed to destroy satellites or disrupt their operation (e.g., "blind" the various observation means). Even though ASAT weapons have not been used in conflict a number of countries (namely: China, India, Russia, and the United States) have demonstrated their abilities (often for decommissioning purposes). The development of ASAT weapons dates back to the late 1950s when the US Air Forces developed a series of advanced strategic missile projects. The most notable example is the Vought ASM-135 ASAT (which in turn is based on the AGM-69 SRAM) which was tested in 1985 against the Solwind P78-1 satellite. Although successful, the program was cancelled in 1988. In 2008, the US Navy destroyed a malfunctioning US spy satellite (USA-193) with a RIM-161 SM-3. The Soviet Union[41] also had an active development program of ASAT weapons, and in 1963 presented the Polyot interceptor. In 1968, Soviet Union successfully tested an orbital ASAT weapon[42]. In the early 1980s the Soviet Union developed the 30P6 "Kontakt", an air-launched (from a modified MiG-31D Foxhound) ASAT missile. Soviet Union's ASAT programs were

ensure the peaceful and responsible exploration and use of outer space. Space law primarily deals with issues related to space exploration, satellite communications, space debris, liability for damages caused by space activities, and the use and protection of celestial bodies.

[39] The United Nations (UN) is an international organization founded in 1945 to promote peace, security, and cooperation among nations. It serves as a forum for member countries to address global issues, coordinate policies, and facilitate humanitarian efforts worldwide.

[40] Celestial body: A single, tightly bound, contiguous entity.

[41] Notably, Soviet Union also experimented with the creation of military space stations under the Almaz project. https://en.wikipedia.org/wiki/Almaz

[42] Soviet Union created the IS (or Istrebitel Sputnikov – destroyer of satellites) program in 1961. The IS was a co-orbital warhead which would track and destroy a satellite with the use of shrapnel. Various tests have been performed, with the system been declared operational in 1973.

continued from Russia, which in 2015 had successfully tested the PL-19 Nudol direct ascent anti-satellite missile. China (SC-19 ASAT, Dong Neng-3, etc.) and India (Mission Shakti, etc.) have also active ASAT programs.

The debris issue: All of the above-mentioned ASAT weapons tests have created a large field of debris, which took months or even years to re-enter the atmosphere and burned. It is estimated that space debris could pose a larger threat than the original hit, in what is known as the "Kessler Syndrome". The Kessler Syndrome, also known as the Kessler Effect or collisional cascading, is a theoretical scenario in space where the density of objects in Earth's orbit becomes so high that collisions between objects create a cascade effect, leading to an exponential increase in space debris. This phenomenon is named after NASA scientist Donald J. Kessler, who was the first to propose it, in 1978.

The privatization of space: The privatization of space refers to the increasing involvement of private companies and individuals in space exploration, research, and commercial activities. Historically, space exploration was primarily the domain of government agencies, such as NASA[43] (National Aeronautics and Space Administration) in the United States and Roscosmos in Russia. However, in recent years, there has been a significant shift towards private sector participation in space-related endeavors. Several key factors have contributed to the rise of private space companies. Firstly, advancements in technology have made space exploration and satellite launches more accessible and cost-effective. This has allowed private companies to develop their own rockets, spacecraft, and satellite systems[44]. Secondly, there is a growing interest from private companies in exploiting the commercial potential of space. Already we have witnessed, how commercial technology, originally designed for public purposes (SpaceX's Starlink: A satellite constellation network which can provide global – satellite – internet coverage) can be used and exploited for military purposes[45][46]. In a public statement made by Ukraine's Minister of Digital Transformation, Mykhailo Fedorov, it was stated that Starlink "*is crucial support for Ukraine's infrastructure and restoring the destroyed territories*."

b. **Rods of God**. Hypervelocity Rod Bundles (or Rods of God) was a system of tungsten rods[47], which are deployed in Earth's orbit and can have global strike capability. The rod itself would have no warhead; its large kinetic energy originating from its orbital velocities (estimated at

[43] https://www.nasa.gov/

[44] . Companies like SpaceX, Blue Origin, and Virgin Galactic have made substantial progress in developing reusable rocket systems, which significantly reduce the cost of space launches.

[45] https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose

[46] https://www.usaid.gov/news-information/press-releases/apr-05-2022-usaid-safeguards-internet-access-ukraine-through-public-private-partnership-spacex

[47] Each rod is made of tungsten and its physical dimensions are 6 meter high and 30 cm in diameter. Tungsten is a greyish-white lustrous metal, which is a solid at room temperature. Tungsten has the highest melting point and lowest vapor pressure of all metals, and at temperatures over 1650°C has the highest tensile strength.

Mach 10 on impact), would have been enough to cause significant damage. It is estimated[48] that the yield would be similar to that of a small tactical nuclear bomb, without the radio-active debris or radiation. This "feature" (no radiation) means that the rods are not categorized as "weapons of mass destruction" therefore are not in direct violation of the Outer Space Treaty! By carefully positioning a constellation of satellites, a target could be hit within a timeframe of 12-15 minutes, which is half the time an ICBM needs, plus there is no launch warning. Such a weapon (if or when it is deployed) is almost impossible to defend against.

Economic Influence/Trade-war

In March 2021 (still a COVID-19 year) the 400-metre-long container ship **Ever Given**[49] runs aground in the Suez Canal[50], effectively blocking all marine traffic through the canal. Eventually, the ship was freed by the combined efforts of several tags after 6 days, and with the canal checked for damage, the traffic was allowed to resume. Until then, almost 400 ships were queued to pass through the canal, with the delay creating panic to the markets and more than US$9.6 billion in damages[51][52].

Figure 12 - Satellite imagery of the Ever Given being stuck in the Suez Canal [source: Wikipedia]

While this was an accident, its impact on the world economy was significant. Maritime historian Sal Mercogliano told the Associated Press[53]: "Every day the canal is closed... container ships and tankers are not delivering food, fuel and manufactured goods to Europe and goods are not being exported from Europe to the Far East." Maritime transport accounts for 80% of international trade, and a significant disruption on one (or more) of the "bottlenecks" can have a significant impact on national security (supply of new weapon systems, spare parts, ammunition, etc.).

[48] https://www.theguardian.com/science/2005/may/19/spaceexploration.usnews

[49] Ever Given is one of the largest container ships in the world. Its design is based on the Imabari 2000 design developed by Imabari Shipbuilding. It was completed on 25 Sep.2018 and have been chartered by Evergreen Marine. She has a length of 399.94 meters, a beam of 58.8 meters and a gross tonnage of 220.940, with a capacity of 20.124 TEU.

[50] The Suez Canal (In Arabic: Qanat as-Suways), is an artificial sea-level waterway running north to south across the Isthmus of Suez in Egypt to connect the Mediterranean Sea and the Red Sea. The canal separates the African continent from Asia, and it provides the shortest maritime route between Europe and the lands lying around the Indian and western Pacific oceans. It is one of the world's most heavily used shipping lanes. The Suez Canal is one of the most important waterways in the world. [https://www.suezcanal.gov.eg/English/Pages/default.aspx]

[51] https://www.bbc.com/news/business-56533250

[52] https://www.bbc.com/news/business-56559073

[53] https://www.kare11.com/article/news/nation-world/cargo-ship-suez-canal-trapped/507-3ca6964c-3ac2-4b13-867c-38d87366ea5d

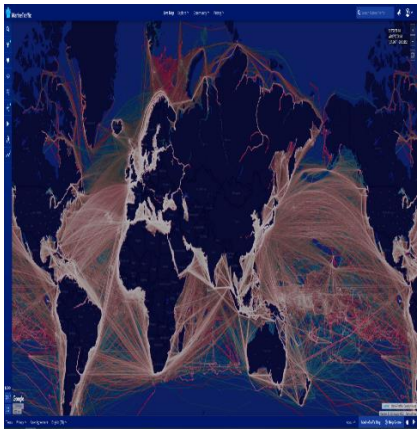


Figure 13 - Marine traffic heat map [source: https://www.marinetraffic.com/blog/shipping-trends-at-a-glance/]

Trade wars occur when countries engage in disputes over commerce, often triggered by the imposition of tariffs or quotas. This economic conflict can arise from a variety of reasons, such as protection of domestic industries, preservation of national security, or response to unfair trade practices. In a trade war, one nation will raise or impose new tariffs on a specific set of goods imported from another country. In response, the affected country often retaliates with its own set of tariffs, leading to an escalating cycle of economic confrontation.

While the ostensible goal of a trade war may be to protect domestic industries and create jobs, they often result in mixed outcomes and can have broad, unpredictable economic implications. For instance, while some domestic industries might benefit from less foreign competition, others can suffer due to increased costs for imported goods or materials, and consumers often face higher prices. Furthermore, trade wars can disrupt global supply chains, as businesses are forced to navigate shifting tariff landscapes, which can in turn lead to decreased economic stability and growth worldwide. Trade wars can also strain diplomatic relations between nations and potentially spill over into other areas of international cooperation.

China's economic influence has had a transformative impact on the global stage. Through its manufacturing prowess, China has become the world's factory, producing a vast array of goods at competitive prices. Its position as the largest exporter and second-largest importer has allowed it to shape global trade flows and supply chains. Chinese companies have invested heavily in foreign markets, acquiring strategic assets, and expanding their reach across various sectors. The Belt and Road Initiative[54], with its ambitious infrastructure projects, has further expanded China's economic influence by fostering trade connectivity and infrastructure development across multiple regions. China's rise as a technological powerhouse has also bolstered its economic influence, with its companies' leading advancements in areas such as e-commerce, telecommunications, and artificial intelligence. As a major lender and development financier, China's economic influence extends beyond trade and investment, enabling it to forge deeper economic ties with countries around the world.

[54] The Belt and Road Initiative (also known as the One Belt One Road) is a global infrastructure development strategy adopted by the Chinese government. It is considered a centerpiece of China's "Major Country Diplomacy" strategy, which is in accordance with China's rising economic and diplomatic power and global status.

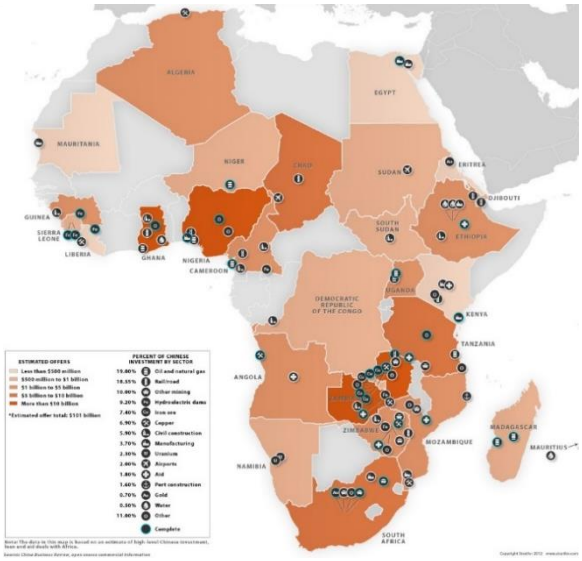


Figure 14 - China's Investment Offers in Africa since 2010 (Copyright: Stratfor 2012)

However, China's economic influence is not without its controversies and concerns. Critics argue that China's state-led economic model and policies, such as subsidies for state-owned enterprises and intellectual property concerns, create an unlevel playing field for foreign competitors. Additionally, China's growing assertiveness in territorial disputes and its approach to human rights have raised questions about the ethical implications of its economic influence. Debt sustainability is another issue, particularly in countries that have borrowed heavily from China to finance infrastructure projects, leading to concerns about potential debt traps and the long-term implications for these economies. As China's economic influence continues to grow, it remains a subject of ongoing debate and scrutiny in the global economic landscape.

Rare Earths

Rare earths, also known as rare earth elements (REEs), are a group of 17 chemical elements that belong to the lanthanide series of the periodic table. Rare earths – contrary to popular belief, or what their name suggests, are plentiful in the Earth's crust. However, they are rarely found in concentrated and economically exploitable deposits, which is why they are considered "rare". Rare earth elements possess unique properties that make them essential in various modern technologies. They are used in the manufacturing of a wide range of products, including electronics, magnets, catalysts, batteries, glass, and lasers. For instance, neodymium is used in the production of powerful magnets employed in computer hard drives, headphones, and electric motors. Lanthanum and cerium are used in catalytic converters for automobiles, while europium and terbium are used in fluorescent lamps and television screens. **Given their strategic importance and widespread use, rare earth elements have become valuable resources in international trade and geopolitics. A few countries, including China, possess significant rare earth reserves and dominate the global production and supply of these elements.**

Addressing Hybrid Threats

Hybrid threats, a complex and evolving form of security challenge, have emerged as a pressing concern in today's interconnected world. Combining a diverse range of tactics that blend conventional military strategies with unconventional methods, such as cyber warfare,

disinformation campaigns, and economic coercion, hybrid threats pose significant risks to nations, organizations, and societies. Addressing these multifaceted challenges requires a comprehensive and adaptive approach that encompasses diplomatic, military, economic, and informational elements. By understanding the nature of hybrid threats and developing robust strategies, governments and international actors can effectively safeguard against these emerging dangers and preserve the stability and security of our interconnected world.

On October 14, 1943, B-17s Flying Fortresses from the 8th Air Force's 1st and 3rd Air Divisions flew 400 miles from their bases in East Anglia, to Schweinfurt, Germany, in a mission known as "Black Thursday" due to the heavy losses inflicted to the bombers (60+ B-17 lost!). In 1943 Schweinfurt was a typical German town, with a unique characteristic. Its factories (such as the Schweinfurter Kugellagerwerke) produced most of Nazi Germany's ball bearing production. Air planners of the 8th Air Force identified that the destruction of the factories could significantly disrupt the whole German war production; and their assumption was correct. A Flack 88 anti-aircraft gun needed 88 of these devices to operate smoothly, while a twin-engine M110 needed more than 600, just for its engines. Interestingly, the "heart" of the Nazi's war production was not in the Ruhr valley, but in a small town in central Germany.

The above-mentioned example gives an overview regarding the challenges raised by **hybrid threats**. It is almost impossible to identify the **key strategic elements** that are critical to national and collective security in our interconnected and digitized world. Everyone should be considered a target, even if what we are targeting is quite different. Modern "bullets" will target the mind and not the flesh. Hybrid threats are blurring the lines between military and societal targets, what is considered a weapon (or how a weapon may be used[55]), or even a casualty. It is safe to assume that **are no borders or defined lines!**

Attribution

According to international law, **Attribution**, is a critical concept that refers to the process by which the actions of individuals or entities are officially recognized and assigned to a particular state. This principle plays a pivotal role, especially in issues concerning the violation of international law, as it dictates when a state can be held legally responsible for such violations. The criteria for attribution are primarily based on control, meaning the state must exercise significant control over the actions of the entity for these actions to be attributed to the state. The International Law Commission's Articles on State Responsibility provide a comprehensive framework for this attribution process, establishing the conditions under which states can be held accountable for

[55] During the Russian – Ukraine war, old S-300/C-300 missiles (normally and air defence weapon) have been used as rockets.

breaches of international law. **Since hybrid threats can exploit cyber-attacks, proxies, or deep fakes, attributing such actions to a specific entity can be extremely difficult if not impossible!**

A hybrid campaign employs a combination of various tools, methods, and actions with malicious intent to achieve its objectives. These activities may involve the use of force and are coordinated to avoid drawing a conventional response. The aim is to disrupt the target's ability to respond effectively while remaining unidentified and unaccountable. Dealing with hybrid threats is challenging due to their ambiguous nature, as they are difficult to classify as threats until they materialize. Additionally, an effective response requires coordination, synchronization, and consistency among governments, international organizations, and the private sector. In recent years, both developed and resilient states have faced challenges arising from the hostile actions of both state and non-state actors. Although resilience strengthens defenses against hybrid means, it alone is insufficient. While resilience should form the foundation of the response to hybrid threats and contribute to deterrence, it needs to be complemented with other measures.

While the main responsibility for addressing hybrid threats lies at the national level, as acknowledged by both the EU and NATO, it is crucial to recognize that these threats surpass national boundaries, emphasizing the importance of multilateral cooperation. Given the nature of such threats, states must collaborate with their allies and partners. Engaging in collective action within the realms of politics, diplomacy, and economics, as well as utilizing multinational attribution and strategic messaging, often yields greater effectiveness compared to individual national efforts.

Deterrence

The classical deterrence theory can be traced back to the Peloponnesian War (431 – 404 BC), the famous ancient Greek war between Athens and Sparta for the hegemony of the Greek world, and the threat of violence in response to adversary actions. It is a well-defined concept that has been studied and practiced throughout history and to an even greater depth following the advent of nuclear weapons. In 1962, Herman Kahn, had coined the idea of “Mutual Assured Destruction” or MAD, based on the strategy of rational deterrence, which holds that the threat of using destructive weapons against the enemy is an adequate measure for maintaining peace and stability. The strategy itself is based upon Nash’s equilibrium in which, once armed, neither side has the will to initiate a conflict. **Deterrence is therefore a form of behavior modification**. A strategy of deterrence, which can be implemented through two primary approaches: imposing costs or punishments, should be integrated with other strategies and policies instead of being isolated. In the real world, states have various priorities when interacting with each other, and security is just one aspect among many. **For**

a deterrence strategy to achieve optimal effectiveness, it must align and work in harmony with other national and multinational strategies.

Hybrid Threats and modern IAMD

Modern Integrated Air and Missile Defenses are a key stakeholder in modern conflict(s). Its significance and importance are already demonstrated in the Russia – Ukraine war, with the anti-aircraft missile batteries playing a key role in the military operations. Nevertheless, modern IAMD should transform its doctrine, strategy, and potentially its equipment, in order to remain valid against a magnitude of threats and the unconventional exploitation of conventional weapons.

A Change in Mentality

Hybrid threats (and the relevant actors) have the potential to use conventional means in unconventional ways. For example, a significant amount of the cruise missiles launched during the first day of the Russian – Ukraine war, was targeting not the conventional (or legacy, or "normal") military targets, like headquarters, governmental buildings, ammunition factories, or military units, but was directed against Ukraine's data center and the relevant network infrastructure. These attacks were in close combination with cyber-attacks exploiting vulnerabilities and targeting significant elements of Ukraine's ICT structure. While networking is among the critical sectors, the extent of the attacks was unpresented. It is safe to assume that Ukraine's connection to the internet is being achieved only through SpaceX's Starlink.

Another key observation from the Russian – Ukraine war, is the extensive use of electronic warfare (EW) systems and techniques. Highly classified and capable Russian EW equipment have been deployed in the front line (Ukrainian forces were able to capture[56] part of Russia's Krasukha-4 EW system). It is the first time that EW capabilities have been exploited is such an extent. If the reports are correct, Ukrainian forces have no communication capabilities expert satellite internet, for a distance of 60 KMs from the front line.

IAMDs Vulnerabilities

Besides its inherited vulnerabilities, IAMD's reliance on modern technology and systems has expanded the relevant threat landscape. The introduction of networks and computer systems, as an answer to interoperability, interconnection, and computing power demands, have made modern IAMD structures vulnerable to cyber-attacks and electronic warfare. Even the slightest disruption in the ICT infrastructure exploited by the IAMD forces can have devastating results. Cyber-attacks (even automatic ones: AI can be utilized to automate certain types of cyberattacks,

[56] https://www.telegraph.co.uk/world-news/2022/03/23/ukrainians-capture-russian-warfare-equipment-used-intercept/

such as brute-force attacks or credential stuffing or it can attempt to gain unauthorized access to systems or accounts by systematically trying different combinations of usernames and passwords) are yet now actively addressed in the IAMD doctrine.

Furthermore, IAMD personnel can be prone to deep fakes, disinformation campaigns or foreign information manipulation actions, which will be supported by AI-generated images, chatbot armies[57], deep fakes and more. Attacks of this kind can be used to manipulate human behavior, for blackmail purposes, or for influence and can be launched well before the actual attack.

Modern IAMD structures implement a variety of sensors (radars, electro-optical systems, etc.), radio networks, computers, missiles, trucks, and equipment. Most of these systems require skilled technicians and a plethora of spare parts, tools, and accessories to keep them functional and to address malfunctions and failures. This effort relies on a steady flow of the needed equipment and parts, which in turn is manufactured in state-of-the-art establishments. Disruption in the supply chain of these elements can severely disrupt IAMDs operations. For example, the largest and one of the most valuable semiconductor companies in the production of semiconductors (which can be found almost in every electronic device) is TSMC, based in Taiwan. If TSMC's production is affected (or even destroyed) the global (mostly Western) production of computer chips and semiconductors will collapse!

Responding to Hybrid Threats

The proposed approach is based on three main pillars: **EDUCATE, IDENTIFY, and finally RESPOND** to the threat of Hybrid Threats.

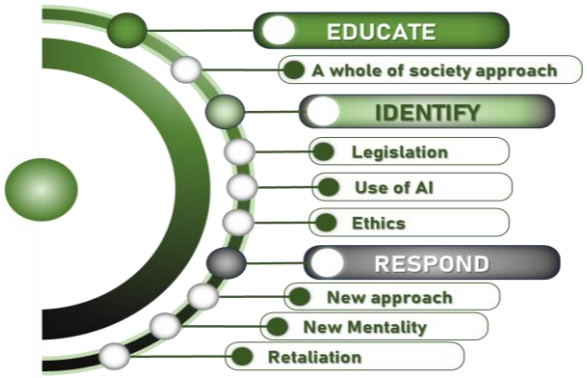


Figure 15 - Addressing Hybrid Threats - A change in mentality (graphic: author)

First Pillar – EDUCATE. As we have already demonstrated, hybrid threats will try to "attack" the hearts and minds of their targets, aiming in disrupting their will to fight or create favorable

[57] A chatbot army refers to a collection or group of chatbots working together to perform various tasks or provide support in an automated manner. These chatbots are typically powered by artificial intelligence (AI) and natural language processing (NLP) technologies. They are designed to engage in conversations with users, understand their queries, and provide relevant responses or assistance. A chatbot army can be used for malicious activities also, like spamming and phishing (malicious actors could create a chatbot army to send out a large volume of spam messages or phishing attempts. These chatbots can mimic human-like conversations to deceive users into revealing sensitive information or clicking on malicious links), social engineering (Chatbot armies could be deployed to manipulate and exploit users emotionally or psychologically. By engaging in conversations that build trust and rapport, the chatbots could extract personal information, gather intelligence, or even persuade individuals to perform harmful actions), spreading misinformation (A chatbot army can be used to disseminate false information, rumors, or propaganda. By leveraging AI and NLP capabilities, these chatbots can generate convincing content that may deceive individuals or manipulate public opinion), etc.

opinions for the opponent/aggressor. One of the best ways to address this challenge is EDUCATION. This should be a "whole of society" effort and should be suitably tailored for a variety of scenarios. One of the best ways to achieve that goal is by "raising awareness". Already most organizations, military units, companies, and governments, implement cybersecurity awareness programs. These can be used as the blueprints for an extensive awareness program against human manipulation (including misinformation campaigns, social engineering, etc.). Furthermore, a change of mentality is needed for the IAMD personnel. Modern conflicts (especially the Russian – Ukraine war) have demonstrated that the form and way of war has changed, and similarly, the identification and prioritization of protected areas and targets should also change.

Second Pillar – IDENTIFY: The introduction of OpenAI's ChatGPT[58] opened a world of tremendous potential and grave danger to the general public. Modern AI models can be used for a variety of tasks, including malicious and legitimate purposes. As malicious actors are using AI to create chatbot armies, deep fakes, or malicious software, similarly AI can be used to detect attacks, attacking patterns, analyze malware, etc. Furthermore, AI can be used for IAMD-related tasks, like target acquisition and tracking, target identification, signal analysis, and more.

Third Pillar – RESPOND: As we have mentioned previously, deterrence is a key aspect of a military strategy. Therefore, modern IAMD elements should have the capacity to answer (or retaliate) outside their conventional doctrine. For example, modern IAMD units should be able to detect cyber-attacks against their networks or have the capacity to address extensive electronic or microwave attacks. Furthermore, modern IAMD should start exploring if new protected areas/targets should be added in its doctrine. For example, should IAMD protect critical space assets, and how this approach will be achieved?

Epilogue - A look into an "apocalyptic" future

In the realm of hybrid warfare, AI technology plays a pivotal role in achieving information dominance and understanding, which can be decisive in conflict situations. AI enables the replication, influence, and alteration of group behaviors, thereby shaping the social and economic impacts of hybrid conflicts. Due to its innate capacity to streamline intricate operations and improve effectiveness, artificial intelligence has become a crucial focus for armed forces and intelligence agencies when addressing hybrid warfare scenarios. For

[58] ChatGPT is an AI-based conversational agent developed by OpenAI. It is powered by the GPT-3.5/4 architecture, which stands for "Generative Pre-trained Transformer 3.5." GPT-3.5 is an advanced deep learning model that uses a transformer architecture to generate human-like text responses. As a language model, ChatGPT is trained on a vast amount of text data from the internet, including books, articles, and websites. It learns to understand and generate coherent responses by predicting what comes next in a given sequence of text. It can provide information, answer questions, engage in conversations, and assist with various tasks.

instance, AI can facilitate advanced intelligence-gathering, processing, and exploitation, making it increasingly challenging to conceal soldiers, proxies, or equipment. With a comprehensive AI-enabled apparatus, a nation-state can effectively combat hybrid insurgents. The United States military has already embraced AI in various aspects, particularly in intelligence, surveillance, and reconnaissance operations. AI enables the utilization of unstructured data sources like full-motion video and automated audio and text analysis, leading to significant reductions in reaction times without compromising precision. Real-time data integration driven by AI provides a deeper understanding of behavioral patterns, structures, and technological relationships. AI finds application in numerous roles and scenarios, ranging from the creation of chatbot armies with deepfake capabilities to automatic target recognition. While autonomous weapon platforms currently require operator approval for firing ordnance, their AI-driven targeting systems rely on extensive training to identify strategic targets. Future developments may incorporate new AI algorithms and systems in Ground-Based Air Defense (GBAD) systems, potentially involving signal processing.

Biosecurity is another aspect of concern. Biosecurity represents a critical set of practices and principles used to prevent the introduction, establishment, and spread of pests, diseases, and invasive species in both agricultural and natural ecosystems. This discipline extends to include measures to prevent the unintended release of genetically modified organisms. A biosecurity plan incorporates preventative tactics for controlling and managing biological risks, utilizing a combination of physical, chemical, and biological methods. By protecting populations against harmful biological threats, biosecurity plays a crucial role in ensuring food safety, environmental protection, public health, and economic stability. In the era of global trade and climate change, biosecurity measures have become increasingly vital to maintain the integrity and sustainability of ecosystems worldwide. It is a multidisciplinary field that combines scientific research, policy development, education, and international cooperation to mitigate the risks posed by biological threats in an increasingly interconnected world. Biosecurity and hybrid threats intersect in the realm of complex, multidimensional risks, representing an emerging field of study and concern. Hybrid threats can be understood as a combination of traditional and non-traditional security challenges that blend methods, and cross borders and sectors. In the biosecurity context, hybrid threats might include bioterrorism, where harmful biological agents are used maliciously, or the deliberate introduction of an invasive species into a vulnerable ecosystem for economic or political disruption. Additionally, cyber threats to biosecurity infrastructure, such as data breaches of sensitive biological data or cyber-attacks on laboratory systems, can pose hybrid threats. Biosecurity strategies must now consider these hybrid challenges, necessitating a multidisciplinary approach that encompasses medical, biological, environmental, cyber, and

policy considerations to maintain the safety and integrity of both natural and human systems.

Quantum computers represent a monumental leap forward in computing technology, employing the principles of quantum mechanics to process information. Unlike classical computers, which use bits that can be either a 0 or a 1, quantum computers utilize quantum bits, or qubits. These qubits, governed by the principles of superposition and entanglement, can exist in multiple states simultaneously and can be correlated in ways that classical bits cannot, vastly increasing computational power and speed. This opens up potential applications in areas such as cryptography, optimization problems, drug discovery, and even quantum simulations, where classical machines struggle. However, as of 2021, quantum computing is still largely experimental, facing significant challenges like maintaining quantum coherence and error correction. Despite these hurdles, the potential impact of quantum computing continues to inspire relentless research and development efforts worldwide. Post-quantum cryptography, also known as quantum-resistant cryptography, refers to cryptographic algorithms (usually public-key algorithms) that are thought to be secure against an attack by a quantum computer. ("Quantum Encryption vs. Post-Quantum Cryptography (with Infographic ...") As of my knowledge cutoff in September 2021, no quantum computer yet exists that could break any but the simplest cryptographic codes, but it's widely understood that such a computer would fundamentally disrupt our current systems of cryptography. Therefore, the field of post-quantum cryptography is devoted to developing new algorithms that could survive even the advent of practical quantum computing. These new cryptographic systems strive to protect data integrity, confidentiality, and authentication in a world where quantum computing is a reality. •

Further reading

- Giulio Douhet (1983). *The command of the air*. Washington, D.C.: Office of Air Force History.
- Sunzi and Nylan, M. (2020). *The art of war*. New York: W. W. Norton & Company
- Ware, W.H. and Rand Corporation (1967). *Security and privacy in computer systems*. Santa Monica, Calif.: Rand Corp
- Karras, T., Nvidia, S., Timo, A. and Nvidia (n.d.). A Style-Based Generator Architecture for Generative Adversarial Networks. [online] Available at: https://arxiv.org/pdf/1812.04948.pdf
- Anon, (n.d.). International Law in Cyberspace. [online] Available at: https://harvardilj.org/2012/12/online_54_koh/
- Carl Von Clausewitz, Howard, M. and Al, E. (1993). On war / Carl von Clausewitz; Edited and transl. by Michael Howard, et. al. London Everyman's Library.
- Herman, P.F. (1994). The military-technical revolution. Defense Analysis, 10(1), doi:10.1080/07430179408405608.
- Hoffman, Frank (2007). Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, Virginia: Potomac Institute for Policy Studies. Available online: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf
- Singer, P.W. and Friedman, A. (2020). Cybersecurity and cyberwar : what everyone need to know. New York, Ny: Oxford University Press
- Kofman, M., Migacheva, K., Nichiporuk, B., Radin, A., Tkacheva, O. and Oberholtzer, J. (2017). Lessons from Russia's Operations in Crimea and Eastern Ukraine. [online]Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1498/RAND_RR1498.pdf.
- A. F. Brantly, "The cyber deterrence problem," 2018 10th International Conference on Cyber Conflict (CyCon), 2018, pp. 31-54, doi: 10.23919/CYCON.2018.8405009.

- Arnold Wycombe Gomme (2019). Thucydides | Greek historian. In: Encyclopædia Britannica. [online] Available at: https://www.britannica.com/biography/ Thucydides-Greek-historian [Accessed 15 Apr. 2019].
- Department of Defense Dictionary of Military and Associated Terms. (2010). [online] Available at: https://irp.fas.org/doddir/dod/jp1_02.pdf [Accessed 23 Oct. 2021]
- Department of Homeland Security, National Infrastructure Protection Plan, Washington: US Department of Homeland Security, 2009.
- European Commission (2009), On critical information infrastructure protection, protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, Communication 149 final, Brussels, 30. 03.09.
- Krepinevich, A. (n.d.). The Military-Technical Revolution: A Preliminary Assessment. [online] Available at: https://csbaonline.org/uploads/documents/2002.10.02-Military-Technical-Revolution.pdf
- Libicki, M.C. (2021). Cyberspace in peace and war. Annapolis, Maryland: Naval Institute Press
- Perlroth, N.: This is How they Tell me the World Ends, London (2021). https://doi.org/10.5038/1944-0472.14.2.1958
- Defending Ukraine: Early Lessons from the Cyber War: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/
- Katherine Mansted, “Engaging the public to counter foreign interference”, 9 Dec 2019, https://www.aspistrategist.org.au/engaging-the-public-to-counter-foreign-interference/
- Leventopoulos, S. (n.d.). RETALIATION WITHIN THE SCOPE OF CYBERSECURITY. [online] Available at: http://www.pyxida.aueb.gr/index.php?op=view_object&object_id=9547.
- D Deudney (1983). Whole earth security : geopolitics of peace. Washington
- Osborne, M.J. and Rubinstein, A. (1994). A course in game theory. Cambridge, Mass.: Mit Press
- "Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present" by Williamson Murray and Peter R. Mansoor
- "Hybrid War and the Future of Global Conflict" by Sean N. Kalic and Sterling Recker
- Strachan, Hew, and Sibylle Scheipers (eds), The Changing Character of War (Oxford, 2011; online edn, Oxford Academic, 19 Jan. 2015), https://doi.org/10.1093/acprof:osobl/9780199596737.001.0001, accessed 18 May 2023.
- https://info.publicintelligence.net/SMA-RussianStrategicIntentions.pdf
- Little Green Men: A Primer on Modern Russian Unconventional Warfare" by John R. Schindler
- NATO's "Handbook of Russian Information Warfare" by Keir Giles
- Radin, Andrew, Hybrid Warfare in the Baltics: Threats and Potential Responses. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1577.html
- Chivvis, Christopher S., Understanding Russian "Hybrid Warfare": And What Can Be Done About It. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/testimonies/CT468.html.
- https://www.rand.org/blog/2022/11/ukraines-lessons-for-the-future-of-hybrid-warfare.html
- https://www.csis.org/analysis/evolution-hybrid-warfare-and-key-challenges
- https://www.csis.org/programs/gray-zone-project
- https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape
- https://www.nato.int/cps/en/natohq/topics_156338.htm#
- https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en

An overview of international hypersonic flight programs and related technologies

By Dr Ioannis NIKOLOS &
Mr Angelos KLOTHAKIS

Introduction

Recent - unconfirmed - information concerning the shot-down of Kinzhal hypersonic missiles in Ukraine, further escalated the ongoing debate on whether the hypersonic weapons are unstoppable with the current technology of anti-ballistic and anti-aircraft surface-to-air defence systems. Nevertheless, the flight characteristics of hypersonic missiles render their detection, tracking, and interception a very demanding task for the existing systems. Hypersonic vehicles, unlike other high-speed vehicles such as ballistic missiles, possess unique characteristics that make them highly maneuverable and challenging to track or intercept[59] [60]. The development, manufacturing, and operation of these vehicles require significant advancements in areas such as gas dynamics, Computational Fluid Dynamics (CFD), propulsion, flight control, and material science. This is necessary to ensure that the vehicles can withstand the complex flow effects, instabilities, accelerations, and heat loads experienced during hypersonic flight. Despite these scientific and technological challenges, major military powers are investing in the development of hypersonic vehicles, due to their potential to significantly impact future military operations and doctrines; the availability of such systems within the inventory of a military power, may prove to be a game-changer in the near future, especially in the case that adversary forces have not the ability to develop effective and efficient countermeasures, within rational cost limits[61].

There are three main types of hypersonic vehicles identified for military applications:

1. Exo-atmospheric ballistic missiles: These rocket-powered missiles operate at hypersonic speeds, partially within the Earth's atmosphere. They follow predictable flight paths and are well-known in military operations.

2. Hyper-glide vehicles (HGVs) (wave-riders): These unpowered vehicles are launched to high altitudes (around 100 km) using rockets and then glide at hypersonic speeds (over Mach 8) for long distances by utilizing the wave-riding effect. HGVs have the ability to maneuver during flight, making their trajectory unpredictable compared to exo-atmospheric ballistic missiles. They are designed to operate at high altitudes where rarefied gas conditions prevail.

3. Hypersonic cruise missiles: This type of hypersonic vehicle is powered by

[59] "Asking the Right Questions about Conventional Prompt Global Strike", *Carnegie Endowment for International Peace*, 2013; https://carnegieendowment.org/files/cpgs.pdf

[60] R.H. Speier, et al., "Hypersonic Missile Nonproliferation: Hindering the Spread of a New Class of Weapons", *RAND Corporation*, Santa Monica, CA, 2017.

[61] H.-L. Besser, D. Goege, M. Huggins, A. Shaffer, D. Zimper, "Hypersonic Vehicles; Game Changers for Future Warfare?", *JAPCC 24*, 2017 (Transformation & Capabilities).

scramjet engines, known as Supersonic Combustion Ramjets (SCRJ). In scramjet engines, the flow remains supersonic throughout the engine, which has no rotating parts, and combustion occurs under supersonic conditions. These missiles operate at speeds around Mach 5, where the scramjet engine exhibits maximum efficiency. They fly at lower altitudes as their air-breathing engine requires high-density air for combustion.

The development and utilization of hypersonic vehicles represent a significant advancement in military technology, offering new possibilities for future military operations.

Main Developers

In the global race for the development of hypersonic vehicles, several major and secondary countries are actively involved. The major countries leading in this field include the United States, Russia, China, and India. Secondary countries that are also engaged in hypersonic research and development include Iran and North Korea. Additionally, countries like Australia, Japan, France, the United Kingdom, and Germany are conducting extensive scientific research on hypersonic flight. Among the major countries, the United States currently has the most well-known hypersonic programs. While there is some publicly available information about these programs, specific technical details such as vehicle geometry, materials used, and booster specifications are generally kept proprietary.

One notable hypersonic program developed by the United States is the OPERATIONAL FIRES (OpFIRES) system (*Figure 1*). This ground-launched system utilizes a hypersonic boost glide missile to penetrate enemy air defenses and engage time-sensitive targets rapidly. The OpFIRES program is a collaboration between the Defense Advanced Research Project Agency (DARPA) and Lockheed Martin[62] [63]. The system employs a hypersonic glide vehicle that glides through the upper atmosphere before descending to strike its intended target. In July 2022, the OpFIRES system successfully conducted a test flight, although specific details regarding the flight duration and maximum altitude achieved have not been disclosed [63].

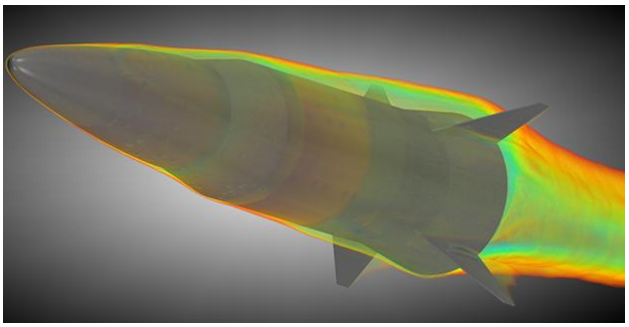


Figure 1. *Overview of OpFIRES (DARPA).*

The Boeing X-51 Waverider (*Figure 2*) is an unmanned hypersonic research platform that was specifically developed as a demonstration vehicle to showcase the operation of a scramjet engine within the Mach 4.5 to 6 speed range[64]. The X-51 conducted a series of test flights spanning

[62] Lockheed Martin, "Lockheed Martin's Hypersonic OpFires Missile Has Medium Range Covered"; https://www.lockheed-martin.com/en-us/news/features/2020/lockheed-martins-hypersonic-opfires-missile-has-medium-range-covered.html

[63] DARPA, "Operational Fires Program Successfully Completes First Flight Test"; https://www.darpa.mil/news-events/2022-07-13a#:~:text=The%20OpFires%20system%20achieved%20all,to%20initiate%20the%20test%20mission

[64] U.S. Air Force, "Propulsion Directorate Monthly Accomplishment Report"; https://web.archive.org/web/20061212072043/http://www.pr.afrl.af.mil/mar/2005/sep2005.pdf.

from 2010 to 2013. Notably, its final flight holds the record for the longest flight achieved by a scramjet engine thus far[65] [66].

Figure 2. *Boeing X-51A Waverider (adopted from af.mil).*

The Southern Cross Integrated Flight Research Experiment (SCIFiRE) shown in *Figure 3* is the result of a collaboration between the United States and Australia, spanning more than 15 years. This hypersonic vehicle is equipped with an air-breathing scramjet engine and is designed to achieve speeds of Mach 5. It is anticipated that SCIFiRE will be operational and in service within the next 5 to 10 years[67].

Figure 3. *Overview of the SCIFiRE aircraft (image obtained from the-riotact.com).*

The US Army is currently developing the Long-Range Hypersonic Weapon (LRHW), a surface-to-surface hypersonic missile. This ballistic missile shown in *Figure 4* is designed to accelerate the Common Hypersonic Glide Body (C-HGB) warhead to speeds up to Mach 5. It has the capability to be launched from both land and sea platforms. Two tests have been conducted so far, one in October 2017 and another in March 2020[68].

Figure 4: *LRHW system overview (adopted from navalnews.com).*

The Advanced Hypersonic Weapon (AHW) is a hypersonic glide vehicle designed to fly within the Earth's atmosphere at hypersonic speeds (*Figure 5*). It has a range of 6000 km and a flight duration of 35 minutes. In November 2011, the AHW was launched from the Pacific Missile Range Facility (PMRF) in Hawaii and successfully hit a target located approximately 3700 km away at the Reagan Test Site on the Marshall Islands. The test aimed to demonstrate the capabilities of hypersonic boost-glide technologies and assess long-range atmospheric flight[69].

[65] FlightGlobal, "August failure of Boeing X-51 likely due to fin, resonance"; https://web.archive.org/web/20161014135102/http://www.flightglobal.com/news/articles/august-failure-of-boeing-x-51-likely-due-to-fin-resonance-378080/.

[66] Boeing, "Boeing X-51A WaveRider Sets Record with Successful 4th Flight", May 3, 2013; https://boeing.mediaroom.com/2013-05-03-Boeing-X-51A-WaveRider-Sets-Record-with-Successful-4th-Flight

[67] L. Kay, "Boeing, Lockheed Win SCIFiRE Hypersonic Weapons Preliminary Design Contracts", Defence World; https://www.defenseworld.net/2021/09/02/boeing-lockheed-win-scifire-hypersonic-weapons-preliminary-design-contracts.html.

[68] S.J. Freedberg Jr, "Hypersonics: Army, Navy Test Common Glide Body", *Breaking Defence Magazine*, March 20, 2020; https://breakingdefense.com/2020/03/hypersonics-army-navy-test-common-glide-body/.

[69] Army Technology, "Advanced Hypersonic Weapon (AHW)", April 10, 2012; https://www.army-technology.com/projects/advanced-hypersonic-weapon-ahw/.

Figure 5: *Advanced Hypersonic Weapon (AHW) (image obtained from wired.com).*

The Hypersonic Air-breathing Weapon Concept (HAWC) program focuses on developing and demonstrating critical technologies for an air-launched hypersonic cruise missile presented in *Figure 6*. This kinetic energy weapon does not have an explosive warhead. Successful flights have been conducted, with at least three tests completed by September 2021. In a test performed on July 18, 2022, the HAWC achieved a speed of Mach 5 at an altitude of 18 km, covering a distance of over 300 nautical miles[70].

Figure 6: *Render view of the HAWC concept (Image credit: Northrop Grumman).*

The HTV-3X vehicle (*Figure 7*), also known as the Blackswift, was a project based on DARPA's HTV-2. It aimed to develop a reusable Hypersonic Cruise Vehicle, an unmanned aircraft capable of taking off from a conventional runway and delivering a payload of 5400 kg to targets up to 16,650 km away. The Blackswift flight demonstration vehicle was intended to be powered by a hybrid engine, combining a turbojet and a ramjet. However, the HTV-3X did not receive further funding and was canceled in October 2009[71].

Figure 7: *Model of the HTV-3X (Image credit: wired.com).*

Limited information is available about the Lockheed Martin SR-72, nicknamed "Son of Blackbird." This vehicle is expected to have a top speed exceeding Mach 6 and is primarily intended for surveillance, intelligence, and reconnaissance purposes. Lockheed Martin announced in November 2018 that a prototype of the SR-72 was scheduled to fly by 2025[72]. The SR-72 will be similar in size to the SR-71, with a length of over 30 m and a comparable range. It is anticipated to enter service around 2030.

Figure 8: *Lockheed Martin AGM-183 Air-Launched Rapid Response Weapon (ARRW) (Images credit: airandspaceforces.com, Lockheed Martin).*

[70] DARPA, "Third Test Flight for DARPA's HAWC Yields New Performance Data", July 18, 2022; https://www.darpa.mil/news-events/2022-07-18.

[71] G. Little, "Mach 20 or Bust, Weapons research may yet produce a true spaceplane", *Air & Space Magazine*, January 1, 2013; https://www.smithsonianmag.com/air-space-magazine/mach-20-or-bust-20679807/.

[72] "SR-72 Hypersonic Demonstrator Aircraft", *Airforce Technology*, 30 January, 2014; https://www.airforce-technology.com/projects/sr-72-hypersonic-demonstrator-aircraft/.

The AGM-183A Air-Launched Rapid Response Weapon (ARRW), developed by Lockheed Martin for the US Air Force (USAF), is another hypersonic missile system (*Figure 8*). It is designed to have a maximum speed exceeding Mach 5[73] and an operational range of approximately 1,600 km. The ARRW utilizes a boost-glide system, where it is initially propelled to hypersonic speeds by a rocket before gliding towards its target. Several tests have been conducted for the AGM-183A, although some have encountered technical issues. The first successful test occurred on May 14, 2022, demonstrating the weapon's separation capability from a B-52H Stratofortress[73]. The USAF conducted subsequent successful tests on July 12, 2022, and December 9, 2022[73]. The December test involved a fully operational prototype, showcasing the essential functionality of the complete AGM-183A vehicle. These successful tests position the AGM-183A to potentially become the first operational air-launched hypersonic weapon in the US inventory.

Figure 9: *Perspective view of the HTV-2 vehicle (Image credit: Wikipedia).*

The Hypersonic Technology Vehicle 2 (HTV-2) is an experimental gliding vehicle and an unmanned rocket-launched maneuverable vehicle developed as part of the DARPA Falcon project (*Figure 9*). It served as a predecessor to the HTV-3X. The HTV-2 was designed to reach speeds in the Mach 20 range and cover a distance of 17,000 km in 49 minutes. Two flight tests have been reported for the HTV-2. The first test took place on April 22, 2010, during which the vehicle flew a distance of 7,700 km over the Pacific Ocean at a speed of Mach 20 and an altitude of 160 km[74].

However, communication with the vehicle was lost 9 minutes after launch. A second flight test occurred on August 11, 2011, but contact with the vehicle was again lost 9 minutes after launch, resulting in the autopilot terminating the flight abruptly[75]. A summary of all known US hypersonic programs can be seen in *Table 1*.

[73] Air & Space Forces, "AGM-183 ARRW", May 17, 2022; https://www.airandspaceforces.com/weapons-platfoms/agm-183-arrw/.

[74] G. Little, "Mach 20 or Bust, Weapons research may yet produce a true spaceplane", *Air & Space Magazine*, January 1, 2013; https://www.smithsonianmag.com/air-space-magazine/mach-20-or-bust-20679807/.

[75] "DefenceTalk, Hypersonic Vehicle Advances Technical Knowledge", *DefenceTalk.com*, 11 August 2011; https://www.defencetalk.com/darpa-hypersonic-vehicle-advances-technical-knowledge-36347/.

USA					
Project Name	**Organization**	**Type**	**Speed (Mach)**	**Expected date to service**	**Status**
OPERATIONAL FIRES (OpFIRES)	DARPA	Hypersonic glide missile	5	-	Under development
BOEING X-51 WAVERIDER	Defence Advanced Research Project Agency (DARPA)	Unmanned research experimental aircraft	5	-	Under development
Southern Cross Intergrated Flight Research Experiment (SCIFIRE)	USA/Australia	Hypersonic Cruise missile	5	Before 2030	Under development
Long Range Hypersonic Weapon (LRHW)	United States Army	ICBM	5	Before 2023	Under development
Advanced Hypersonic Weapon (AHW)	US Army Space and Missile Defence Command (USASMDC) / Army Forces Strategic Command (ARSTRAT)	Hypersonic Glide Vehicle (HGV)	5+	Before 2025	Under development
Hypersonic Air-Breathing Weapon Concept (HAWC)	DARPA	Hypersonic Cruise Missile	5+	Before 2025	Under development
Hypersonic Technology Vehicle HTV-3X	USAF	Hypersonic Glide Vehicle (HGV)	5-10	-	Cancelled
SR-72 Blackbird	Lockheed Martin	Hypersonic Reconnaissance UAV	6	Before 2030	Under development
AGM-183 Rapid Response Weapon (ARRW)	Lockheed Martin	Hypersonic air-to-ground missile - glide vehicle	5+	Before 2025	Under development
Hypersonic Technology Vehicle HTV-2	DARPA	Hypersonic glide Vehicle	20+	Before 2025	Cancelled

Table 1. *A summary of known US hypersonic programs.*

Limited information is available to the public regarding the Russian hypersonic programs, and caution should be exercised when considering the available information. Currently, two Russian hypersonic missiles are known: the Kh-72M2 (Kinzhal) and the Avangard. The Kh-72M2 (Kinzhal) missile is reported to have a range of over 2,000 km and a speed of Mach 10. It has the capability to carry both conventional and nuclear warheads. The missile can be launched from bombers or other military aircraft and operates at a maximum altitude of 20 km. The Kinzhal project commenced in December 2017, and in November 2019, the first launch of the Kinzhal missile took place, successfully hitting a ground target at Mach 10 speed according to the Russian News Agency. The Kinzhal missile utilizes a conventional rocket engine with solid propellant fuel. It has dimensions of approximately 8 m in length, 1 m in diameter, and weighs around 4,300 kg[76]. The Kinzhal missile has reportedly been used by Russia in the conflict with Ukraine[77]. On the other hand, the Avangard is a hypersonic gliding vehicle designed with maneuvering capabilities.

[76] MISILETHREAT, "Kh-47M2 Kinzhal", March 19, 2022; https://missilethreat.csis.org/missile/kinzhal/.

[77] D.J. Judd, "Biden confirms Russia's use of hypersonic missiles in Ukraine", *CNN*, March 22, 2022; https://edition.cnn.com/europe/live-news/ukraine-russia-putin-news-03-21-22/h_38fe9317803ffd4f7cafe92e6bb53c1c.

Specific details about its propulsion system are not publicly known. It is claimed to achieve speeds of Mach 20-27, although there are concerns and doubts regarding the actual performance of the vehicle[78].

India has undertaken its own hypersonic program, dedicated to the development of the BrahMos missile platform. BrahMos Aerospace is responsible for the platform's development, which includes various variants capable of launching from mobile launchers as well as ships. The hypersonic iteration of this platform is referred to as BrahMos-II. As of now, no operational prototypes of BrahMos-II have been deployed. However, BrahMos Aerospace has expressed its intention to commence testing of the missile by 2024. The projected specifications for BrahMos-II include an estimated range of approximately 290 km and a speed surpassing Mach 6[79]. Further details regarding the platform have not been disclosed publicly to date. The country has also recently announced the development of another hypersonic platform named Shaurya. This particular platform is a nuclear-capable hypersonic missile designed for surface-to-surface engagements. It boasts a range of 750 km and can attain speeds of Mach 7.5. Shaurya is a two-stage missile employing solid propellant. With a weight of around 6 tons, it has the capacity to carry nuclear as well as conventional payloads weighing up to 1 ton. It's important to note that the provided information is based on the available public knowledge.

Limited information is available regarding China's hypersonic program. Since 2014, China has been engaged in the development of a hypersonic missile known as the DF-17. The DF-17 prototype incorporates the booster technology used in the DF-16, a short-range ballistic missile. This vehicle employs a two-stage solid rocket to propel it into the outer atmosphere and is capable of carrying nuclear or conventional warheads with a range estimated between 1800 and 2500 km. A test launch of the DF-17 missile occurred on November 1, 2017. During the test, the missile traveled approximately 1400 km before initiating its hypersonic glide phase at an altitude of 60 km. At this altitude, the glide vehicle separated from the boosters and continued its flight trajectory towards the intended target. The overall duration of the test flight was approximately 11 minutes[80].

Propulsion systems

To achieve hypersonic speeds, propulsion systems that differ from conventional ones are required. Conventional turbojet engines utilize mechanical compression in the inlet, driven by a downstream turbine, to achieve a certain level of airstream compression. However, turbojets typically have a maximum achievable Mach number of around 3.5, as this limit is dictated by the maximum temperature that turbine blades can withstand. Ramjets, on the other hand, rely on the inherent compression that occurs when capturing and decelerating a supersonic airstream to subsonic speeds,

[78] N. Novichkov, "Russia announces successful flight test of Avangard hypersonic glide vehicle", *Janes.com*, January 3, 2019; https://www.janes.com/defence-news/news-detail/russia-announces-successful-flight-test-of-avangard-hypersonic-glide-vehicle

[79] Hindustan Times, "India successfully tests nuclear-capable Shaurya missile", October 3, 2020; https://www.hindustantimes.com/india-news/india-successfully-tests-nuclear-capable-shaurya-missile/story-fkY-lozVJ5oq1MWO26GOwNN.html.

[80] A. Panda, "Introducing the DF-17: China's Newly Tested Ballistic Missile Armed with a Hypersonic Glide Vehicle", *The Diplomat*, December 28, 2017; https://thediplomat.com/2017/12/introducing-the-df-17-chinas-newly-tested-ballistic-missile-armed-with-a-hypersonic-glide-vehicle/.

where combustion takes place. To operate efficiently, ramjets generally require a minimum supersonic speed to be maintained. Scramjets, similar to ramjets, capture the incoming airstream, but instead of slowing it down to subsonic speeds, they further compress it at the inlet and allow combustion to take place at supersonic velocities. This enables scramjets to operate at even higher speeds within the hypersonic regime[81].

Both ramjets and scramjets are capable of operating at supersonic and hypersonic speeds. However, the ramjet encounters challenges when operating at speeds exceeding Mach 5 due to the inefficiencies associated with decelerating the airflow to subsonic speeds. Scramjets, on the other hand, are optimized for speeds above Mach 5 and offer improved performance within the hypersonic regime. Both types of engines rely on a booster to accelerate the vehicle to the operating speed of the engine[82]. To achieve hypersonic velocities, it is crucial for the vehicle to be as lightweight as possible. Scramjets are particularly well-suited for hypersonic vehicles as they eliminate the need for an oxidizer fuel tank, which would contribute to the vehicle's weight. Instead, scramjets extract oxygen from the atmosphere, resulting in significant weight savings; however, the utilization of atmospheric oxygen poses an upper ceiling for their flight envelop, due to the air density decrease with altitude. A schematic of a hybrid scramjet and ramjet engine is depicted in *Figure 10*.

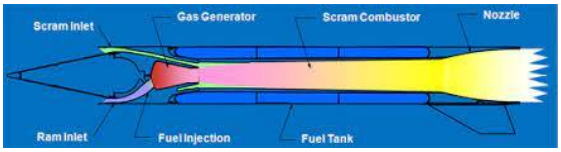


Figure 10: Schematic of a scramjet jet engine (adopted from Aerojet Rocketdyne).

Surveillance methods

Hypersonic missiles pose significant challenges in terms of tracking and detection. Their combination of high maneuverability, unpredictable trajectory and very high speed renders extremely difficult the identification of their target until the last moment. Existing interception systems are primarily designed for intercepting ballistic objects, such as ICBMs, which follow predictable paths based on momentum and gravity. Hypersonic gliding vehicles, on the other hand, operate in a fundamentally different manner. Launched by a ballistic missile, they become unpowered after separation; instead of following a predictable ballistic trajectory, like traditional reentry vehicles, they descend back into the atmosphere. During this phase, they experience both drag, which slows them down, and aerodynamic lift, which allows them to glide and counterbalance their weight. As a result, they can cover distances comparable to or even greater than a warhead on a ballistic trajectory launched with the same booster. One advantage of this trajectory is that hypersonic gliding vehicles maintain a lower altitude, typically ranging from 30 km to 100 km. This proximity to the ground makes them harder to detect from surface-based sensors, as conventional radar and optical systems face limitations due to Erath's curvature. Therefore, such vehicles

[81] R.S. Fry, "A Century of Ramjet Propulsion Technology Evolution", *Journal of Propulsion and Power*, 20(1), pp. 27-58, 2004.

[82] V. Amati et al., "Exergy analysis of hypersonic propulsion systems: Performance comparison of two different scramjet configurations at cruise conditions", *Energy*, vol. 33(2), pp. 116-129, 2008.

can approach their target with minimal detection until the final stages, significantly complicating defensive measures. For hypersonic cruise missiles, flying at even lower altitudes, the challenges become even more pronounced. Current surveillance systems are generally divided into two main categories: geostationary constellations and low-orbit systems.

The MIDAS system, deployed by the Defense Support Program (DSP) in the United States, was the first of its kind. Launched in 1970, it consisted of a constellation of typically three primary and three backup satellites in geostationary orbit. This orbital configuration provided a constant view of one-third of the globe to each satellite, enabling easier detection of transient infrared events and ensuring continuous operational capability. The Soviet Union developed a similar system called Oko (Eye), launched in 1972. However, Oko used Molnya orbits instead of geostationary orbits, resulting in a longer timeframe for achieving operational readiness. After approximately 30 years of service, the MIDAS system was eventually replaced by the Space-Based Infra-Red System (SBIRS). SBIRS also operates in geostationary orbit and incorporates infrared sensors carried by US signal intelligence satellites in Molnya orbits to enhance polar coverage[83].

While SBIRS possesses exceptional capabilities, they have their limitations. The system can only detect missiles when their engines are firing, which is a relatively brief phase of their flight. For the majority of their trajectory, the vehicles, along with their boosters, operate passively or make minor course adjustments, resulting in minimal heat signatures. This renders them indistinguishable from the background thermal emissions, making them visible to satellites only when they are above the Earth's horizon[84].

In addition to the challenges of detecting hypersonic missiles, another significant hurdle is distinguishing between the actual threat and the decoys that are often deployed alongside the real weapons. Decoys are designed to have similar radar signatures to the actual missiles, making it difficult to differentiate between them. Detecting subtle differences in the infrared signatures of these small objects is a task that is best accomplished by satellites positioned relatively close to the Earth. Originally, the Space-Based Infra-Red System (SBIRS) had plans for a low-orbit component that would handle midcourse tracking and discrimination. However, these plans were scaled back, and only two proof-of-concept satellites, known as the Space Tracking and Surveillance System (STSS), were launched in 2009 to test and evaluate the concept[85].

The United States is currently in the planning phase for a new constellation of satellites positioned in lower orbits, which will have the capability to detect and track missiles from their launch phase to their terminal phase. This system will serve as the foundational element of a future integrated system combining missile warning, missile tracking, and missile defense, which is not currently available. These

[83] J.T. Richelson, "America's Space Sentinels: The History of the DSP and SBIRS Satellite Systems".

[84] US National Academies of Sciences, "Making Sense of Ballistic Missile Defense", 2012; https://nap.nationalacademies.org/catalog/13189/making-sense-of-ballistic-missile-defense-an-assessment-of-concepts.

[85] StelliteObservation.net, "Detecting hypersonics", November 15, 2018.

satellites will provide the initial capabilities for missile warning and missile tracking within the future National Defense Space Architecture (NDSA). The project entails the development of two distinct infrared satellite constellations positioned in different orbital layers, along with the corresponding ground facilities. The U.S. Space Development Agency (SDA) and the Space Force's Space Systems Command (SSC) have been assigned separate responsibilities for each layer of missile-tracking satellites. The SDA will oversee the constellation deployment in low-Earth orbit (LEO), while the SSC will be responsible for the constellation in medium-Earth orbit (MEO).

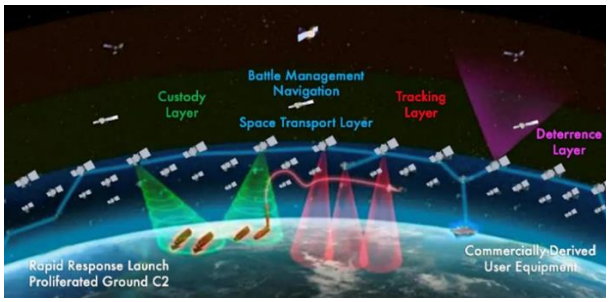


Figure 11*: *Overview of the Tranche 0 tracking layer (adopted from U.S. DoD).

The constellation developed by the U.S. Space Development Agency (SDA) consists of two layers: the Transport Layer and the Tracking Layer[86]. The Transport Layer focuses on providing reliable and secure military data and connectivity worldwide for various warfighter platforms. It is designed to have 300 to over 500 satellites positioned in low-Earth orbit (LEO), at altitudes ranging from 750 kilometers to 1,200 kilometers. The Tracking Layer, on the other hand, aims to deliver global indications, warnings, tracking, and targeting capabilities for advanced missile threats, including hypersonic missile systems. To achieve this, a large constellation of distributed, cost-effective, small satellites will be deployed. This approach enhances responsiveness, flexibility, and resilience against potential enemy anti-satellite attacks. In addition to the SDA's constellation, the Space Systems Command (SSC) is developing a separate constellation of satellites that will operate at higher altitudes in medium-Earth orbit (MEO), specifically around 10,000 to 20,000 kilometers. By positioning these satellites at greater distances, they become more difficult to target with ground-launched anti-satellite weapons, adding to the overall resilience of the system[86].

In the development of the Tracking Layer for the early warning constellation, two companies, SpaceX and L3Harris, have been awarded contracts to construct the "Tranche 0" proof-of-concept satellites (*Figure 11*). These satellites are scheduled to be launched in 2023. For the subsequent phase, known as Tranche 1 (*Figure 12*), contracts have been awarded to L3Harris Technologies and Northrop Grumman Strategic Space Systems. Each contractor will be responsible for building 14 satellites equipped with wide field-of-view (WFOV) overhead persistent infrared (OPIR) sensors. These satellites will form part of the Tranche 1 component of the Tracking Layer. To support the operation and integration of the Tranche 1 Tracking Layer, additional contracts have been awarded to General Dynamics Mission Systems and Iridium. These contracts involve establishing the ground Operations and Integration (O&I) segment for the Tranche 1 satellites,

[86] H. Altman, "How the New Hypersonic Weapons Tracking Constellation Will Work", *The War Zone*, July 19, 2022; https://www.thedrive.com/the-war-zone/how-the-new-hypersonic-weapons-tracking-constellation-will-work.

ensuring smooth coordination and functioning of the overall system.

***Figure 12**: Overview of the Tranche 1 transport mesh satellite communications layer (adopted from U.S. DoD[87]).*

Conclusions

The ongoing development of hypersonic vehicles is driven by the potential advantages they offer, despite the significant costs associated with countering them. The ability to effectively survey, track, and intercept these weapons remains a challenge, and no nation currently possesses a fully integrated capability in this regard. However, various countries are working on developing key components to address these challenges. Two critical issues that arise in this context are the effectiveness of surveillance and the associated costs. It is necessary to find cost-effective solutions to neutralize the expensive hypersonic development programs pursued by potential adversaries. The future National Defense Space Architecture of the United States aims to tackle these challenges by establishing a decentralized, distributed, and interconnected system for efficient surveillance and tracking of hypersonic vehicles. This architecture serves as a potential model for other nations to follow. Key characteristics that such a system should possess include:

1. Comprehensive Surveillance: The system should have the capability to monitor and detect hypersonic vehicles across large areas, including early detection of launches and continuous tracking throughout their trajectory.
2. Rapid Response: It should enable quick response and timely decision-making by providing real-time data on the location, speed, and trajectory of hypersonic vehicles.
3. Multi-Source Data Fusion: The system should integrate data from various sources such as satellites, ground-based sensors, and airborne platforms to enhance situational awareness and accuracy.
4. Interoperability: It should allow for seamless communication and data sharing between different components of the system, including space-based assets, ground control stations, and interceptors.
5. Scalability and Resilience: The system should be designed to scale up or down as per operational requirements and possess resilience against disruptions or potential threats.
6. Cost-Effectiveness: The system should prioritize cost-effective solutions to counter hypersonic threats, ensuring the allocation of resources in an efficient manner.

By incorporating these characteristics, nations can work towards establishing an integrated surveillance and tracking system capable of effectively countering hypersonic vehicles and mitigating the associated risks. •

[87] A. Millier, "Tracking Hypersonics in Real Time", *Air & Space Forces Magazine*, April 29, 2022; https://www.airandspaceforces.com/article/tracking-hypersonics-in-real-time/.

The Implications of UAS to IAMD

By Andrew J. Bogusky, Lt Col, USAF

The unmanned aerial system (UAS) threat is not new. Only a decade after the Wright brothers' first flight, the U.S. developed the 'Kettering Bug,' a track-launched, unmanned "aerial torpedo" capable of striking ground targets up to 75 miles away.[88] In World War II, Germany produced the "world's first operational cruise missile," the V-1, which is not unlike the so-called 'kamikaze drones' that various actors employ today.[89] Simply put, the threat from UAS has been around for over a century. The major difference today, however, lies in the exponential proliferation of UAS and expansion in their capabilities. The increasing volume of attacks and the continued advancement of UAS technologies are exposing gaps in existing capabilities and approaches to integrated air and missile defense (IAMD). Because the problem is a layered one involving factors such as cost, proliferation, doctrine, and technology, the solution will likewise require a layered, interconnected, and comprehensive approach.

First a note on terminology. "UAS" will be used predominantly in this essay as a generic and encompassing term. It describes not only the aircraft or aerial vehicle, but also the logistical footprint involved such as command and control (C2), communications networks, and control stations potentially involved to employ such a system. The term remotely piloted aircraft systems (RPAS) typically refers to the larger, more exquisite types of UAS, for example the MQ-9 Reaper or RQ-4 Global Hawk. "Drones" occupy the other side of the spectrum, usually referring to smaller systems such as quadcopters or other hand-held or hand-launched aircraft. Categorization of UAS (e.g. groups 1-5 UAS, cruise missiles) is an entirely different matter and beyond the scope of this essay.

Since this paper addresses the implications of UAS on IAMD, it is appropriate to also briefly define and describe IAMD:

> *IAMD is an approach that synchronizes aspects of counterair with global missile defense (MD), homeland defense (HD), global strike, and defense against indirect fires (IDFs)… Advancing technology and the proliferation of aircraft and missiles have expanded the scope and complexity of protecting friendly forces and vital interests.*[90]
>
> and
>
> *(1) IAMD is evolving since it is driven by capabilities, which constantly change; (2) it is explicitly integrated and inherently joint, drawing upon the capabilities of each service to*

[88] National Museum of the United States Air Force. "Kettering Aerial Torpedo 'Bug.'" https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/198095/kettering-aerial-torpedo-bug/ (accessed 8 May 2023).

[89] National Air and Space Museum. "V-1 Cruise Missile." https://airandspace.si.edu/collection-objects/v-1-cruise-missile/nasm_A19600341000 (accessed 8 May 2023).

[90] The Joint Staff. *Joint Publication 3-01: Countering Air and Missile Threats*. April 2023.

produce the desired effects; and (3) because it seeks to gain and maintain our access and the ability to operate, IAMD helps us counter A2/AD strategies.[91]

These descriptions of IAMD are especially relevant because they acknowledge that IAMD must adapt to evolving threats, such as UAS. The UAS threat as we know it today has proven to separate itself from other air-based threats due three primary factors or characteristics: their low cost, increasing employment, and exponential development. These factors are interrelated and contribute to the main implications to IAMD which are: cost-effectiveness, proliferation, and detection and interception. Overall, these lead to the outpacing of current IAMD capabilities and doctrine and necessitate continuous evolution in IAMD apace with the threat.

Cost is a Double-Edged Sword

UAS' relatively low cost is captured not only in material terms, but also in human terms. In other words, UAS typically cost less per unit than traditional aircraft, but they can be thought of as 'expendable' or 'attritable' because the human pilot is not at risk in the same way as in a traditional aircraft. Some 'single-use,' so-called "kamikaze drones," and 'loitering munitions' are even designed for one-time use. Besides the lower human risk, or perhaps because of it, there is less strategic and operational risk. The absence of the human element results in less risk for escalation and a higher threshold for provocation—for example, when dealing with incursions into sovereign airspace, or if a UAS gets shot down.[92] The United States' response to Russia for the downing of the MQ-9 in the Black Sea in March 2023 would probably have been different if a manned aircraft had crashed.

The other edge of UAS' low-cost sword, and its implication for IAMD, is represented by cost-effectiveness, or the 'cost-exchange' required to defeat the UAS threat. In many instances, this transaction represents a highly uneven exchange whereby the defender is expending much more than the attacker. Consider the case of the $3 million Patriot missile used to shoot down a $200 drone from Amazon in 2017.[93] Or more recently, when the United States used a $400,000 AIM-9X Sidewinder missile to shoot down a low-tech Chinese spy balloon.[94] This is the equivalent of using a shotgun to kill a fly instead of a fly swatter. These examples show that modern IAMD systems and munitions are designed for high-value targets, and that "large numbers or a swarm of low-cost UAS may quickly turn the cost-benefit ratio of traditional AMD upside down and render current systems inefficient."[95] The cost exchange dilemma is not limited to decisions made during each tactical engagement,

[91] Kenneth R. Dorner, Maj William B. Hartman, and Maj Jason M. Teague. "Back to the Future: Integrated Air and Missile Defense in the Pacific" *Air & Space Power Journal*, Jan-Feb 2015 https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-29_Issue-1/V-Dorner_Hartman_Teague.pdf (accessed 24 Apr 2023).

[92] Lt Col Andre Haider. "Unmanned Aircraft System Threat Vectors." https://www.japcc.org/chapters/c-uas-unmanned-aircraft-system-threat-vectors/ (accessed 24 Apr 2023).

[93] Christopher Woody. "An Ally Used a $3M Patriot Missile to Shoot Down a $200 Drone, According to this General." *Task & Purpose*, https://taskandpurpose.com/tech-tactics/ally-used-3m-patriot-missile-shoot-200-drone-according-general/ (accessed 3 May 2023)

[94] Low de Wei and Bloomberg. "Meet the Sidewinder—the $400,000 missile of choice for shooting down suspected Chinese spy balloons and mystery UFOs." *Fortune*, https://fortune.com/2023/02/13/sidewinder-missile-china-spy-balloon-ufo-raytheon/ (accessed 3 May 2023).

[95] Andre Haider, "A Comprehensive Approach to Countering Unmanned Aircraft Systems and Why Current Initiatives Fall Short" https://www.japcc.org/flyers/a-comprehensive-approach-to-countering-unmanned-aircraft-systems (accessed 1 May 2023)

but also applies broadly to national defense budgets. When the so-called Chinese spy balloon revealed gaps in American IAMD, the incident prompted $90 million in additional air defense spending.[96]

Horizontal and Vertical Proliferation

UAS represent a technology that meets perfectly at the intersection of low cost and high capability; this combination has resulted in an explosive proliferation in the horizontal and vertical planes. As mentioned, the low material, human, and risk-cost encourages increased procurement and use of UAS. Not only is employment boosted in terms of numbers of UAS, but also in the frequency of use and in the will of the actor. The horizontal proliferation of UAS means that no longer do superpowers or developed countries hold a monopoly on airpower, but states of all levels of development and even non-state actors can employ airpower through UAS to hold others at risk and even challenge air superiority. Vertical proliferation refers to the development and use of UAS which stretches from tactical micro-drones to exquisite and large, strategic RPAS, and everything in between.[97]

UAS has enabled the democratization of air power, which has already produced fundamental changes to long-standing air power doctrine. For example, in the current war in Ukraine, US Air Force leaders such as Lieutenant General Hinote have noted a shift from air control or air superiority to a strategy of 'air denial;' denying the use of airspace for all is far easier than controlling it.[98] General James Hecker noted, "One of the things that we see is the lack of either side, whether it be the Russian or Ukrainians, the ability to get air superiority, has really changed this into a different fight that we haven't seen in quite a while…The number one priority to make sure that we're able to get air superiority is to make sure that we can do the counter [integrated air defense systems] mission."[99]

Beyond brute force attacks, Russia is using UAS also as decoys to lure Ukrainian air defenses to switch on in an effort to find and target them. This in turn has reportedly led to a ban on Ukrainian use of air defense systems unless in a case of a mass attack by Russian aircraft.[100]

Detection and Interception

Although UAS typically fly at relatively low altitudes and speeds, which should make them theoretically easier to defeat through offensive or defensive means, they also exhibit low radar, infrared (IR), and visual signatures. For example, in the 2020 Nagorno-Karabakh war, the relatively low and slow Bayraktar TB2 (Turkish produced medium-altitude long-endurance [MALE] UAS) escaped detection by Armenia's Soviet-era radars and surface-to-air missiles (SAMs) which were

[96] Chris Gordon. "Chinese Spy Balloon Prompts $90 Million in New Air Defense Spending." *Air and Space Forces Magazine.* https://www.airandspaceforces.com/chinese-spy-balloon-new-air-defense-spending/ (accessed 15 April, 2023).
[97] Paul van Hooft and Lotje Boswinkel. "Surviving the Deadly Skies Integrated Air and Missile Defence 2021-2035." https://hcss.nl/wp-content/uploads/2021/12/Integrated-Air-and-Missile-Defense-HCSS-Dec-2021.pdf (accessed 24 Apr 2023)
[98] Aidan Poling. "Airpower after Ukraine: The future of air warfare." *Atlantic Council*, September 6, 2022. https://www.atlanticcouncil.org/event/the-future-of-air-warfare/ (accessed 15 May 2023).
[99] Chris Gordon. "Lack of Airpower in Ukraine Proves Value of Air Superiority, NATO Air Boss Says." *Air and Space Forces Magazine,* March 22, 2023. https://www.airandspaceforces.com/airpower-ukraine-air-superiority-hecker/ (accessed 15 May 2023).
[100] Parth Satam. "Russia's 'Bait & Hit' Strategy Out! Reports Claim Iskander & Kalibr Missiles Lure Ukraine's Air Defense, While Kh-31 Strikes Them." December 3, 2022. https://eurasiantimes.com/russias-bait-hit-strategy-out-reports-say-iskander-kalibr-missiles/?amp (accessed 11 May 2023).

best suited against traditional, faster fighters.[101]

Detection will only worsen as technology and tactics—or both—adapt to outpace defenses. Technologically, stealth or low-observable (LO) technologies will only become more prevalent features of UAS, along with increasing capabilities on even smaller platforms. Even if detection is possible, interception presents an issue with continually advancing technologies and tactics such as swarming and artificial intelligence (AI) or machine learning (ML). These technologies and tactics will likely be employed in the whole spectrum of small-to-large UAS, and tactical-to-operational environments—from swarms of quadcopters to formations of collaborative combat aircraft (CCA) serving as 'uncrewed wingmen' to next generation fighters to capitalize on the principle of mass to overwhelm air defenses. The Secretary of the US Air Force Frank Kendall recently announced plans to acquire 1,000 CCA, which signifies a formal acknowledgement to the changing character of air power and the role of UAS.[102]

The Proliferation and Advances in UAS are Outpacing Current IAMD Capabilities and Doctrine

The sum of these implications—cost, proliferation, and detection/interception difficulties—results in an overall effect that the current IAMD paradigm is ill-equipped to address this growing threat. This applies not just to the technological challenges, but also to gaps in organizational and doctrinal capabilities of IAMD. The relatively low cost of UAS means it is unsustainable to rely on traditional defenses. Lower cost and lower risk also lead to explosive proliferation in numbers and in employment. The vast numbers of UAS and unique characteristics leads to novel tactics and uses such as loitering munitions and swarms, all potentially enhanced by AI or autonomous technology.

These issues are highlighted especially in a NATO/European context, where IAMD was designed to for Warsaw Pact threats moving from predictable locations and speeds, and "they were pertinently not designed for slow-moving and potentially static threats such as intelligence, surveillance and reconnaissance (ISR) UAVs or loitering munitions."[103] Furthermore, many defense systems were reduced following the end of the Cold War. Moreover, there are various systems employed in Europe that are not well-integrated, if at all.[104]

These are not distinctly European issues, as some also believe the US military's "primary [air and missile defense] AMD gap is its obsolete command and control (C2) system."[105] And if the nations of NATO are expressing these concerns, we must assume the same problems will apply to its adversaries also—not only by logic but also from observation in recent conflicts such as in Ukraine, Syria, Libya, Israel and Iran, etc.

[101] Paul van Hooft and Lotje Boswinkel.
[102] Stephen Losey. "US Air Force wants drone wingmen to bring 'mass' airpower on a budget." *Air Force Times*. May 11, 2023. https://www.airforcetimes.com/unmanned/2023/05/11/us-air-force-wants-drone-wingmen-to-bring-mass-airpower-on-a-budget/ (accessed 15 May 2023).
[103] Paul van Hooft and Lotje Boswinkel.
[104] *Ibid.*
[105] Jeremiah Rozman. "Integrated Air and Missile Defense in Multi-Domain Operations." *The Association of the United States Army*. May 2020. https://www.ausa.org/sites/default/files/publications/SL-20-2-Integrated-Air-and-Missile-Defense-in-Multi-Domain-Operations.pdf (accessed 13 April 2023).

No Silver Bullet

A note of clarification: while the following solutions involve the counter-UAS (C-UAS) effort, this represents a limited view of the problem. To be sure, C-UAS capabilities should be pursued; however, these tend to be very specific, technologically reliant, tactical in nature, and not integrated within the greater IAMD infrastructure/network. Just as there are various implications of UAS to IAMD causing multiple dilemmas, the solution must involve several approaches. The scope of this paper limits an all-inclusive list of potential solutions and will mainly attempt to highlight the principles required. Another temptation is to think that the solution will be purely technological. But technology is only part of the solution, perhaps even the smallest portion. The bulk of the solution lies in changing our understanding and thinking of the UAS threat and formulating a comprehensive approach to dealing with this growing problem**.** Overall, the solutions should be: technological, cost-effective, layered, interconnected, and comprehensive.

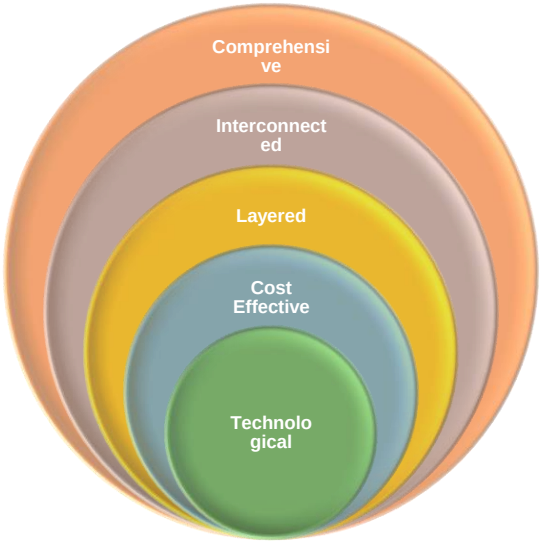


Figure 1. The principles of bolstering IAMD with respect to UAS

The technological aspect is a key component of the solution. One approach is to 'fight fire with fire.' For example, employing defensive swarms is a potential method to counter enemy offensive swarms.[106] We must leverage AI to mitigate AI-enabled weapons, as Admiral Stavridis explains, "America and its military are facing a major test when it comes to AI. The country that best incorporates artificial intelligence technology into its defense will have significant military advantages over its competitors."[107]

While technological improvements are needed, the solution must also be cost-effective. Effective, exquisite solutions already exist, but they are not cost-effective, efficient, or appropriate as previously discussed. Some cost-effective ideas needing further development include directed energy weapons (DEW) and electronic warfare (EW). Conversely, short-range and

[106] Paul van Hooft and Lotje Boswinkel.

[107] Adm. James Stavridis. Book review/commentary on *Four Battlegrounds: Power in the Age of AI* by Paul Scharre. May 2023.

even legacy anti-aircraft artillery (AAA) can continue to serve as existing, efficient, and effective components of IAMD with respect to UAS.[108]

The next three components of the IAMD solutions represent distinct concepts but are very much interrelated. The concept of a layered defense is certainly not new for AMD applications, but it needs to expand to meet the horizontal and vertical proliferation of the UAS threat. This will again involve technology, not only in terms of defense systems, but also in C2, so that the layers are interconnected. Various platforms, from tactical, point defenses to theater level defense of strategic targets, must be layered and interconnected by a C2 network that is efficient and interoperable. Overlap will inevitably occur, but we cannot afford gaps or seams.

Lastly, the IAMD solution must be comprehensive. Decision-makers will need to reassess IAMD with respect to the rising UAS threat when evaluating defense budgets. The fix cannot focus purely on technologically heavy C-UAS programs but must be addressed holistically. It's not only about 'shooting it down,' but just as important is detecting, identifying, and mitigating the advantage the UAS provides the enemy. This includes evaluating all parts of the UAS framework (e.g. control stations, cyber and satellite communication links, and the aircraft itself) and pursuing all of these attack surfaces in a combined, joint manner. This should include a coordinated effort from space capabilities, SOF, traditional AMD and counterair, down to the individual soldier equipped and trained to handle the various threats. Comprehensive by design also means addressing the UAS threat holistically with other air threats, and not as a specialized "C-UAS" function—which again, leads to stovepipes and tribes. The strict categorization of UAS and segregation from other air threats such as cruise missiles is arbitrary and counterproductive when it comes to a comprehensive view of IAMD.

Therefore, the strategic policy maker and tactical ground troop alike have roles to play in bolstering IAMD against UAS. In other words, the solutions require collaboration across many organizations and many sectors of the defense apparatus. The relatively small skirmishes of recent times have shown that militaries are unprepared for today's UAS threat, which is only growing and evolving. NATO and allied nations are arguably behind the power curve and should learn from these trends to anticipate and prepare for tomorrow's threats. •

[108] Haider.

Countering Unmanned Aircraft Systems "On-going efforts in NATO for C-UAS"

By Mr. Gabriele CASCONE

The widespread proliferation of Unmanned Aircraft Systems (UAS) poses a clear risk to civilian and military infrastructure, assets and people. The use of UAS capabilities by adversaries, both conventional forces and non-state actors, is rapidly increasing and evolving as demonstrated by recent conflicts, especially by Russia's war of aggression against Ukraine. In this context, both sides have used drones as a tactical technology for a range of missions, including Intelligence, Surveillance and Reconnaissance (ISR), direct fire, attack armoured vehicles and convoys, making UAS decisive for the development of the conflict.

Class I UASs are growing increasingly sophisticated, offering autonomous flight, high-end ISR capabilities, and ever-expanding payload capacity, range, and endurance. They are widely accessible to potentially disruptive actors and could be assembled using components without identifiable markings, thus increasing the difficulty of attribution if used in an attack.

Considering all these, it is worth to assume that, for the first time in a generation, a viable and deadly threat from hostile enemy airpower has emerged, making necessary to rethink the existing form of force deployment.

C-UAS technology is also becoming smarter. From the original stand-alone equipment, new systems are becoming more sophisticated, integrating and fusing different technologies, making use of innovative approaches such as machine learning, sensor fusion, cognitive and holographic radars and augmented reality.

NATO has been pursuing a dedicated Counter UAS (C-UAS) effort since 2019, led by the NATO C-UAS Working Group, the single forum that includes the required expertise from different communities within all Allied nations. The Group is looking holistically through the DOTMPLFI (Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities, Interoperability) spectrum to support Allies in developing solutions in this domain. In particular, the Group is currently looking at the following priorities:

· Development of NATO C-UAS strategic, doctrinal and tactical documents
· Threat Scan and Intelligence sharing
· Development of technical standards
· Demonstration of integration in Integrated Air and Missile Defence (IAMD)
· Demonstration of C-UAS / UTM integration
· Capability Development
· Awareness, education and training
· Research and Development and Innovation
· Tests and Exercises
· Procurement and Acquisitions
· Deployment
· Development of a NATO C-UAS Centre of Excellence concept. •

C-UAS GNSS Jamming

By Dr Cristian COMMAN

The work reported in this paper focuses on the use of an airborne jammer to disrupt autonomous navigation of Class I Unmanned Aircraft System (UAS) based on Global Navigation Satellite System (GNSS). The main use case for this study is represented by the GNSS 2x2 array antenna observed in Shahed SH-131 and SH-136 UASs. Theoretical analysis and experimental measurements were performed to support the investigation of using an airborne GNSS jammer against the Class I UAS. Open-source information about Shahed drones was used in this report only.

The theoretical analysis of the 2x2 array antenna system clearly indicates that the array can continuously neglect up to 3 (i.e., N-1) jammers, by software-based blocking of the received signals from the direction of perceived jammers. However, the resilience and effectiveness of the 2x2 antenna system do not only depend on the number of expected jammers. Theoretical modelling, supported with experiments, indicate that the system suffers a lack of accuracy in determining the direction of a jammer signal beyond 65 degree theta and 45 degree phi (angles measured from the normal to the array in two orthogonal plans). This corresponds to 35 degree in azimuth and 45 degree in elevation of the impinging signals towards the array. Due to a metal ground plate onto which the 2x2 array is mounted, the system might be less susceptible to jamming signals from the ground. Therefore, one or more jamming signals, coming obliquely from above within the azimuth and elevation range in which the nulling accuracy is lacking, might be able to challenge the nulling capacity of the array.

Abstract: Despite the speed and agility of drones in responding to potential incidents, they are also considered an important threat for critical infrastructures. Drone detection is highly complex and difficult, especially in urban environments and aerial warfare. Currently, drone detection technologies rely on dedicated high-cost transmitters. Nevertheless, passive radar systems (PRS) are becoming increasingly popular due to their low cost, low power consumption, and reduced susceptibility to electronic warfare. PRS rely on the detection and characterization of signals emitted by other sources, such as cellular networks, instead of a dedicated transmitter. Notably, the ever increasing deployment of 5G networks, which offer high-bandwidth, low-latency, and multiple-input-multiple-output capabilities, could enable the widespread use of PRS for drone surveillance in complex environments. Motivated by this, our work highlights the key concepts related with the development of a PRS for drones detection that learns and extracts meaningful patterns and relationships from large amount of 5G signals via properly designed machine learning models. The proposed approach enables classification and separation of drone reflected signals from other sources, as well identification of different drone types, whilst suppressing the effects of interference, cluttering, and low signal-to-noise ratio. Moreover, it can be directly used in passive radar systems where the illuminating signal duration and bandwidth are content-dependent and the radar resolution may vary significantly.

ML-Empowered Drone Passive Radar Using 5G Signals

By Dr George Tzagkarakis &
Dr Stefanos Papadakis

1. Introduction

Drones, also known as Unmanned Aerial Vehicles (UAVs), Miniature Pilotless Aircrafts, or Flying Mini Robots, are rapidly gaining popularity and breaking through traditional barriers in various industries. Despite being relatively new and not yet fully adopted, drones have already become essential tools in businesses and government organizations, revolutionizing areas that were stagnant or struggling. Whether it is enabling efficient deliveries during peak traffic, accessing remote military bases, or conducting surveillance, drones offer unparalleled capabilities in locations where human presence is limited or where timely and efficient performance is challenging. The military sector particularly highlights the widespread use of drones, serving purposes like target decoys, combat missions, research and development, and surveillance. The global market for military drones is projected to exceed $30

billion by 2029[109], reflecting their crucial role in military operations and the substantial investment involved. With their ability to minimize losses and enhance the execution of critical and time-sensitive missions, drones will continue to find diverse applications in military operations.

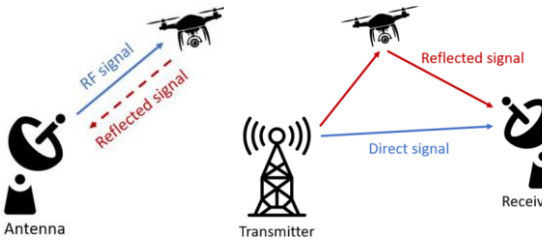
Designing drone detection radar systems (DDRS) for military operations is of utmost importance in today's rapidly evolving battlefield scenarios. With the ability of DDRS to detect and track drones in real time, military operators can gain valuable intelligence about enemy activities. As such, DDRS play a vital role in enhancing situational awareness on the battlefield, while their integration into existing military networks and command systems gives a more comprehensive picture enabling more proactive and responsive operations.

The proliferation of drones has presented new challenges and threats that traditional radar systems are ill equipped to handle. Specialized DDRS, specifically tailored for detecting, tracking, and countering drones, have become a crucial necessity for modern military forces. Another key challenge is the design of low-cost, versatile and scalable DDRS enabling real-time identification and accurate classification of an increasing variety of drones that come in various sizes, shapes, and flight characteristics.

Now is the right time to tackle all these challenges, towards designing the next-generation of DDRS. For this, we capitalize on commercially deployed ubiquitous telecommunication networks and state-of-the-art machine learning (ML) technologies that are able to extract meaningful information from big data volumes. Our vision is to design a software-defined DDRS, enabling easy upgrades and futureproofing, as soon as new hardware devices or computational intelligence models become available.

2. Active vs Passive Radar Systems

DDRS are roughly categorized into active radar systems (ARS) and passive radar systems (PRS). ARS (ref. Figure 1a) generate their own electromagnetic waves (transmitted pulses) and transmit them into the surrounding environment. These waves are then reflected by objects such as drones, and are detected by the radar receiver. The radar system measures the time delay, frequency shift (Doppler effect), and amplitude of the received signals to determine the range, velocity, and direction of the targets. On the other hand, PRS (ref. Figure 1b) rely on existing sources of electromagnetic waves, such as commercial radio or TV broadcasts, as illuminators of opportunity. These waves are reflected by objects in the environment, and the PRS detects and processes these reflected signals to extract target information. Target identification in PRS relies on sophisticated signal processing algorithms and feature extraction techniques to distinguish between different types of drones.



(a) Active radar system (b) Passive radar system

Figure 1: *Types of radar systems.*

[109] GlobeNewswire military drone market size forecast; URL: https://tinyurl.com/y4ychfne.

2.1 ARS vs PRS: Pros & Cons

Figure 2 summarizes the main differences of PRS versus ARS solutions for drone detection. First, ARS have the capability to detect targets over longer distances, due to the full control over the characteristics of the emitted waves, whilst they typically track more accurately the position, speed, and trajectory of fast-moving flying targets. On the other hand, PRS enable covert operation since they do not emit their own radar signals. Instead, they rely on the ambient signals present in the environment, making them difficult to detect and locate by adversaries. In contrast to ARS, PRS generally consume much less power since they do not need to generate and transmit their own radar signals. As such, PRS could be mounted to drones with limited power resources. Furthermore, PRS can be more cost-effective compared to ARS. They leverage existing illuminators of opportunity, such as commercial radio or TV broadcasts, for signal transmission, eliminating the need for dedicated transmitters. This reduces equipment costs and operational expenses. Finally, PRS are made primarily of hardware components of significantly reduced size, whilst they mostly depend on software-defined modules. These characteristics enable much easier deployment – even on drones – and interoperability of PRS against ARS.

Figure 2: *Pros and cons of ARS versus PRS.*

3. ML-driven PRS for Drone Detection

One of the recent research activities, carried out jointly by the Signal Processing Lab (SPL) and Telecommunications & Networks Lab (TNL) of FORTH-ICS, focuses on the design and development of an innovative PRS for drone detection by capitalizing on ML computational tools and ubiquitous 5G networks. The reasons that motivate us to tackle the problem of drone detection are manifold: first, their number is expected to rise exponentially in the next years, whilst they can be used for malicious (intended or unintended) reasons, which makes their early detection a highly important task. Besides, they present different characteristics from usual radar targets such as higher mobility, flight at lower altitudes, more degrees of freedom (DoF), much smaller form factor (size, shape, and other physical specs), and operation in complex environments (e.g. with many obstacles and non-line-of-sight).

Regarding our interest in leveraging 5G networks, this stems from the fact that 5G base stations will be ubiquitous in a few years from now. Most importantly, they provide very attractive features for the design of PRS, namely, (i) operation at mmWave frequencies, which provides a better ability to detect smaller targets; (ii) operation at wide bandwidths (100-800 MHz), which allows for an increased range resolution; and (iii) multiple-input and multiple-output (MIMO) technology, supporting up to 256 antennas, which improves the detection and classification accuracy of drones via the cross-correlation of more reflected signals.

As for our focus on designing an ML-empowered PRS, this is justified by several facts. First, drones can have unpredicted behavior due to more DoF. Notably, classical tracking approaches may fail to analyze reflected signals acquired in cluttered environments, or characterized by low signal-to-noise ratios (SNR). On the other hand, ML-based tools have proven better capable in resolving such issues, while our recent advancements at SPL and TNL in designing deep learning (DL) architectures enable the joint target detection, classification and tracking. Finally, an ML-driven solution supports a highly versatile software-defined PRS that enables on-the-fly selection and adaptation of operational frequency band and/or bandwidth to maximize accuracy and the probability of correct detection and classification.

3.1 System Architecture

Figure 3 depicts the overall architecture of our proposed ML-driven PRS for drone detection. Specifically, the 5G signals reflected by a drone are first captured by a software-defined radio (SDR) system that acts as a real-time spectrum analyzer, designed in-house by TNL. The captured spectral data are collected in a database, forming the training dataset. Next, each spectral snapshot is properly divided into spectral sub-bands, and each sub-band is given as input to a separate neural network. The outputs of all neural networks are then fused to provide the result, that is, the target class. Currently, we leverage the efficiency of Convolutional Neural Networks (CNN) for extracting informative signatures from the spectral snapshots of each target class. Nevertheless, we emphasize that our system architecture is modular enough allowing for the replacement of our trained CNN by an improved learning model that may arise in the future, without affecting the remaining system components.

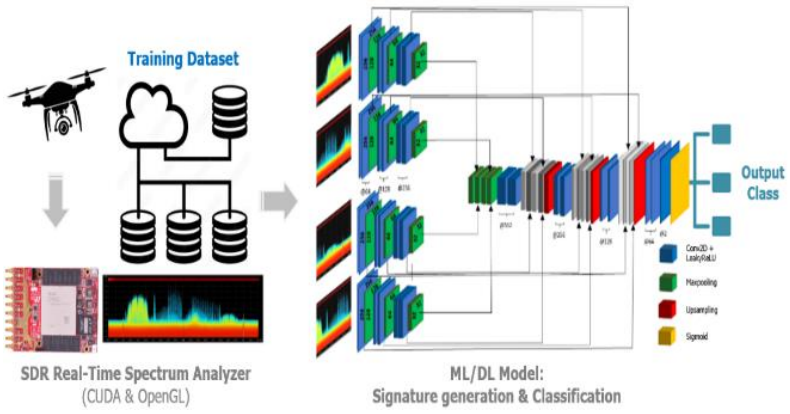


Figure 3: *Architecture of proposed ML-driven PRS.*

3.2 Advantages and Value Added

Overall, our proposed ML-driven PRS for drone detection offers the following advantages:

- It is primarily a software-defined solution that enables easy upgrade and futureproofing;
- In contrast to the majority of existing commercial solutions that act as "black boxes", our PRS is a "white-box" solution providing full access to the architecture of individual modules;
- It supports the integration of state-of-the-art ML/DL models, as soon as they become available, whilst offering a self-training option to the end-user;
- It supports scalability to multi-modal data, allowing for the integration of data gathered by heterogeneous sensing devices, as well as interoperability with existing military command and control systems.

4. Conclusion

In conclusion, the demand for improved PRS for drone detection has become inevitable, primarily driven by the limitations and high costs associated with operational ARS that often require extensive resources and infrastructure to operate effectively, making them expensive and less covert in military operations. On the other hand, existing PRS have demonstrated efficiency in detecting and tracking targets without emitting detectable signals, but they suffer from limited upgradability and lack transparency, acting as black boxes. To overcome these challenges, our ML-driven solution offers a promising approach. By leveraging the ubiquitous signals of 5G networks, we enable the development of a PRS that is scalable and versatile. The utilization of 5G signals as the basis for detection provides several advantages. Firstly, 5G networks are increasingly widespread, ensuring a broad coverage area for the PRS. Secondly, the inherent characteristics of 5G signals, such as their high bandwidth and low latency, offer enhanced capabilities for accurate detection and tracking.

On the other hand, one of the key strengths of our ML-driven solution is its ability to provide scalability and versatility. The ML/DL models employed in the system allow for continuous learning and adaptation, enabling the radar system to effectively handle diverse and evolving scenarios. Moreover, the use of 5G signals ensures compatibility and interoperability with existing military infrastructure and communication networks, facilitating seamless integration into military operations.

In summary, our ML-driven PRS for drone detection, based on ubiquitous 5G signals, offers a promising solution to address the limitations of ARS and existing PRS. With its scalability, versatility, and potential for situational awareness and interoperability, it holds tremendous promise in enhancing the effectiveness and efficiency of military operations. •

Abstract

Modern Warfare operations have completely shifted over the last 5 years due to the standard adoption and irregular usage from a great number of tactical or guerilla forces; a true modern day "technical"[110] . Libya, Syria and Ukraine are just the high profile theaters that drones have proved how important are to provide a tactical advantage regardless of their size.

From Medium-Altitude Long-Endurance (MALE) to small Unmanned Aerial Systems (sUAS) they have undeniably earned their accolades on the battlefield. Thus a new challenge arose; How to take down opposing forces' UAVs? While taking down the UAV seems the primary objective, a more thorough analysis of the available options brings to attention an also important issue; the economical impact of counter measures. At which point is it viable to use a Patriot missile against a sUAS and at which point non destructive force could be used?

A highly increasing trend on the usage of UAVs is the denial of usage of drones regardless of their size, leading to high uncertainty on the decision making for counter attacks or diplomacy solutions. The latest example of denial of usage was seen in Ukraine, where a UN sanctioned state was proved to provide drones found on the battlefield. Both supplier and end-user refused accountability of actions. This is where forensics and digital forensics provide intelligence on an otherwise unknown fact, where other approaches fail to address. Establishing the ground truth is imperative for decision makers (from strategic to tactical level) as improves the level of certainty in an era of "doublethink"[111].

Dead Drones Talking: Digital forensics considerations on the usage of CUAS technologies.

By Mr Evangelos MANTAS

Introduction

While focusing on the Ukrainian conflict might seem oversaturated and well discussed by now, significant trends and "lessons learned" on the future of unmanned warfare have been seen. The rapid transformation of the battlefield with the advent of drone technology is arguably one of the most obvious as drones have revolutionized warfare by offering enhanced situational awareness, reconnaissance capabilities, and even offensive capabilities to both sides involved in the conflict. This introduction will delve into how drones have reshaped the dynamics of the conflict in

[110] A technical, in professional military parlance often called a non-standard tactical vehicle (NSTV)

[111] Doublethink is a process of indoctrination in which subjects are expected to simultaneously accept two conflicting beliefs as truth

Ukraine, examining the utilization of both domestically produced drones and those acquired through export control agreements and commercial off-the-shelf (COTS) equipment.

Intelligence reports on the conflict demonstrate how drones have become a key asset for both the Ukrainian government forces and the Russian-backed separatists in Ukraine. The Ukrainian military has leveraged drones to gather intelligence, monitor troop movements, and enhance their tactical decision-making process and conduct offensive operations. They have employed various drones, from indigenous manufactured models to imported from other countries through export-controlled weapon agreements. On the other side, the separatists have utilized drones to support their operations, including surveillance and reconnaissance missions, utilizing a mix of domestically produced drones and those acquired from external sources.

The utilization of drones by both sides is not solely limited to domestically produced systems. Export control agreements have allowed for the acquisition of advanced drones, which have further enhanced their capabilities. Additionally, commercial off-the-shelf equipment has played a significant role, enabling both sides to modify and adapt consumer-grade drones for military purposes. This accessibility to commercial drones has democratized the technology, providing affordable and readily available platforms for deployment in the conflict.

The proliferation of drones and their increasing capabilities on both sides has resulted in a pressing need for counter-unmanned aerial vehicle (C-UAV) equipment. As drones have become more prominent on the battlefield, the threat they pose, including intelligence gathering, weaponization, and disruption of operations, has necessitated the development and deployment of effective countermeasures. Counter-UAV systems, such as radio frequency jammers, kinetic solutions, and advanced detection systems, have been sought to mitigate the risks posed by enemy drones oftenly shadowing an important question; who is operating the drones?

A Shift in Operations

The conflict in Ukraine witnessed a notable shift in the utilization of drones, moving from larger military-grade drones to smaller commercial unmanned aerial vehicles (UAVs). In the early days of the conflict, larger military drones played a prominent role with various Medium Altitude Long Endurance (MALE) deployed. These drones offered extended range, longer flight durations, and the capability to carry heavier payloads, utilized in a number of operations such as Intelligence, Surveillance, Target Acquisition & Reconnaissance (ISTAR) and precision strikes. However, as the conflict progressed, there was a noticeable shift towards the use of smaller drones that were originally designed for commercial purposes. These drones, manufactured by companies like DJI, offered increased affordability, ease of use, and accessibility, enabling both sides to deploy them with a smaller logistical footprint.

When comparing the cost of operating larger military drones like the Predator and TB2 with smaller commercial UAVs like those produced by DJI, a significant disparity becomes apparent. The larger drones, with their advanced capabilities and military-grade construction, incur substantial

expenses in terms of acquisition, maintenance, and support infrastructure. Conversely, the smaller commercial drones, also known as small-Unmanned Aerial Systems (sUAS) built for non-military applications, have considerably lower upfront costs, reduced maintenance requirements, and can leverage existing consumer-grade support infrastructure, resulting in significantly lower operational expenses.

The small drones, due to their compact size and maneuverability, excelled in urban environments and close-quarters operations, allowing for better surveillance and real-time intelligence gathering. They provided flexibility, rapid deployment, and the ability to operate from areas otherwise inaccessible to larger drones that require infrastructure such as airstrips and/or catapults or other equivalent take-off requirements.

The challenges of rapid adoption

This rapid adoption of equipment in what essentially is guerrilla warfare, has spawned new challenges, particularly on the cyber domain. These sUAS were never meant to be used on a battlefield and the specifications of their emitted signals are following the standards of airspace regulatory authorities; that of course differ from a solution aimed to be utilized by any security force. Therefore they were not hardened (e.g protected by cyber or other security controls) up to the standards of any military operation and therefore are vulnerable to a number of cyber attacks that can be launched with minimal equipment. Reports state that almost 10.000 drones have been lost from Ukraine's side, a truly significant loss count[112], from Russian electronic warfare weapons.

One of the primary concerns regarding the usage of commercially available sUAS is the ability to track and intercept their signals. As sUAS operate on publicly available radio frequencies (2.4-5.6 GHz) for communication and control (C2), these signals can be intercepted with relatively cheap equipment, potentially compromising the security of the drone and its data. Signal tracking can enable attackers to hijack control of the drone, intercept video feeds, or manipulate flight operations. While signal intelligence (SIGINT) as part of military operations doctrine is not a new concept, a particular incident in the Ukraine conflict raised a concern for the safety of these types of operations.

The DJI Aeroscope Incident; A brief explanation

The chinese owned company DJI is the leading manufacturer of commercial drones that also manufactures equipment to track the location of their own made drones with a CUAV equipment named DJI Aeroscope. This product was meant to be used by law enforcement units or other organizations after making a purchase request. This means that the access to it was limited to specific customers and the market circulation was controlled. It makes sense that since both sides started operating small drones, those CUAS equipment would be used as well. Operators from Ukraine reported that after flying their DJI drones, they would almost immediately be shelled from artillery strikes and that their own Aeroscopes would not function

[112] Jack Watling and Nick Reynolds, 'Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine', Special Resources, 19 May 2023, RUSI https://rusi.org/explore-our-research/publications/special-resources/meatgrinder-russian-tactics-second-year-its-invasion-ukraine

properly; raising the speculation that the equipment provided to them was purposefully inoperational compared to the opposing forces', a claim that was denied by the manufacturer[113]. This incident proves how important information on active drones is and the risk of using equipment that is not up to operational standards (either the drone or the CUAS products).

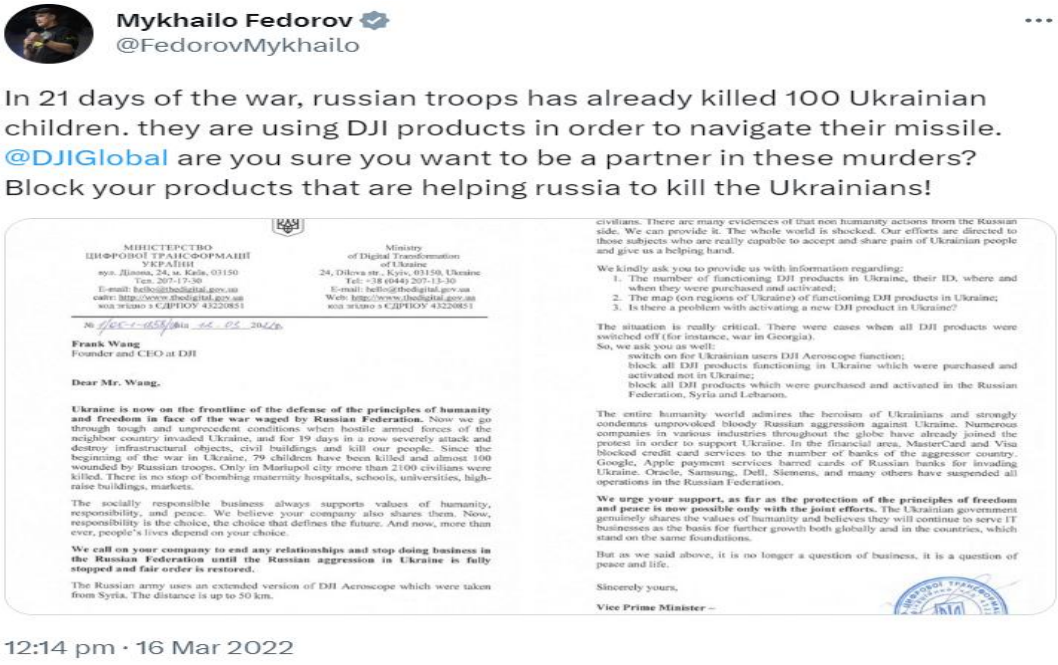


Image: Official Statement of Ukraine government issued to DJI. Source

(https://twitter.com/FedorovMykhailo/status/1504068644195733504?)

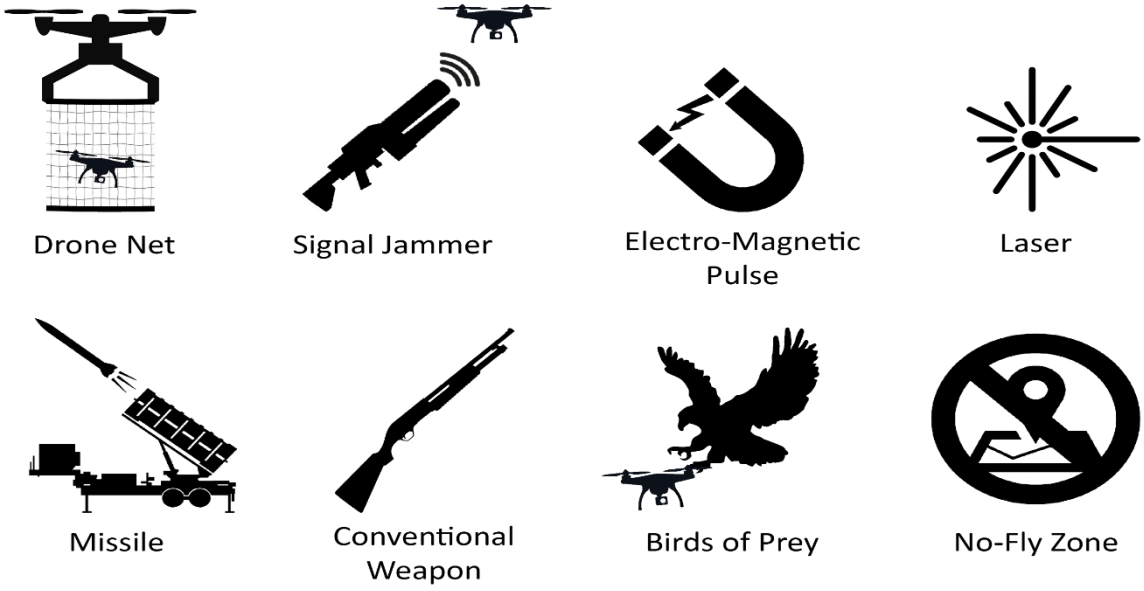


Image: Indicative list of Counter UAS equipment/solutions

[113] Singh, I., Crumley, B. and Crumley, B. (2022) *DJI denies deliberate action to downgrade AeroScope drone detection in Ukraine*, *DroneDJ*. Available at:https://dronedj.com/2022/03/11/dji-aeroscope-drone-detection-ukraine-russia/ (Accessed: 30 May 2023).

The need of Digital Forensics Practices

Taking all the above into consideration it becomes apparent that the need to identify drone operators and their location is an important task. Mitigating the threat while it is still airborne can surely protect and minimize the risk for anyone operating on the ground. While there is currently a growing market of CUAV equipment with a variety of options ("destructive/non destructive" or just tracking/communication eavesdropping) and results, already existing practices of the cybersecurity realm can provide crucial information on drones that were not or just partly damaged and recovered from the ground.

Drones and their corresponding systems encompass a range of identifiable traces and evidence. Similar to any evolving technology, drone technology continually evolves, introducing fresh functionalities, which consequently generate new forensic artifacts that can be examined and analyzed. Since drones can be employed to perform unauthorized reconnaissance missions, gather intelligence on military operations or infrastructure, digital forensics enables military organizations to analyze the data collected from intercepted drones, such as captured images, video footage, and navigational data, to determine the extent and nature of the reconnaissance activities. This intelligence can be actionable and assist the identification of the potential adversaries, fortification of security measures, and implementation of countermeasures to mitigate future drone-based reconnaissance threats.

Drones have been increasingly utilized as a means to carry out attacks or deliver improvised explosive devices (IEDs) in military settings. Digital forensics plays a vital role in investigating such incidents by analyzing the digital artifacts present in the captured drones. This includes examining the drone's communication logs, video recordings, and any other relevant data to reconstruct the attack, identify the perpetrators, and gather evidence for legal proceedings or intelligence purposes. There are instances in Syria (one of the first operational theaters of sUAS usage) where both the drone and the IED payload were successfully recovered providing information about the IED manufacturer leading to uncovering Islamic State's (ISIS) drone modification program in Mosul (circa 2017)[114].

Last but not least, military forces rely on digital forensics to strengthen operational security and develop effective anti-drone defense strategies. By studying captured or neutralized hostile drones, experts can extract critical information about the drone's communication protocols, navigation systems, and potential vulnerabilities. This knowledge helps in devising countermeasures, improving airspace security, and developing technologies to detect, track, and neutralize hostile drones. Such information was used to assess the current technological state of Russian made drones such as Orlan-10, where it was proven that the electronic equipment was made in the West and had somehow ended up in Russia, according to a video posted by Ukraine's security forces on social media[115].

[114] Rueben Dass, 'Militants and Drones: A Trend That is Here to Stay', Commentary, 6 September 2022, RUSI https://www.rusi.org/explore-our-research/publications/commentary/militants-and-drones-trend-here-stay

[115]Twitter:https://twitter.com/Osinttechnical/status/1513211530904580098?t=MhMOEGZf-MAD2vneIY8JRgw&s=19

While digital forensics can offer an otherwise unseen aspect of drone warfare, it is arguably a “nice to have” option when the risk of an armed drone in the airspace is higher and the need to mitigate it in a timely manner might supersede the intelligence gathering. Understanding the tactical and strategic advantages that it might offer could be a beneficial toolkit to a rapid changing operational environment. •

NATO Warfighting Capstone Concept

By Lisa BARTEL, Col, US A

Russia's illegal invasion of Ukraine reminded us all that large scale combat against near-peer adversaries is not a mere relic of history, and that a robust network of layered air and missile defense capabilities will be critical to success against such adversaries. In response to the invasion, NATO and its Allies and partners have committed to optimizing the military capabilities they can bring to bear in defense of freedom and security. One way to ensure success in doing this is through operationalizing NATO's Warfighting Capstone Concept (NWCC), NATO's long-term vision for the development of the Alliance's military instrument of power, as well as a realistic path forward for individual member nations to turn the vision into reality.

The theme of this year's conference is "integrated air and missile defense: a valuable pillar in NATO's Deterrence and Defense." This is certainly true, but it can only be a valuable pillar if successful. This raises the question of what will be to ensure European IAMD, and the roles we all play in it, are successful now and into the future. One place to start is by looking to NATO's strategic military documents to ensure coherence with the rest of the Alliance's approach to long-term peace and security.

NWCC has five warfighting imperatives meant to ensure sustained success. This presentation will offer recommendations of what the European IAMD community needs to do in order to accomplish these five NWCC imperatives. Doing so will provide a shared path forward for how we can best posture ourselves to provide the Alliance combat credible air and missile defense capabilities. •

Image Source: Author; The British Army

What has the RUS/UKR Conflict Taught us About IAMD, and how Should it Shape NATO's Prepares for the Future?

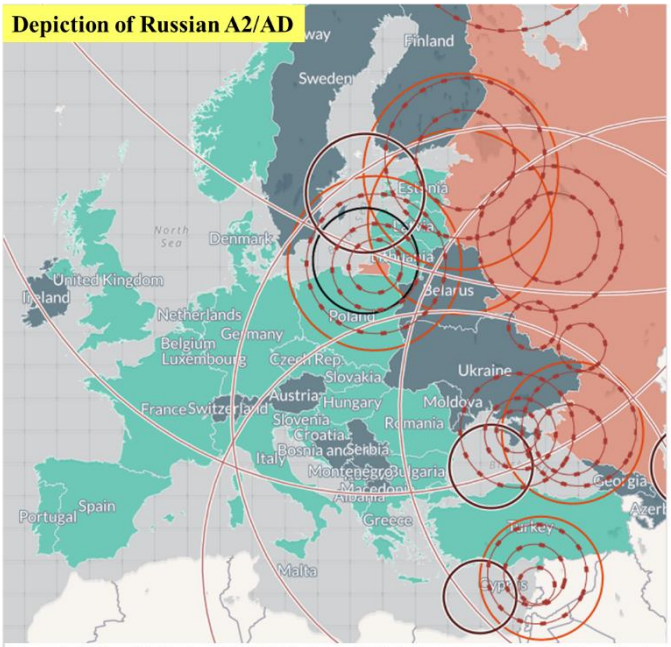
By Graham TAYLOR, Col, UK A

Introduction

Russia's invasion of Ukraine in February 2022, which heightened tensions across the world, has provided a sobering reality of the importance of defence, and in particular, Integrated Air and Missile Defence (IAMD). The operational environment is rapidly evolving, and so are our potential adversaries. Advancements in technology and the proliferation of multiple threats from the air, such Unmanned Aerial Systems (UAS), aviation, fixed wing, cruise, ballistic and hypersonic missiles provide an increasingly challenging target set for air

defence (AD) systems. The evolution of technology, and the ease of access to that technology, is challenging NATO's current existing doctrinal models and presenting a changing character of conflict in new and novel forms.

The conclusion of the Madrid Conference in 2022 and the unveiling of NATO's *2022 Strategic Concept*[116] directed a robust Allied future force that is capable of deterring and defending against a near-peer adversary in a high-intensity, multi-domain conflict.[117] What has the Russia-Ukraine conflict taught us about IAMD, and how should it shape NATO as it prepares for the future? This article first highlights the challenges to Air Defence in the operational environment. Second, it briefly illuminates the Air Defence lessons identified from the current Russia-Ukraine conflict, including the United Kingdom's Ground-Based Air Defence (GBAD) deployment in Poland. Third, it will provide insights on NATO's approach to warfare development as it relates to IAMD.



Source: Ian Williams, "The Russia – NATO A2AD Environment," *Missile Threat*, Center for Strategic and International Studies, January 3, 2017, last modified November 29, 2018, https://missilethreat.csis.org/russia-nato-a2ad-environment/.

Challenges in the Operational Environment

Control of the Air. The airspace (including space and cyberspace) is becoming increasingly contested, and to that effect, more complex. Control of the air remains paramount; to achieve this requires a comprehensive Air and Missile Defence (AMD) capability. With the growth of missile technology and capabilities at one end of the spectrum, and the ubiquitous nature of UAS at the other end, creating a protective IAMD coverage over the battlefield is proving to be difficult.

Put simply – is total air supremacy achievable? While localized and episodic air superiority remains feasible, sustaining this is very difficult and it requires the synchronization and convergence of capabilities that are owned by multiple countries and throughout the joint services. Furthermore, we also have to consider Multi Domain Operations (MDO) and the rise in Space and Cyber influence on the battlefield. Does Air remain the most important domain, or is it being diluted by effects generated by other domains? What is clear is that IAMD is inherently joint, multi-dimensional, and multinational.

Mass Still Matters. The variety and sheer number of threats from the air is increasing and exacerbating the complexity of controlling the air. Not only has missile and UAS technology grown in quantity, the

[116] The *NATO Strategic Concept (SC)* defines three core tasks: collective defence, crisis management, and cooperative security, framed by the *Concept for Deterrence and Defence of the Euro-Atlantic Area* (DDA), and materialized by the *NATO Warfighting Capstone Concept* (NWCC), which is the North Star vision for warfare development initiatives of those who share the values of the Alliance.

[117] The *NATO Warfighting Capstone Concept* establishes that the Alliance must be ready to operate in a multi-region, multi-dimensional (physical, virtual, and cognitive) and multi-domain operating environment, which will be persistent, simultaneous, and boundless. The implications of this environment will challenge commanders and staff in the traditional ways of warfighting, thus, forcing NATO to evolve.

proliferation of these threats has also increased. The range and precision of missiles can now threaten friendly support areas. Additionally, technology allows simultaneity to be applied to air threats – UAS pre-programmed to arrive at a specific time and place combined with stand-off missile launches adds to the multitude of threats to which an enemy can strike. It means that the battlespace contains a 360-degree threat and an adversary who has the capacity to sustain and control tempo.

Not to mention, air threats are increasingly cheap. UAS can be bought in their hundreds for a fraction of the price of an air and missile defence system and munitions. With the relatively low cost added to the speed of technological advance, how do we keep pace with the developing threat with our own IAMD capability design and production? It is an industry challenge as much as a military problem; but mass still matters.

Nowhere to Hide. A third challenge is the increasingly difficult ability to remain undetected in the battlespace. In addition to the increased technology aiding air threat platforms with regards to distance and precision, the advancements in sensor technology makes it much easier for enemies and adversaries to find us and our IAMD platforms. The electromagnetic spectrum (EMS) is being exploiting far more than it has ever been. We need to be able to fire and move to improve survivability. How do larger IAMD platforms manage to retain the necessary mobility? Passive air defence measures remain important, as does the ability to operate in a denuded or denied electro-magnetic spectrum, because on the 21st century battlefield, sanctuary is an illusion.

Exploiting Lessons Learned

Russia's Fire Complex. The literature covering the tactics and operations of the Russia-Ukraine war is extensive; and whilst there have been several questions raised about Russia's performance and how they have failed in several areas, there remain many constants in how they process operations.

Russia continues to use Artillery Fires as it's decisive arm. Whilst it has been less successful than many expected, it is still the dominant threat and the greatest challenge to Ukraine. Russia has maximised the use of Electronic Warfare (EW) and Intelligence, Surveillance, and Reconnaissance

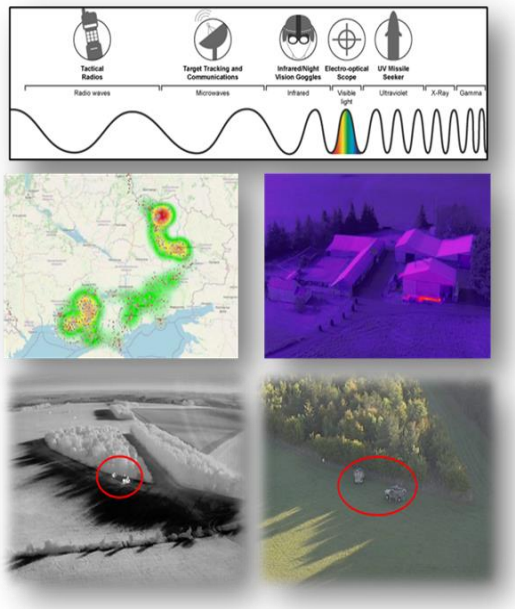


Image Source: Author; The British Army

(ISR) assets to find and target Ukraine assets. The lesson here is that static targets that can be seen and found on the battlefield are…dead targets. As the proverbial Survivability Onion postulates: *Don't Be Seen, Don't Be Acquired, Don't Be Hit, Don't Be Penetrated, Don't Be Killed.*

Russia has also used a mixture of Air, Land and Maritime delivered capabilities to

strike targets in Ukraine. Furthermore, it has developed tactics to combine a mixture of air threats in its targeting to overwhelm Ukrainian air defence assets. Combining long-range precision missiles with massed UAS timed to arrive over or on the target has been an increasingly prevalent tactic. Mass (and tempo) still matters.

Ukraine's Air Defence. Ukraine's response has been impressive, but it is important to recognise that they have had nearly a decade to refine their tactics.[118] Since the ISR cued fires that destroyed Ukraine battle groups during Russia's annexation of Crimea in 2014, Ukraine has been constantly evolving and refining its Air Defence tactics. Ukraine's IAMD has forced Russian air to operate either at a high altitude – thereby reducing precision and accuracy; or at a low level and thereby permitting the effective use of MANPADs. As a result, air and aviation has been largely replaced by long range missiles and UAS. Despite Russia's overmatch, Ukrainian air defences have survived through the effective employment of passive air defence measures and mobility.

Ukraine's more recent challenge has been how to swiftly integrate a wide range of different Air Defence capabilities into a coherent IAMD approach. Capability that has been Gifted-in-Kind has demanded swift adaptation of tactics in order to master and integrate different Air Defence capabilities.

The current conflict reiterates the importance of passive air defence measures – camouflage and concealment, movement, and reduced active radar exposure. It has also introduced new, novel, and innovative measures – including the well documented use of mobile phone applications to allow the civilian population to act as Air Observers.

But what does this mean for NATO and our approach to IAMD? A lot of these lessons and observations are not necessarily all new (lessons we've always been aware of but need to re-learn), but it reinforces the importance of NATO doctrine and in particular, passive air defence.

Coalition Operations. The conflict in Ukraine has also provided opportunities for NATO countries to develop IAMD. In Poland, the IAMD force of Poland (SA-3, SA-6), United Kingdom (SkySabre), United States (Patriot), and now Germany (Patriot), has had over 12 months of developing and providing an integrated AMD capability. One key lesson learned is that of command and control. Combined joint kill chains look simple on a chart but require training and repetitions to develop the skill necessary to process engagements. Additionally, not all systems were created equal, which only complicates joint kill chain operations when "swivel-chair" tactics are required. However, the lessons in Poland and the enduring deployment have provided invaluable training and experience, which are difficult to replicate within the national or NATO exercise programme.

Additionally, the coalition Gift-in-Kind support has enabled Ukraine to extend their operational reach in the war. With respect to the United Kingdom, as part of a programme that trained Ukrainian Air Defenders and supplied High-Velocity Missile (HVM) capability (armoured and light role),

[118] Preliminary lessons from the RUS-UKR war revealed that the Russian Aerospace Forces (VKS) underestimated Ukrainians, which were made a top priority by the Ukrainian government since 2014. Mykhaylo Zabrodskyi, Mykhaylo, Jack Watling, Oleksandr V Danylyuk and Nick Reynolds. *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February-July 2022.* Royal United Services Institute for Defence and Security Special Report, 30 November 2022. Accessed 15 January 2023, Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022 | Royal United Services Institute (rusi.org).

the lessons being fed back in from Ukrainian operators fighting the capability has proven priceless in the understanding of both the limitations and opportunities regarding to Air Defence operations. Bottom line, people (and leadership) are our most precious asset and cannot be developed overnight.

applied. What is clear is the consistent requirement to adopt commonality across NATO as much as possible. We all recognise the Human, Technical and Procedural pathway to interoperability: we're good at the Human, we are improving in the Technical, but we need to get better at Procedural. That starts with common language, common procedures, open architecture and accessible networks and shared understanding.

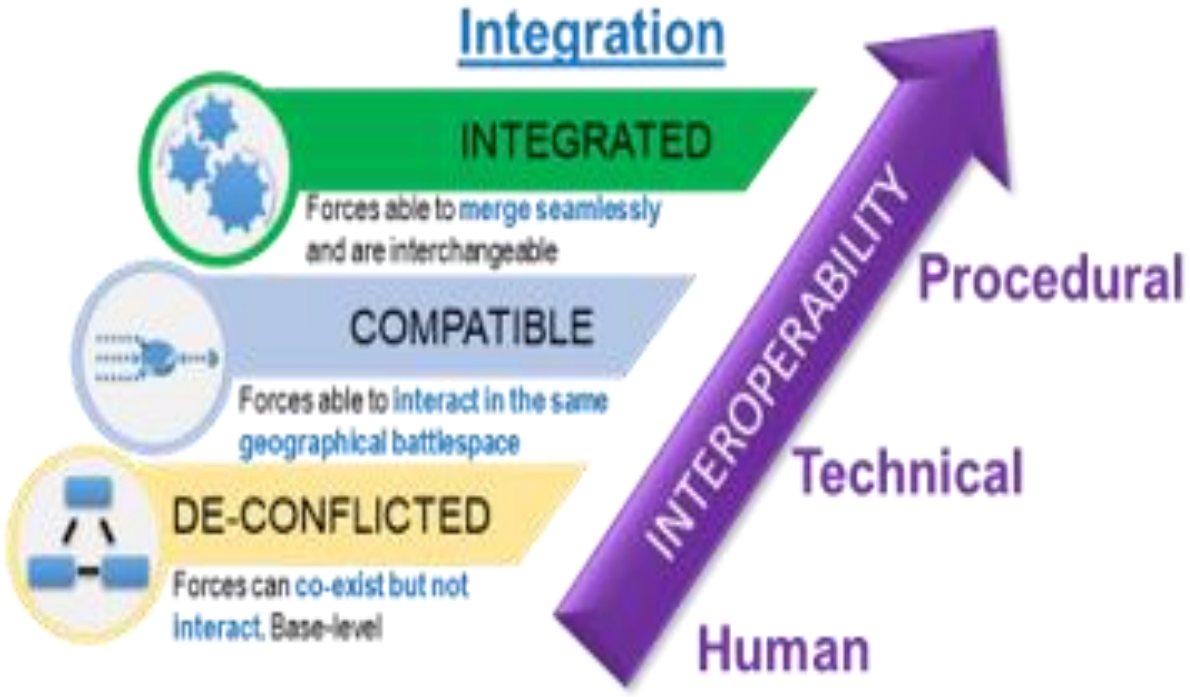


Image Source: Author, UK Ministry of Defence

Future of NATO IAMD Warfare Development & Training

So, what does this all mean for us as NATO's collective IAMD force? Despite the number of lessons identified from the conflict in Ukraine, for the military practitioner, the key is to learn from them and apply them judiciously. Lessons from the Russia-Ukraine war are important – but we must not simply adopt all of them until further analysis and wider context are

The Russia-Ukraine war has reinforced the importance of the airspace and the key battle to control it. Mass retains its own quality and still matters. Survivability is paramount and greater success has been achieved where passive air defence, dummy positions and careful management of the electromagnetic spectrum have all proven critical. Integrating a mix of AMD capabilities remains vital – either as a sovereign state or as part of a coalition.

Control of the air remains essential; to achieve this requires a comprehensive Air and Missile Defence capability. Collectively, we need to ensure that we can generate and hold a multi-national IAMD capability at readiness. That extends to having an authorised and empowered command and control chain above that collective IAMD force held at readiness. Speed and relevance in multi-national space is difficult to achieve, but we must improve. The current framework under the NATO Military Strategy (SC, DDA), along with NWCC as the North Star for warfare development, will enable us to train as we need to fight.

NATO's warfare development must address, and operate, across the full spectrum of conflict. We must be able to balance our collective ability to protect and permit Combined Arms Manoeuvre – Land Forces operating on the ground; but also, how we support Multi Domain Operations. Reinvigoration of survivability and passive air defence needs to be a focal point.

In conclusion, the future of NATO IAMD must recognise that no single sovereign state is fully capable of bringing every layer of AMD to bear, success will continue to be achieved through multi-national integration. Future NATO IAMD training requires a return to fundamentals: clear command and control channels; a robust, open architecture network; exploitation of tactical data links; movement and protection measures; shared doctrine and operating procedures; and a comprehensive multi-national training environment. NATO IAMD must be multi-national by design, not aspiration. •

On 24 February 2022, massive strikes utilized by thousands of missiles and loitering munitions stoke Ukraine's cities, critical infrastructure, and military units and forces. It was clear that Russia had a clear advantage over Ukraine in long-range, precisionguided munitions. The missile strikes were carried out across Ukraine, extending as far west as Lviv using different directions and by using high-precision weapons which is not novel nor unique. Operations Desert Storm and Operation Allied Force saw an increase in precisionstrike munition usage and cruise missile employment, which peaked during the Operation Iraqi Freedom.

21st Century Warfare: Long Distance Fires- Are We Ready to Defend Against it?

By Savvas ALMETIDIS, Maj, GRC AF

Long-range precision strike refers to the ability to accurately engage and neutralize targets at extended distances, often utilizing advanced guided munitions and sophisticated targeting systems. It has become a critical component of modern military operations, allowing forces to project power and eliminate high-value threats from afar. However, with the increased capability of long-range precision strikes, the need for effective defense measures to counter such attacks becomes equally crucial. Defending against long-range precision strikes requires a comprehensive approach that integrates various defensive systems, including robust air defense networks, advanced radar and sensor capabilities, responsive command and control systems, and effective countermeasures. Additionally, developing resilience in critical infrastructure, enhancing cybersecurity measures, and implementing active defense strategies are key aspects of countering long-range precision strikes. By adopting a multi-layered defense approach and continually adapting to emerging threats, nations can enhance their capabilities to protect against long-range precision strikes and safeguard their interests.

1. Lessons from Ukraine

Despite the increased density and integration of Russian air defenses, the VKS (Russian Aerospace Forces) shows hesitancy in entering Ukrainian airspace. Instead, Russian aviation predominantly relies on stand-off attacks. Most of these stand-off effects are achieved through aviation-launched cruise missiles, One of the key points of this campaign, is that Russia, even though it could deploy thousands of airplanes, did not (or could not) attempted, or managed to assume air superiority over Ukraine. Currently, Ukrainian Ground Based Air Defense system is not only intact, but perhaps more capable than before the invasion. The root causes of such situation,

is that Russia failed to engage strategical targets (e.g., disrupt Ukrainian supply lines coming from the West, etc.), and effectively destroy Ukraine's air defence. This resulted in Russian forces heavily rely on field artillery, drones and kamikaze-UAVs and cruise missile strikes, which proved extremely vulnerable to air defence. According to data released by the Ukrainian Air Force - UAF, there has been a notable increase in the proportion of Russian cruise missile salvos intercepted by Ukrainian air defenses since October. Furthermore, the interception rates achieved by Ukrainian air defenders in the later months of 2022 were significantly higher compared to the initial months of the war.

2. A New Form of Warfare

While new technologies are emerging almost daily in every industrial, economic, or social aspect of our lives, they are all share a common factor, and that is their ability to collect, store, process, and transmit every bit of information. This flow of information is made possible by four major factors:

1. Computing power
2. Information storage
3. Information Transmission
4. Advance Algorithms

The revolution in military affairs is a profound transformation in the very nature of warfare brought about by advancements in technology, tactics, and organizational concepts. It encompasses the integration of information technology, precision-guided weaponry, unmanned systems, and networkcentric warfare. This revolution has significantly impacted military operations, enabling faster decision-making, enhanced situational awareness, and increased lethality on the battlefield. The ability to gather and analyze vast amounts of data, coupled with improved communication and coordination, has reshaped the way armed forces plan, execute, and adapt to conflicts. The revolution in military affairs continues to shape the future of warfare, presenting both opportunities and challenges for military forces worldwide. All-domain warfare (or Multi-Domain Operations – MDO) refers to the integration and synchronization of military operations across all domains: land, sea, air, space, and cyberspace. It recognizes that conflicts are not confined to a single domain but rather involve complex interactions and dependencies across multiple domains. The aim is to create synergies and maximize the effectiveness of military operations in a multidimensional battlespace. By adopting an all-domain approach, militaries strive to gain a competitive edge and maintain superiority across all operational domains in modern and future conflicts.

3. Modern developments in Integrated Air and Missile Defence

Integrated Air and Missile Defense (IAMD) is a comprehensive approach to defending against airborne threats, including both aircraft and missiles. It involves the integration of various defensive systems, sensors, command and control networks, and engagement capabilities to provide a layered defense against aerial threats. The primary objective of IAMD is to detect, track, identify, engage, and defeat incoming airborne threats to protect assets, forces, and population centers. This includes countering a wide range of threats, such as manned and unmanned aircraft, ballistic missiles, cruise missiles, and other

aerial threats. Key components of an IAMD system typically include:

1. Sensors: These include radar systems, electro-optical sensors, and other detection systems that provide situational awareness by detecting and tracking airborne threats.

2. Command and Control (C2) and Battle Management.: A robust C2 network is essential for coordinating the defense against multiple threats. It facilitates the fusion of sensor data, analysis, and decision-making to generate a comprehensive air and missile defense picture.

3. Engagement Systems: These are the defensive weapons and systems used to engage and destroy incoming threats. They can include interceptor missiles, anti-aircraft artillery, directed energy weapons, and other defensive measures.

4. Communication Networks: Reliable and secure communication networks are crucial for effective coordination and information exchange between different elements of the IAMD system. One of the main enablers in modern communication networks are the Military 5G.

The strength of an IAMD system lies in its layered defense approach. By deploying various defensive assets and capabilities at different altitudes and ranges, it increases the likelihood of successfully intercepting and neutralizing threats at different stages of their trajectory.

4. Addressing the threat of Long-range Precision Fires

Modern IAMD forces will need to confront, the following – distinct – families of threats:

a. Modern fixed and rotary wing airplanes, equipped with advanced sensors, data fusion capabilities, and stealth characteristics.

b. Swarms of unmanned/uncrewed air systems, with advanced and expanded autonomy and capabilities.

c. Information warfare/hybrid warfare. Information warfare refers to the use of information and communication technologies to gain an advantage in conflicts by influencing, disrupting, or manipulating the perception, decision-making, and behavior of adversaries.

d. Tactical/Theater Ballistic Missiles.

e. Long Range Precision Strikes. When addressing the threat of long-range precision strikes, we must address three distinct categories: artillery shells that can reach ranges of almost 100 km, cruise missiles and hypersonic weapons. The analysis of each threat is as follows:

i. Artillery shells . Even with the longer range, artillery shells fall within the responsibility of Counter Rocket Artillery Mortar or C-RAM[119] approach.

ii. Cruise missiles. Most (if not all) cruise missiles currently in service, can reach speeds up to Mach 3+ and have limited to no capability to perform evasive maneuvers. One of their advantages is that can fly close to earth (NOE) without any compromise in their speed. Modern IAMD

[119] Counter-Rocket, Artillery, and Mortar (C-RAM), also known as counter-RAM, refers to a collection of systems designed to detect and intercept incoming rockets, artillery, and mortar rounds in mid-air before they reach their intended ground targets. Alternatively, these systems can also serve as early warning mechanisms, providing timely alerts of incoming threats. C-RAM systems are specifically employed to neutralize or mitigate the destructive impact of these projectiles, thereby safeguarding potential ground targets from damage

sensors and missiles are more than capable of addressing cruise missiles, and the introduction of new shooters (like Iron Dome, or High-power Laser Systems) can effectively confront the threat of cruise missiles.

iii. Hypersonic.

Currently, hypersonic weapons pose the most critical threat for air-defence systems[120].

The emergence of hypersonic weapons has presented distinct obstacles for air defense systems. These weapons, such as Hypersonic Glide Vehicles (HGVs), deviate from traditional ballistic missile trajectories by following steeper and lower-altitude paths. Their exceptional speed, maneuverability, and flight at low altitudes pose significant challenges for detection and defense. Furthermore, Hypersonic Cruise Missiles (HCMs) have the capability to be launched from aircraft and ships, further complicating their initial detection. This delayed detection reduces the available time for decision-making, often resulting in limited opportunities for interception attempts. Additionally, the deployment of additional measures, such as Anti-Satellite (ASAT) missiles, can impede early warning capabilities, exacerbating the difficulty in countering hypersonic threats.

Furthermore, the task of accurately determining the intended target of a hypersonic weapon would prove extremely challenging. This aspect adds an additional layer of complexity to defense efforts since the time available for alert and response would be minimized. For instance, the Kinzhal missile, with a range of 2000 km, can reach its destination in as little as 8 minutes when launched from a MiG-31K aircraft. The key enabler in addressing the hypersonic threat is the development, and introduction of new sensors, tailored to overcome the obstacles introduced by the very nature of the hypersonic missiles. Advanced algorithms, modern computer systems, and networks should be deployed to facilitate rapid exchange of information. New effectors (e.g., highpower lasers, exoatmospheric kill vehicles, etc.) should be deployed to effectively confront hypersonic.

Another intriguing factor is the formation of a plasma cloud during hypersonic flight, particularly around the missile's cone, due to intense air pressure and heat. This plasma cloud can lead to the absorption and interference of electromagnetic radiation, potentially resulting in disruptions to communication, as seen during the re-entry phase of the Apollo missions. Furthermore, the presence of a plasma cloud can significantly diminish the target's radar cross-section (RCS), leading to the concept of "Plasma Stealth".

5. Final Thoughts

The history of integrated air and missile defense (IAMD) dates back to the early development of air defense systems during the mid – 20th century. Initially, air defense focused on countering aerial threats such as enemy aircraft, but with the advancement of technology, the need for comprehensive defense against missile attacks emerged. The concept of integrating air and missile defense systems gained prominence

[120] https://edition.cnn.com/2023/05/16/politics/patriot-missile-damage-ukraine/index.html [accessed: 02 July 2023]

during the Cold War, where the proliferation of ballistic missiles posed a significant threat. Over the years, various countries and defense organizations have worked to develop and refine IAMD capabilities by combining radar systems, command and control networks, interceptors, and sensor technologies. This integration allows for a coordinated and layered defense approach, leveraging the strengths of different systems to detect, track, and engage both aircraft and missiles. As the threat landscape continues to evolve, the history of IAMD serves as a testament to the ongoing efforts to enhance defensive capabilities and protect against airborne and missile-based threats in an integrated and efficient manner. Modern IAMD forces and approaches should address two profound issues. The first one is that the "threat landscape" that modern IAMD is called to answer is constantly expanding. From the single aircrafts or the formations now IAMD should defend against RAM, UAVs, precision strikes, aircrafts, helicopters, all kind of TBMs, Cruise Missiles and Hypersonic missiles etc., and the list is keep growing. Furthermore, the introduction of and the exploitation of computer systems, networks, and communications and the dependence of modern IAMD systems on their availability and effectiveness, is creating a new area of confrontation and a new list of vulnerabilities that modern IAMD forces should be able to answer. Today, modern IAMD forces should be ready to "think out of the box" (the implementation and integration of SM-6, a typical naval air-defence missile into ground platforms can be considered as such), expand its reach to all domains of warfare, and should be able to go toe-to-toe in ammunition expenditure. •

Integrated Air and Missile Defense Battle Command System (IBCS)

By Br. Gen (Retd), Donald G. FRYC

WHAT IBCS IS (AND IS NOT)

IBCS (Integrated Battle Command System) performs all the command and control, battle management and fire control functions needed to plan, coordinate and execute an effective defense against a broad array of airborne threats to include cruise, ballistic and hypersonic missiles. The IBCS net-centric architecture allows Commanders to jointly plan, coordinate and synchronize operations across air, land, sea and space assets to defeat threats using a wide variety of sensors and weapons. IBCS does not perform functions for Air Operations C2 such as air mission planning, fighter escort, air mobility, combat air patrol and attack. A US military Area Air Defense Commander will use IBCS to conduct ground-based air and missile defense operations in conjunction with US Air Force air operations. USAF uses specific Tactical and Operational C2 systems that are complimentary to IBCS for that purpose. IBCS integrates sensors (e.g., radars) and effectors (e.g., PAC-3 missiles) to an Integrated Fire Control Network (IFCN) as components (see Figure 1). Componentization allows IBCS to network those sensors and effectors into a cohesive Integrated Air and Missile Defense (IAMD) weapon system with performance that is greater than the sum of its parts. The IFCN can exchange data over dedicated radio channels, as provided by the IFCN relays shown in Figure 1, or through any IP capable media such as SATCOM, fiber, microwave or 4G/5G cellular networks. The IBCS data distribution management intelligently manages the data exchange on the IFCN to ensure timely delivery of data and a consistent air and missile picture at all nodes. IBCS fuses data from the sensors connected to the IFCN into fire control quality composite tracks. As demonstrated during a July 2021 IBCS Flight Test, IBCS connections to the Cooperative Engagement Capability (CEC) and F-35 are in development by the US Government. IBCS used those connections during FT06 to receive data from F-35s and a TPS-80 radar (via CEC) and fuse it with other sensors such as Patriot and Sentinel radars. This test was conducted in a “contested” electronic attack environment. IBCS was able to defeat the cruise missile threat during the test by using its Engage-On-Network (EON) firing mode. This mode fuses data from all sensors into a fire control quality track that is used to guide the effector, in this case a PAC-3 missile, to the intercept point. This was a demonstration of applying an All Sensors – Best Effect approach to all-domain operations. The IBCS Engagement Operations Centers (EOC) shown in Figure 1 provides the “brains” – servers, software and networking – for IBCS. There are typically multiple EOCs connected to the IFCN to support defense operations in a specific area of responsibility. The EOC can be contained in a shelter as

Figure 1 IBCS Integrated Fire Control Network connects sensors, weapons and C2 Nodes to include bridging with other Fire Control Networks Such As CEC

depicted or fielded to fixed command posts such operations centers. The IBCS battle staff and fire control element typically will occupy an IBCS Interactive Collaborative Environment (ICE) that is housed in tents, shelters or buildings. The ICE provides operators workstations, communications and large screen displays. The IFCN Relays are used to extend C2 functions across the distributed span of control by integrating sensors and effectors attached to onboard Mission Processors or by functioning as pure relay nodes to other relays with connected sensors or weapons. Because the IBCS IFCN operates over IP networks (IPV4 and IPV6) this enables defense assets – sensors, C2 nodes, missiles and communications – to be geographically dispersed to increase overall effectiveness and survivability. For example, commanders can position forward based sensors to support long range detection, tracking and engagement of threats. The commander is no longer constrained by current weapon system limitations that restrict distances between launchers, radars and C2 components. IBCS allows the commander to emplace weapon and sensors where they are most effective and disperse C2 nodes to maximize continuity of operations. IBCS is currently in low rate initial production. Beginning in 2022, after the planned IBCS Initial Operational Capability (IOC) milestone, the US Army will initiate a modernization all US Army Patriot units with IBCS. Patriot is the first in a series of planned IBCS modernizations that will eventually cover all US Army AMD systems to include THAAD, SHORAD, C-RAM and C-UAS systems. IBCS modernization provides an open architecture foundation, common mission command software at all echelons and eliminates single points of failure that are common in today's AMD systems. With IBCS, commanders will have the tools to:

- Maintain a high confidence, single integrated air and missile picture from multiple sensors to provide earlier warning, assured combat ID and reduced fratricide risk

- Expand the battlespace through sensor netting to provide 360-degree, gapless coverage that enables earlier engagements, at extended ranges, for defended assets

- Acquire, assign, engage and defeat threats with the best weapon for the threat, and then perform a rapid hit assessment and re-engagement if needed

- Conserve effector (e.g. missile) inventories by increasing efficiency in weapon/target pairing

• Increase time available to make the right decisions and rapidly execute those decisions

• Monitor and control sensors/effectors from anywhere on the IBCS network

• Increase defended asset protection levels without increasing the quantity of weapon systems

• Create adaptable and scalable AMD force structures to meet defense needs

• Increase resilience against electronic attack though communications and sensor diversity

• Improve force readiness through embedded training, usability features and simplified logistics.

THE IBCS OPEN ARCHITECTURE IBCS was designed and implemented during the Internet age and benefits from major advances in technology. Unlike legacy air and missile defense systems, IBCS uses a modern, non-proprietary Enterprise Integration Bus to integrate new capabilities through a Publish/Subscribe mechanism that is powered by open standards such as the Object Management Group (OMG),

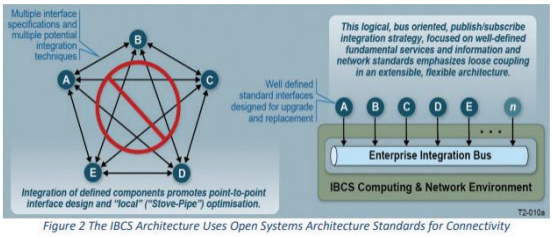


Figure 2 The IBCS Architecture Uses Open Systems Architecture Standards for Connectivity

Data Distribution Service (DDS). This is depicted on the right side of Figure 2.

The left side of Figure 2 illustrates how legacy C2 systems are integrated using point to point connections. This implementation results in data stovepipes and costly upgrades when any one system is modified due to the tight coupling between the individual systems. As new threats emerge, new sensors and new effectors can be integrated via IBCS A/B Kits rather than procuring an entirely new, standalone AMD system that is specific to a threat. This concept is illustrated in Figure 3. IBCS A/B Kits

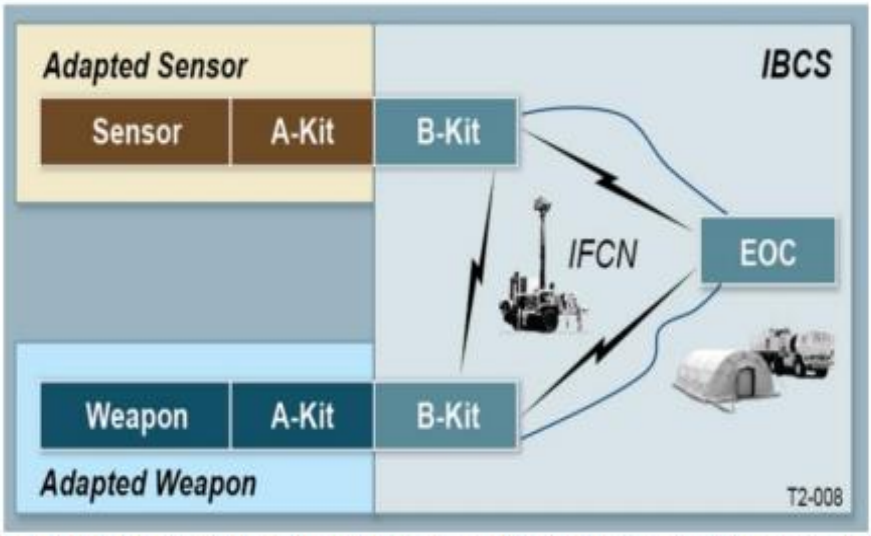


Figure 3 The IBCS A/B Kit Approach for Rapid Adaptation of New Sensor and Weapons Allows for both RF and Fiber Connections to the IBCS C2 in the EOC

are also sometimes known as IBCS Plug-and-Fight (P&F) kits or A/B "sides". Note that new sensors and effectors inherently

implement the IBCS A-Side and do not require “kitting”.

The IBCS B-Kit show in Figure 3 is the common interface for the IBCS IFCN. The IBCS B/A Interface Control Document (ICD) is the US Government owned standard that describes the A and B interface requirements and how to adapt components to that interface. The A-Kit adapts sensors and weapons to the IBCS B-Kit. Typically the original equipment manufacturer (OEM) builds the A-Kit using the IBCS B/A ICD as guidance. The modular IBCS software architecture supports the addition of the OEM’s weapon and sensor models to IBCS to complete the integration of a new component. Northrop Grumman has demonstrated successful integration of missiles from different suppliers. For example, the Patriot Advanced Capability-3 (PAC-3) missiles are built by Lockheed Martin who developed the A-Kit that adapts the PAC-3 launcher to the IBCS B-Side interface. Lockheed Martin also supplied the certified PAC-3 missile model that was integrated into IBCS. The A/B Kit paradigm enables sensor or weapon OEM’s to provide their component without fear of compromise or loss of intellectual property.

Significant cost savings in test and certification is achieved by allowing the certified weapon and sensor models to be reused through incorporation into IBCS. The IBCS software intercommunication model is depicted in Figure 4. The top part of the figure (shaded gray box) shows a detailed view of an EOC with its software applications (blue boxes) and their interaction with the Enterprise Integration Bus (EIB). The EIB is comprised of topics, each of which represents a labeling of messages that contain like information as characterized by the topic name. The messages utilize DDS compliant middleware to exchange traffic along the IFCN in accordance with Quality of Service

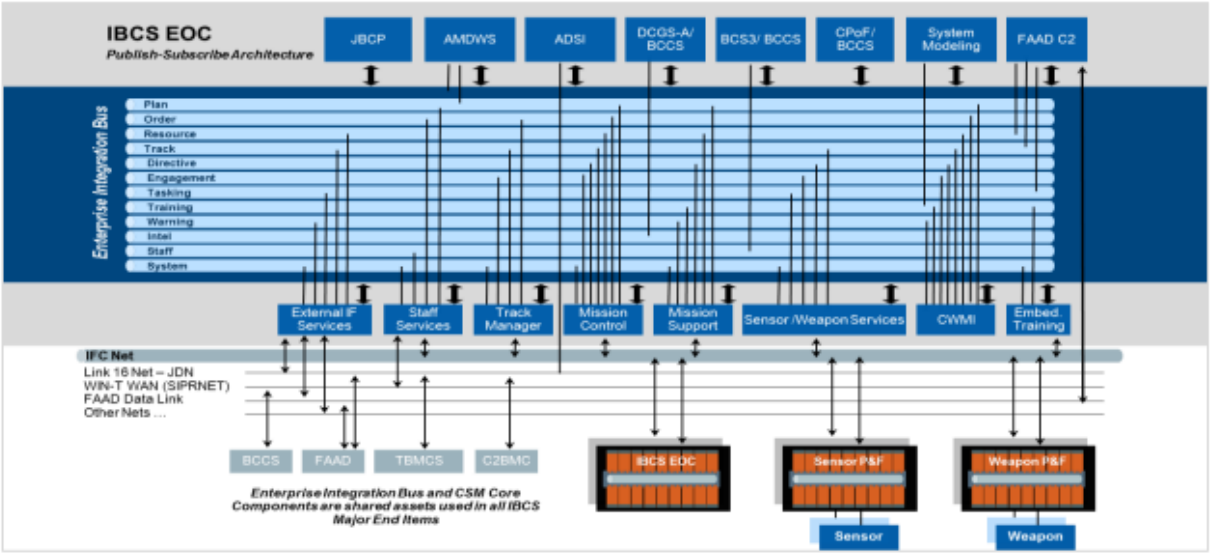


Figure 4 IBCS Software Architecture – Built On an Open Architecture Enterprise Integration Bus

(QoS) criteria. Applications publish and subscribe to relevant topics on the EIB (e.g. Plan, Order, Track, etc.) as shown by the thin vertical black lines that connect applications to topics. The top row of software applications above the EIB indicate the particular external applications that interface to IBCS to meet US military requirements.

By utilizing a Modular Open Systems Approach (MOSA), IBCS allows for rapid integration of new capabilities, ranging from external networks, to new sensors and effectors, to integration of unique mission applications. IBCS provides for the integration of multiple vendor software applications while protecting intellectual property rights of those vendors. Contractors have demonstrated the ability to rapidly integrate existing and new sensors and effectors to include the SAAB Giraffe Radar, TPS-80 radar and the MBDA CAMM-ER effector. The software applications developed on the IBCS Program are shown beneath the EIB. These IBCS Common Software Modules (CSMs) are External Interface (IF) Services, Staff Services, Track Manager (TM), Mission Control (MC), Sensor/Weapon Services, Common Warfighter Machine Interface (CWMI) and Embedded Training (ET). As expected, these organic applications are the ones that have the most interaction with the EIB. Most of these applications connect directly to the IFCN and some of these applications also have direct connections to external networks such as Link 16. Shown in orange is another instance of an IBCS EOC whose software architecture is identical to that in the gray box. Organic sensors (e.g. Sentinel Radar, Patriot Radar) and weapons (e.g. PAC-3 missile), shown bottom right in blue boxes, connect to the IFCN through common P&F kits. Each of these P&F kits (shown in orange) houses its own EIB and also contains copies of the CSMs that service the particular needs of the hosted platform. The IBCS provides a gateway to connect numerous external networks as shown in Figure 5. The IFCN provides a high bandwidth, fire control quality transport for data between the IBCS Command Posts and the IAMD weapons and sensors. In addition, IBCS connects with multiple existing networks such as Link16 and Variable Message Format (VMF, used by ground units) and Fires Data Link (FDL, used by SHORAD units). The IBCS data distribution manager intelligently manages data volume on the IFCN in order to maintain bandwidth at a level that ensures a timely and consistent air and missile picture across all IBCS nodes. Data on the IFCN is tagged with a priority to ensure the most critical information, e.g. data supporting an active missile engagement, is delivered in a time critical manner. This feature is especially important in conditions where network capacity is degraded, as is expected during conflict operations.

The IBCS Payload delivery approach allows IBCS to be adapted and tailored for a

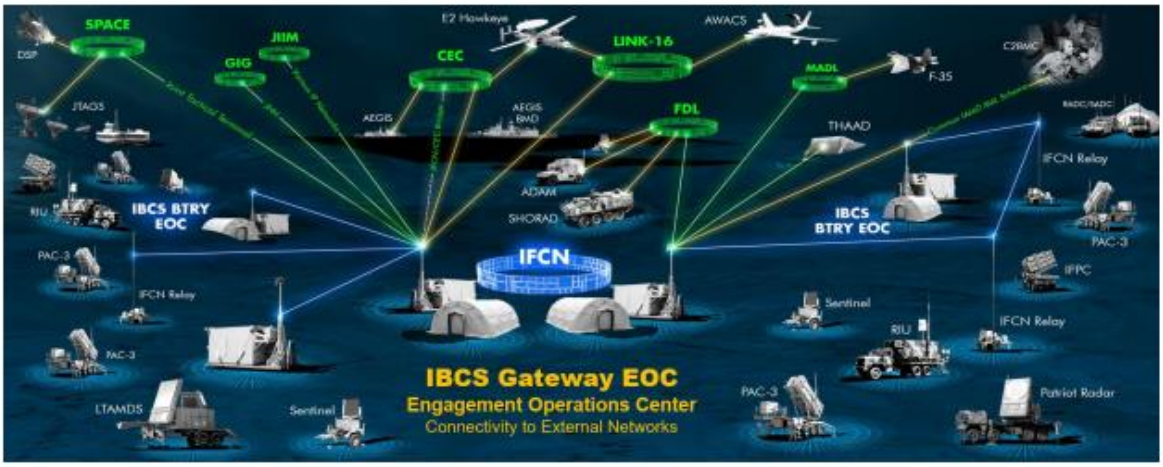


Figure 5 IBCS Connectivity to the All Domain Battlespace

country's specific needs. Figure 6 depicts the current standard US Army IBCS configuration at the top of the diagram.

Integrated Collaborative Environment: The ICE is the main working environment of the commanders, fire control element operators, mission planners and supporting staff.

Engagement Operations Center (EOC): The EOC consists of a shelter that contains the IBCS computing, networking and communications components. The EOC hosts the IBCS software and is connected to the ICE to drive the displays, workstations and communications in the ICE. The EOC also include two operator workstations to support minimum engagement operations.

Integrated Fire Control Network (IFCN) Relay: The IFCN Relay functions as a 360o communication relay and/or interface to sensors and weapons. The IFCN Relay supports a 30 meter antenna mast, networks, power generation and a Plug-and-Fight processing unit that connects sensors and weapons to IBCS. An IBCS Payload is a US Government controlled IBCS configuration item that must be delivered through the Foreign Military Sale channel. Sample IBCS Payloads are shown on the bottom of Figure 6. Controlled components of IBCS include software, computing infrastructure and communication security devices. The remainder of the IBCS configuration can be provided by a country's local industry to include shelters, radios, networks, sensors, weapons, voice switching, displays and command posts. The IBCS open architecture described in Appendix A allows local defense industry to build the A-Kit adaptors for locally provided sensors and weapons. The Payload delivery approach has great benefits for a country:

• Local production of IBCS Configurations tailored to local needs

• Growth and sustainment of the procuring country's defense industrial base

• High level of technology transfer

•Localized sustainment and operations support

Figure 6 The IBCS Payload Approach Allows IBCS Delivery to be Tailored to Local Needs

The four left diagrams of Figure 7 illustrate an example where multiple sensors are each providing discrete and duplicate track states with defined errors in position and velocity,

but without the ability to remove those known errors.

The solid blue line in each diagram represents the true position and heading, or truth, of an airborne threat. Each sensor detects the threat and reports individual tracks that vary from the truth. Even though there is only one threat, warfighter C2 system displays show multiple tracks with different track numbers and often different track identifications. Tracks appear and disappear from C2 systems displays as sensors acquire then lose track on the threat. Because no one sensor can track the threat consistently, a fire control quality track cannot be produced. Additionally, track ambiguities delay the combat identification process that must be completed before a threat can be engaged.

To achieve a single, fire control quality track, IBCS made the architectural choice to integrate attached radars by fusing measurements instead of correlating track states. The outcome is depicted in the right most diagram of Figure 7. While consuming data from the exact same set of sensors, IBCS's distributed composite quality track. By using intelligent dissemination agents, this type of track clarity and quality becomes available to every warfighter and device connected to IBCS. Using CT, track fusion ambiguity is eliminated and every warfighter is presented the exact same set of high quality tracks. IBCS's CT capabilities were demonstrated in multiple IBCS Flight Tests (FT) where multiple sensors contributed measurements to a single composite track with high track containment [small track covariance] to achieve a target kill.

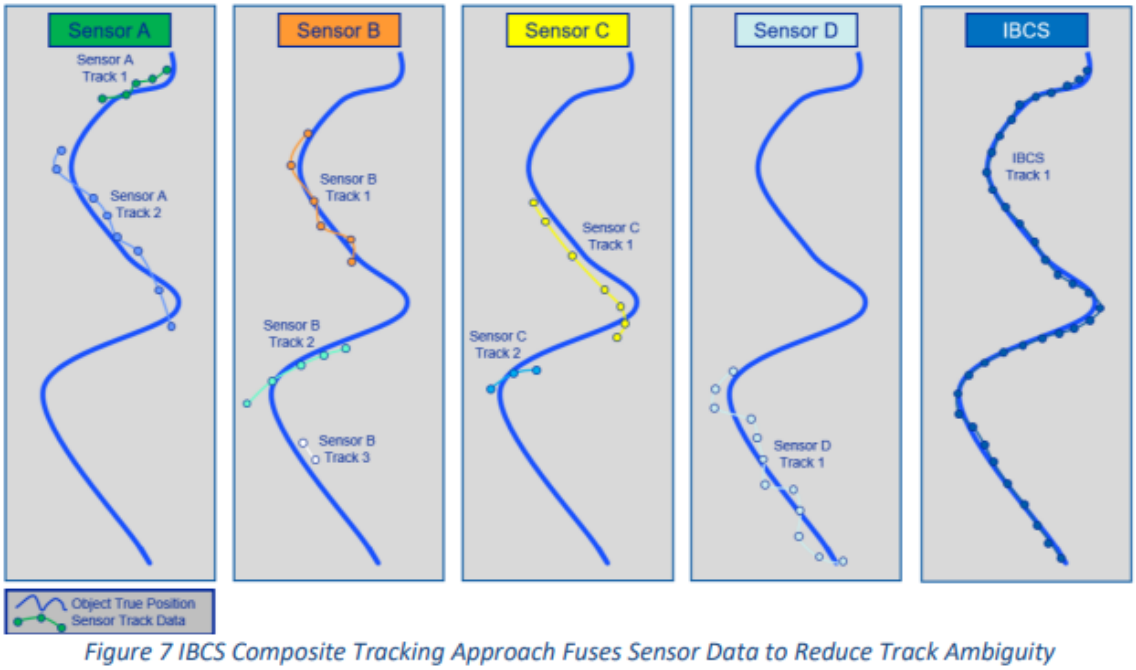


Figure 7 IBCS Composite Tracking Approach Fuses Sensor Data to Reduce Track Ambiguity

tracking (CT) removes individual sensor errors through a bias adjustment process that aligns the reported measurements geodetically to produce a single contiguous, fire control

IBCS Flight Test 06 highlighted the all-domain capabilities of IBCS by using Army, Navy and Air Force sensors to successfully defeat a cruise missile surrogate. The test occurred in Jul 2021

at White Sands Missile Range (WSMR). This test demonstrated a successful engagement in a contested environment and was the first ever Patriot engagement using US Air Force and Navy sensors. During the test the TPS80 and F-35 depicted in Figure 8, provided radar inputs that IBCS fused into a continuous fire control quality track to enable engagement by a PAC-3 missile fired by IBCS.

The flight test incorporated first-time live testing and demonstration of a Joint Track Manager Capability (JTMC) that provided a bridge between IBCS and the US Navy's Cooperative Engagement Capability (CEC), enabling the sharing of TPS-80 sensor data on the IBCS Integrated Fire Control Network (IFCN). The flight test architecture also incorporated two F-35 combat aircraft integrated with IBCS and their on board sensors contributed to the IBCS developed joint composite track that was used to perform the engagement. Two surrogate cruise missiles were launched in the test, one performing the electronic attack mission to disrupt radar performance, and the other flying a threat profile targeting friendly assets. Soldiers of the 3-43 Air and Missile Defense Test Detachment used IBCS to track the surrogate cruise missile targets, identify the threatening missile, and launch a Patriot Advanced Capability Three (PAC-3) interceptor. FT-06 demonstrated IBCS's capability to successfully defeat a surrogate cruise missile threat in a highly contested environment by networking a diverse set of distributed sensors. Additional flight tests in Nov 2021 demonstrated IBCS's ability to disperse IAMD operations by successfully operating the fire control network over a SATCOM link. This enabled the IBCS engagement operations center to be located many kilometers from the sensors and launchers that IBCS used to defeat multiple surrogate ballistic missile threats at WSMR. •

Figure 8 IBCS Flight Test Demonstrates Joint Engagement in Electronic Attack Environment

RPAS & Airspace management in NATO Single European Sky initiative– SES

By Joao CAETANO

THE EUROPEAN DEFENCE AGENCY

The European Defence Agency (EDA) is an intergovernmental EU Agency established to support the Council and the Member States in their effort to improve the Union's defence capabilities in the field of crisis management and to sustain the Common Security and Defence Policy as it currently stands and as it develops in the future.

Founded in 2004, EDA is headquartered in Brussels, Belgium, and operates under the EU Council's decision, working collaboratively with other EU institutions, and external stakeholders to promote defense cooperation and coherent capability development among the member states[121]. Within the overall mission set out in the aforementioned decision, EDA has three main missions:

- To support the development of defence capabilities and military cooperation among the European Union Member States;
- to stimulate defence Research and Technology (R&T) and strengthening the European defence industry;
- to act as a military interface to EU policies.

It aims to enhance Europe's defence industrial base, promote defense-related research and development, and create a favorable environment for defense cooperation and investment. Furthermore, the EDA contributes to the overall security and stability of the EU by promoting a common security and defense policy and fostering closer ties with NATO and other international partners – Figure 16 presents the structure of EDA.

[121] European Defence Agency

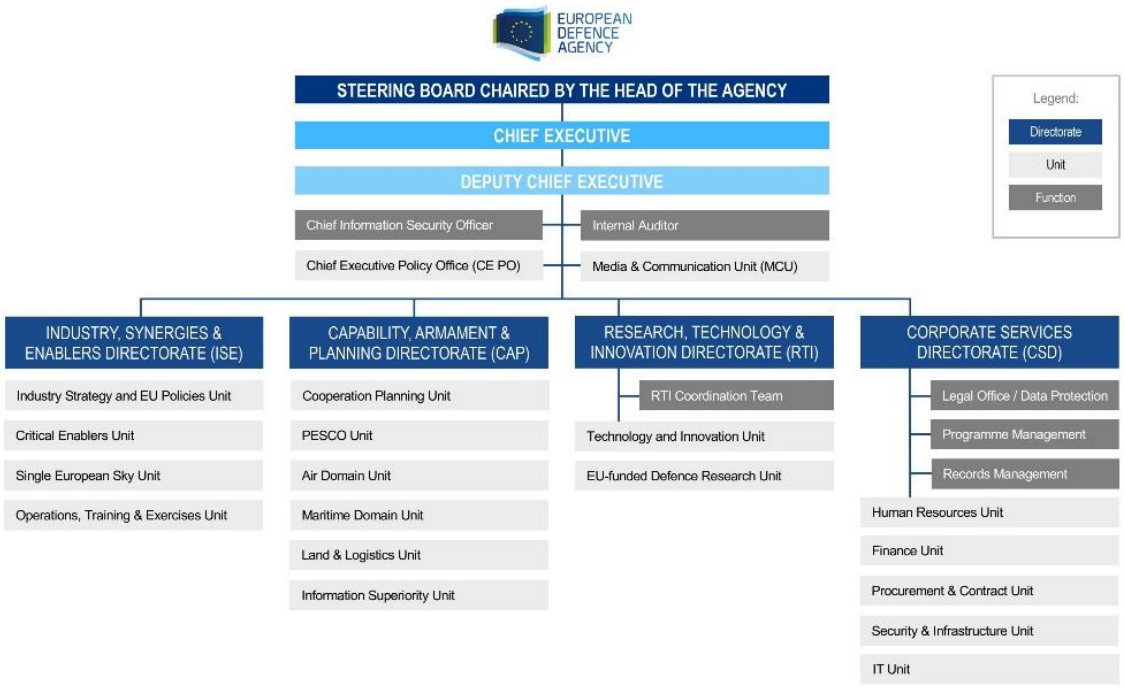


Figure 16 – Organigram of EDA

EDA AND NATO COLLABORATION

The cooperative relationship between the European Defence Agency (EDA) and NATO is founded upon a mutual dedication to improving defense capabilities and fostering security within Europe, as part of the wider EU-NATO cooperation framework. In 2016, the EU and NATO signed a joint declaration with the intention of strengthening their alliance and collaborative efforts through increased staff cooperation. It emphasized the importance of complementarity and synergy between the two organizations, acknowledging that they share common values and face similar security challenges. The signing of the EU-NATO joint declaration in January 2023[122] further strengthens and expands the strategic partnership these bodies. This declaration builds on the unprecedented progress in cooperation between the two organisations since previous declarations were signed in 2016 and 2018. The intention is to deepen cooperation in addressing evolving security threats, including geostrategic competition, resilience, critical infrastructure protection, emerging technologies, climate change's security implications, and foreign information manipulation. Transparency and the involvement of non-EU NATO Allies and non-NATO EU members are emphasized. Regular progress assessments continue to be provided to Allies and Member States and evaluate the partnership's effectiveness.

EDA and NATO participate in a range of collaborative efforts and synergistic activities. They consistently share information, disseminate best practices, and synchronize their endeavors in domains such as capability enhancement, defense planning, and matters pertaining to defense industries. Their objective is to prevent redundancy, optimize resource utilization, and facilitate

[122] Joint Declaration on EU-NATO Cooperation

interoperability among member countries. Both entities acknowledge the critical nature of a cohesive and coordinated approach towards defense; their cooperative efforts contribute to a more efficient and effective European security and defense framework.

At the implementation level, staff cooperation constitutes a fundamental component of the EDA-NATO partnership. Periodic meetings and consultations occur between personnel from both agencies to address shared challenges, exchange specialized knowledge, and identify potential opportunities for joint undertakings. These exchanges enable the dissemination of expertise and insights, fostering an atmosphere of deeper comprehension and collaboration between both organizations. Furthermore, jointly organized events, workshops, and seminars augment the cooperation concerning defence-related matters.

A notable area of cooperation between the EDA and NATO pertains to Unmanned Aircraft Systems (UAS). Both organizations acknowledge the increasing significance of UAS in defense and security operations and strive to endorse their advancement and application. They collaborate on various aspects of UAS, encompassing research initiatives, capability development endeavors, as well as standardization projects. Through sharing information and expertise, the EDA and NATO aim to optimize the advantages offered by UAS technology, while simultaneously addressing its concurrent challenges, including safety concerns, regulatory aspects. This cooperation ensures a coordinated approach to UAS development and deployment, enhancing the overall defense capacities of EU and NATO member states.

UAS AT EDA

EDA has a considerable track record of successfully delivered Unmanned Aircraft Systems (UAS) related projects, with an onset list of current and programmed activities in this domain, in the ISE, CAP and RTI directorates (cf. Figure 16). These

activities are very important and have a detrimental effect on:

Enhanced Capabilities: UAS offer unique capabilities that can significantly enhance military operations. They provide the ability to conduct aerial surveillance, reconnaissance, and intelligence gathering without putting human pilots at risk. UAS can also be equipped with various sensors and payloads to perform tasks, e.g., target acquisition, monitoring, and communications relay. By investing in UAS projects, the EDA aims to improve the overall operational capabilities of European defense forces.

Interoperability and Standardization: The development of common standards, protocols, and interoperability among European defense forces is of prime importance for a stronger EU Defence. Standardization ensures that different UAS platforms and systems can effectively communicate and operate together, facilitating joint operations and cooperation among member states.

Technological Advancements: UAS technology is rapidly evolving, with advancements in areas such as autonomy – including artificial intelligence (AI) –, endurance, and payload capabilities. By engaging in UAS projects, the EDA stays at the forefront of technological developments, allowing member states to benefit from the latest advancements and ensure that

European defense forces remain technologically competitive.

European Industrial Base: UAS projects also contribute to the development and growth of the European defense industry. Investing in UAS research, development, and procurement supports the defense sector, stimulates innovation, and creates job opportunities. It helps foster a competitive European defense industry that can provide cutting-edge UAS solutions, reducing reliance on foreign suppliers and enhancing Europe's strategic autonomy.

Security Challenges: UAS projects address emerging security challenges faced by European defense forces. These challenges include counter-terrorism operations, border surveillance, maritime security, disaster response, and situational awareness in complex environments. UAS provide valuable tools to tackle these challenges efficiently and effectively, making them an essential component of European defense strategies.

Table 1 presents a summary of recent and ongoing projects related to UAS. A detailed description of some of the can be found online.

	Acronym	Title
Finalized	ERA[123]	Enhanced RPAS Automation
	MIDCAS[4]	Mid Air Collision Avoidance System
	IEDDET[124]	IED Detection Programme – Phase I
	SAFETERM[125]	Safe Termination of UAV Flights Using AI
	APOS-UE[126]	Advanced positioning system for soldiers in urban environment
	ADPS[127]	Active Anti-drone Protection System
Ongoing	ACHILLES	Autonomous, reconfigurable swarms of unmanned vehicles for defence applications
	SS2	Soldier System Architecture - The Next Level (HMI perspective)
	SMAS	Sustaining machines - autonomous systems for logistics operations
	AI-GNC Air	AI in Guidance, Navigation and Control for aerial assets
	FS2CATI[128]	Military Transport Drone (platform, propulsion and autonomous precision airdrop)
	NSGR[129]	Next Generation Small RPAS
	RPSS[130]	Remote Pilot Station Standardization
	U-Space[131]	Study on the implications of U-Space on the military
	MIL-UAS-Specific	Military UAS Specific Category Regulatory Harmonisation

Table 1 – summary of recent and ongoing UAS projects at EDA

[123] https://eda.europa.eu/what-we-do/all-activities/activities-search/remotely-piloted-aircraft-systems---rpas
[124] https://eda.europa.eu/news-and-events/news/2017/01/12/eda-programme-launched-to-improve-ied-detection
[125] www.safeterm.eu
[126] https://eda.europa.eu/what-we-do/all-activities/activities-search/captech-guidance-navigation-and-control
[127] https://eda.europa.eu/procurement/other-notices/21.rti.np3.097-for-a-study-on-active-anti-drone-protection-system-for-mobile-land-platforms-(adps)
[128] https://eda.europa.eu/what-we-do/all-activities/activities-search/captech-air
[129] https://www.pesco.europa.eu/project/next-generation-small-rpas-ngsr/
[130] https://rps-core.eu
[131] https://eda.europa.eu/U-Space-study

EU COMMISSION DRONE STRATEGY 2.0

On 29 November 2022 the Commission debuted the Drone Strategy (DS) 2.0[132]. It aims to establish a robust regulatory framework that promotes the safe and sustainable integration of drones in the European Union. It seeks to create a harmonized European market, enhance safety and security, and foster innovation and collaboration. By addressing key challenges and providing a clear roadmap, the strategy aims to unlock the full potential of drones while ensuring the protection of citizens and the environment.

To achieve these goals, the Drone Strategy 2.0 outlines a set of strategies and actions. It emphasizes the importance of research and innovation, supporting the development of new drone technologies and applications. The strategy encourages collaboration between public and private stakeholders, fostering partnerships and knowledge sharing. It also promotes the use of digital tools and data-driven solutions to enable efficient and safe drone operations. Furthermore, the strategy aims to engage with international partners, harmonizing standards and regulations globally to facilitate cross-border drone operations.

The military relevance is evident in the document, with thirteen out of the nineteen Flagship Actions (FA) being related or leveraging the military experience and expertise in the drone domain. Actions are on the way for the implementation of the FA, where the contribution of EDA can have a positive impact, e.g., development of dual-use technology, contribution to strategic autonomy, coordination and cooperation, security and defence implications.

ENVISIONING THE FUTURE

Outlooking the future on the UAS domain in Europe and European Defence, we can highlight, among others:

Digital Sky and Airspace Integration

Regulatory Advancements: Europe is paving the way with the development of harmonized regulations and standards for safe and efficient UAS operations, creating a standardized and futuristic regulatory environment.

Urban Air Mobility (UAM): Imagine a world where UAS are used for transportation and logistics in urban areas and within the military theater. European cities and organizations are exploring UAM concepts with the use of electric vertical take-off and landing (eVTOL) aircraft and delivery drones, working towards more efficient and futuristic transportation. This has a direct impact on novel and next-gen military mobility and logistics.

Sustainability and Environment: The push towards sustainability in UAS operations is at the forefront of European efforts. With a focus on eco-friendly technologies, sustainable flight planning, and reducing noise pollution, European countries are leading the way in greener and more sustainable aviation practices.

Next Generation UAS and Capabilities

The capabilities of next-generation military Unmanned Air Systems (UAS) are

[132] EU COM 652 2002 – Drone Strategy 2.0

continually evolving as technological advancements progress. We can highlight:

Extended Range and Endurance, allowing them to operate for longer durations and cover larger distances. This capability enables extended surveillance, reconnaissance, and target engagement missions.

Enhanced Payload Capacity, enabling the integration of advanced sensors, communication systems, weapons, and other mission-specific equipment. This would enable more versatile and effective operations across various domains, including intelligence gathering, target acquisition, and electronic warfare.

Increased Autonomy and AI, possibly involving increased onboard processing capabilities, advanced algorithms, and sensor fusion, enabling UAS to autonomously navigate, adapt to changing environments, and conduct complex missions with minimal human intervention.

Swarm Capabilities, where multiple UAS collaborate and communicate with each other to perform collective missions. Swarm capabilities could provide increased situational awareness, redundancy, and distributed operations, enabling enhanced intelligence gathering, target engagement, and mission flexibility. AI will be a driver here.

Connectivity and Network Integration: within military and civil networks, to allow for better communication, information sharing, and coordination with other manned and unmanned platforms, in the future digital (European) sky.

Improved Stealth and Low signature, e.g., reduced radar cross-section and enhanced signature management. This would enable them to operate in contested environments with reduced detectability, enhancing survivability and mission success. •

Civil and Military Airworthiness Regulatory Framework and Airworthiness Certification

By Stefanos KRYOVRYSANAKIS, GRC A

1. INTRODUCTION

The rapid development of the UASs created two trends, the military reality on the one hand with the existing use of UAS in the battlefield and the need for their gradual certification and compliance with the applicable requirements. The other trend has as its starting point the world market which is "pushing" for the development of a regulatory framework with the aim of immediately starting their commercial exploitation [133]. This evolution simultaneously raises concerns regarding the way UASs will operate in the already "burdened" aviation environment with the necessity to establish a regulatory framework becoming imperative and immediate for their safe exploitation for both military and civilian operations[134]. The operation of the UASs in the existing aviation environment raises important safety issues that need to be resolved not only in terms of their use and operation, but also in terms of their design, production and maintenance. The operations of such aircraft require manufacturers and operators to comply with the existing civil aviation system and the relevant regulatory framework, which is strictly controlled, with operational and technical aspects defined in detail in order to ensure maximum safety. UASs are prohibited to put in danger the existing "manned" aviation and therefore must be integrated into the existing aviation environment in a uniform and appropriate manner [135] [136] [137]. In civil aviation the safety of the aircraft, the passengers and the population on the ground is provided by the "Chicago Convention" of 1944 and in Europe by the Regulation (EU) 1139/2018 of the European Parliament (establishing common rules in the field of civil aviation) with specific reference to unmanned aircraft which perform flights in the same airspace as manned [138].

The above regulatory documents are not directly applicable to state aircraft (military, police, civil protection etc.) however, the contracting parties are recommended to take actions that will ensure a level of safety equivalent to the one of civil aviation. In the context of the Regulation (EU) 1139/2018 the EDA developed the European Military Airworthiness Requirements

[133] Souvlakis, Christos. "Drones in the Armed Forces and Security Bodies." Thessaloniki, ADISPO, 2019.

[134] Lebesis, Athanasios. "Integration of the European Military Airworthiness Requirements in the Greek Armed Forces - Proposed organizational changes in the Branches". ADISPO, Thessaloniki, 2020.

[135] RPAS Concept of Operations. "Remotely Piloted Aircraft System Concept of Operations for International IFR Operations." ICAO, 2017.

[136] Kokkalas, Georgios. "Airworthiness Regulatory Framework for Military—Civil RPAS. in Proceedings of the Cranfield University Alumni Event and Defence Education Conference, Athens, Greece, 1 June 2017." Athens, 2017.

[137] Notice of Proposed Amendment. "Introduction of a regulatory framework for the operation of drones unmanned aircraft system operations in the open and specific category. " EASA, May 2017.

[138] Regulation (EU) 2018/1139 of The European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008

(EMARs) which are setting requirements for the design, production, maintenance of military aeronautical products and parts, as well as in the training and licensing of the personnel involved in the those activities. The provisions of the EMARs are based on the european civil aviation regulations for initial and continuing airworthiness (EU) 748/2012 & 1321/2014 which are referred to the manned aviation. EDA has set the basic requirements for the airworthiness of the military UAS in the European Military Airworthiness Basic Framework (BFD edition 4.0) [139]. However, up to date EDA has not developed a corresponding detailed framework for UAS, in accordance with the European Regulations (EU) 945 & 947/2019. The issuing of related harmonised requirements is already in progress with the name EMASRU (European Military Aviation Safety Requirements for UAS), which will include the European military airworthiness requirements for the design, production, maintenance and operation of military UASs [134] [140]. The NATO has issued Standardization Agreements (STANAGs) that defines various aspects of the UAS such us, classification, airworthiness, minimum training requirements for operators and pilots etc.; however these STANAGs do not provide a holistic approach and specifically does not cover vital domains of the military aviation safety [136]. In the Hellenic Armed Forces, as in many other countries, there is no holistic regulatory framework for the management of military UAS in the form and structure deriving from the above European regulations. However, since its establishment, the HNMAA has initiated the procedures to develop a regulatory UAS airworthiness framework based on the EDA efforts.

2. UAS DEFINITION

The definition of the term "unmanned aircraft" has evolved over years. The term "pilotless aircraft" was original used in Article 8 of the "Chicago Convention" of 1944. In the 1960s, the term "Remotely Piloted Vehicle" (RPV) was used, which was later replaced by the term "Unmanned Aerial Vehicle" (UAV) in the 1980s. Other terms have also been used, such as "Unmanned Aircraft Systems" (UAS), "Remotely Piloted Aircraft Systems" (RPAS) and "Drones". Nowadays, the term "drone" is the most popular one referring to UAS. However, the International Civil Aviation Organization (ICAO) uses the term "RPAS" while EASA use the term "UAS" which has also been adopted by the Greek legislation[141]. Regarding military organizations both NATO and EDA uses the term "UAS" [133] [134] [140]. For the effective communication of this paper the two main definitions derived from Regulation (EU) 2019/945 are provided below [142]:

a. Unmanned Aircraft System (UAS) means the unmanned aircraft and its equipment for its remote control.

b. Unmanned Aircraft (UA) means any aircraft that operates or is intended to operate autonomously or remotely without a pilot on board.

[139] The European Harmonised Military Airworthiness Basic Framework Document BFD 4.0, EDA, 2022

[140] Stefanos Kryovrysanakis. "National Regulatory Framework for the Exploitation of Military UASs - Adaptation to the European Regulatory Framework for Civilian UASs". ADISPO, Thessaloniki, 2022.

[141] Presidential Decree 85/2020."Airworthiness requirements for military aircraft and organisation of the National Military Airworthiness Authority (NMA)" (Government Gazette A198/16 October 2020).

[142] Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on thirdcountry operators of unmanned aircraft systems

3. UAS CIVIL REQULATORY FRAMEWORK

3.1 ICAO

ICAO has been actively working on developing policies and recommended practices to facilitate the safe and efficient integration of UAS into the global aviation system. A concise overview of ICAO's policy for UAS is provided below [135]:

• Development of UAS Policies: ICAO recognizes the need to establish international standards and regulations to ensure the safe integration of UAS into the global aviation system. It has been actively involved in developing policies and guidelines to address the operational and safety challenges associated with UAS operations.

• Safety Management: ICAO emphasizes the importance of safety management for UAS operations. It encourages states and stakeholders to implement robust safety management systems that identify and mitigate potential risks.

• International Standards and Recommended Practices (SARPs): ICAO develops SARPs to provide a global framework for the regulation of UAS operations. These SARPs cover various aspects, including airspace integration, certification and airworthiness standards, licensing requirements for UAS pilots, operational procedures, and unmanned traffic management systems.

• Airspace Integration: ICAO recognizes the need to integrate UAS into existing airspace systems without compromising safety. It promotes the development of unmanned traffic management (UTM) systems that can facilitate the safe and efficient operation of UAS in both controlled and uncontrolled airspace.

• Provides guidelines for the licensing and qualification of remote pilots operating UAS.

3.2 European Aviation Safety Agency (EASA)

In accordance with the Regulation (EU) 2018/1139, the following two regulations have been issued in order to specify the ways in which UAS will operate in the EU:

a. Commission Delegated Regulation (EU) 2019/945 on Unmanned Aircraft Systems and on Third-Country Operators of Unmanned Aircraft Systems. This regulation provides detailed rules for the operation of unmanned aircraft systems (UAS) in the European Union with the following key points covered [142]:

• General provisions. This regulation lays down the requirements for the design and manufacture of UAS intended to be operated under the rules and conditions defined in Implementing Regulation (EU) 2019/947 and of remote identification add-ons. It also defines the type of UAS whose design, production and maintenance shall be subject to certification

• Obligations of the manufactures, importers and distributors. When placing their product on the Union market, manufacturers shall ensure that it has been designed and manufactured in compliance with the requirements of the above regulation.

• Product requirements. UAS intended to be operated in the open category or in the ‘specific’ category under operational declaration, accessories kits bearing a class identification label and remote identification add-ons

• Rules and conditions for affixing the CE marking, the identification number of the notified body, the UAS class identification label and the indication of the sound power level.

• Technical Requirements. It sets out technical requirements for UAS and their components, focusing on design, production, maintenance, and operation. These requirements ensure the safety and reliability of UAS systems.

• Requirements for classes C0 to C4. Establish the technical requirements based on theirs technical and natural characteristics for the identification label.

b. Commission Implementing Regulation (EU) 2019/947 on the Rules and Procedures for the Operation of Unmanned Aircraft: This regulation complements the Delegated Regulation and provides further details on the rules and procedures for UAS operations. With the following key points covered [143]:

• General Provisions. It outlines the general requirements for UAS operations, including airspace limitations, operational limitations, and responsibilities of remote pilots and operators.

• Categorization. It introduces three categories for UAS operations based on the level of risk (operational risk based approach): "open", "specific", and "certified". Each category has different requirements and limitations.

• Operational Limitations. The regulation specifies limitations on altitude, distance, and visibility for different UAS categories and operational scenarios. It also addresses flight over assemblies of people and operations near aerodromes.

• Operational Authorizations: The regulation outlines procedures for obtaining operational authorizations for UAS operations in the specific category. These authorizations cover various aspects, such as flight in specific areas and beyond visual line of sight operations.

• Safety Management. It emphasizes the importance of safety management systems and risk assessments for UAS operations, providing rules and procedures for conducting an operational risk assessment.

• UAS Identification. The regulation mandates, for specific cases, the registration and individual identification of UAS to ensure traceability and accountability.

• Rules and procedure for the competency of the remote pilots.

4. MILITARY REQULATORY FRAMEWORK

4.1 EDA

EDA along with EASA are the EU bodies to which the European Commission has assigned the convergence of the regulatory frameworks for the airworthiness of both civil and military UAS. This convergence aims to enable their use in the Single European Sky (SES). In this context, EDA established the UAS Airworthiness Regulatory Framework Working Group (UAS ARF WG) to develop a common harmonized European regulatory framework for the airworthiness of military UAS and to achieve convergence or harmonization with the corresponding provisions of EU civil regulations. The approach chosen by EDA to fulfil

[143] Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft.

this task involves the development of military UAS airworthiness requirements as documents separate from EMARs [136] [134]. These documents called EMASRU (European Military Aviation Safety Requirements for UAS) will encompass European military airworthiness requirements for the design, production, and maintenance of the military UASs. Another important task undertaken by the EDA, is the development of the Military UAS Specific Risk Assessment Tool (MUSRAT). MUSRA is a tool for assessing the risks associated with UAS operated in the "specific" category, similar to Specific Operational Risk Assessment (SORA) which is recommended by EASA. The tool takes into account parameters such as weight, estimated area of impact, population density and integrity of UAS structure and systems [134] [140].

4.2 NATO

NATO has issued standardisation agreements (STANAG) that cover various domains of UASs (such as airworthiness, pilot training, etc). Examples are STANAG 4671 "Airworthiness requirements for unmanned aircraft systems" [144], STANAG 4702 "Airworthiness requirements for rotary wing unmanned aircraft systems" [145] and STANAG 4703 "Airworthiness requirements for light unmanned aircraft"[146], which comprise the certification specifications for the UAS, and STANAG 4670 "Minimum training requirements for unmanned aircraft operators and pilots"[147]. It is noted that STANAG 4670 includes the classification of UAS into three categories (I, II and III), based on the mass of the UAS, and seven (7) categories (Strike/Combat, HALE, MALE, Tactical, Small, Mini, Micro), based on various criteria (operational and technical). However, this classification is intended to standardise the training requirements for UAS crews and does not address the standardisation needs in the context of the holistic management of military aviation safety of UAS (operations, air traffic and airworthiness) [136] [148]. Moreover, NATO has established a specific working group [Joint Capability Group on Unmanned Systems (JCGUAS)] that focuses on the development and integration of unmanned systems capabilities within the NATO alliance. The JCGUAS works towards developing common standards, procedures, and doctrine related to unmanned systems. It facilitates information sharing, promotes best practices, and conducts assessments of emerging technologies and capabilities in the field of unmanned systems and is responsible of developing and amending the STANAGs.

5. HELLENIC MILITARY UAS AIRWORTHINESS REGULATORY FRAMEWORK

Per the Presidential Decree 85/2020 the HNMAA is the competent national military authority responsible for the development and the oversight of the national airworthiness system for military aircraft, including UASs [141]. HNMAA has recently issued the Airworthiness Bulletin (HNMAA-AWB-00-005) that provides information and recommendations regarding [148]:

- The categories of military UASs and the criteria for their classification in these

[144] STANAG 4671. "Unmanned aircraft systems airworthiness requirements (UAR)." ed. 3, 2 Apr 19, NSO.
[145] STANAG 4702. "Rotary wing unmanned aircraft systems airworthiness requirements."ed.2, 24 Nov 16, NSO.
[146] STANAG 4703 "Light unmanned aircraft systems airworthiness requirements." ed. 2, 24 Nov16, NSO.
[147] STANAG 4670 (ED-3). "Guidance for the Training of Unmanned Aircraft Systems (UAS) Operators. " NSO
[148] HNMAA-AWB-00-005. "Categorization of Military UAS and Airworthiness Certification Requirements." HNMAA, Athens, 24 Feb 23

categories, based on the UAS categories defined by EDA.

- The airworthiness certification requirements for the UAS of the "certified" category of operations. For the time being HNMAA follows the evolutions of EASA and EDA efforts on the development of airworthiness requirements for the “specific” and “certified” UAS categories in order to issue the relevant national regulations.

5.1. HNMAA UAS CERTIFICATION PROCESS

The HNMAA process for the certification of UAS of the "certified" category is based on the requirements and procedures described in the EMAR 21 and Presidential Decree 85/2020. Basic prerequisite for the initiation of the certification process is the establishment of rigid and effective Concept of Operations (CONOPS) and the approval of the organization as design organization. In general the certification process includes four basic phases as follow [149] [141]:

a. Phase 1: Technical familiarization and Certification Basis:. The aircraft manufacturer presents the project to HNMAA when it is considered to have reached a sufficient degree of maturity. The HNMAA certification team and the set of rules that will apply for the certification of this specific aircraft type are being established (Certification Basis).

b. Phase 2: Establishment of the certification programme: HNMAA and the manufacturer need to define and agree on the means to demonstrate compliance of the aircraft type with each requirement of the Certification Basis. This goes hand in hand with the identification of HNMAA’s «level of involvement» during the certification process.

c. Phase 3: Compliance demonstration: The aircraft manufacturer must demonstrate compliance of its product with the regulatory requirements: the structure, engines, control systems, electrical systems and flight performance are analysed against the certification basis. This compliance demonstration is done by analysis, ground testing (such as tests on the structure to withstand bird strikes, fatigue tests and tests in simulators etc) but also by means of tests during flight.

d. Phase 4: Technical closure and issue of approval: If technically satisfied with the compliance demonstration by the manufacturer, HNMAA closes the investigation and issues the relevant certificate.

6. CONCLUSION

The implementation of regulatory airworthiness framework for UAS plays a crucial role in ensuring the safe and effective integration of these systems into both military and civil operations. Current military regulations focus mainly on operational capabilities, mission requirements, and national security considerations. They establish guidelines for UAS deployment, training, airspace integration and coordination with manned aircraft. These regulations prioritize interoperability, situational awareness, and mission success while mitigating risks associated with UAS operations in military settings. On the other hand, civil regulatory frameworks emphasize on public safety, privacy protection, and the integration of UAS into airspace.

[149] EMAR 21. "Certification of Military Aircraft and Related Products, Parts and Appliances and Design And Production Organisations." EDA, 2020

They establish licensing requirements, operational limitations, and airspace restrictions for UAS operators, ensuring compliance with safety standards and minimizing potential hazards to manned aircraft and ground infrastructure. Both military and civil regulatory frameworks strive to strike a balance between enabling innovation and addressing safety and security concerns. Collaborative efforts between military and civil authorities, industry stakeholders, and regulatory bodies are important for developing a comprehensive and holistic framework with aim of maximizing the benefits these systems offer. Adapting or adjusting the civil aviation framework in the military domain is a good approach and will help the nations to expedite the establishment of a common, harmonised and effective regulatory framework to ensure safe usage of airspace by civil and military aircraft. International cooperation is also vital to harmonize regulations enabling seamless UAS cross-border operations in global airspace.[150]

[150] Hadjidakis, Emmanuel. "The Role of Unmanned Aerial Vehicles in Strategy." Athens, SEEΘA, 2019.

Single Air Picture (SAP, UAS UTM improvement) French Approach

By Lionnel PENNING – REEF, LtCol (FA&SF)

There are three parts to explain SAP

- Firstly, why SAP? What was our approach to creating SAP?
- Secondly, the principle of SAP
- Thirdly, the SAP Road map.

The use of UAVs is very easy and we have noticed an increase in friendly or malicious flights, especially above prohibited areas like political buildings, Airbases and civilian nuclear installations.

In charge of the Air Defense, the French Air and Space Forces has started investing in counter UAVs systems since 2015. For the anecdote, the police forces have begun to invest in counter UAVs in 2018.

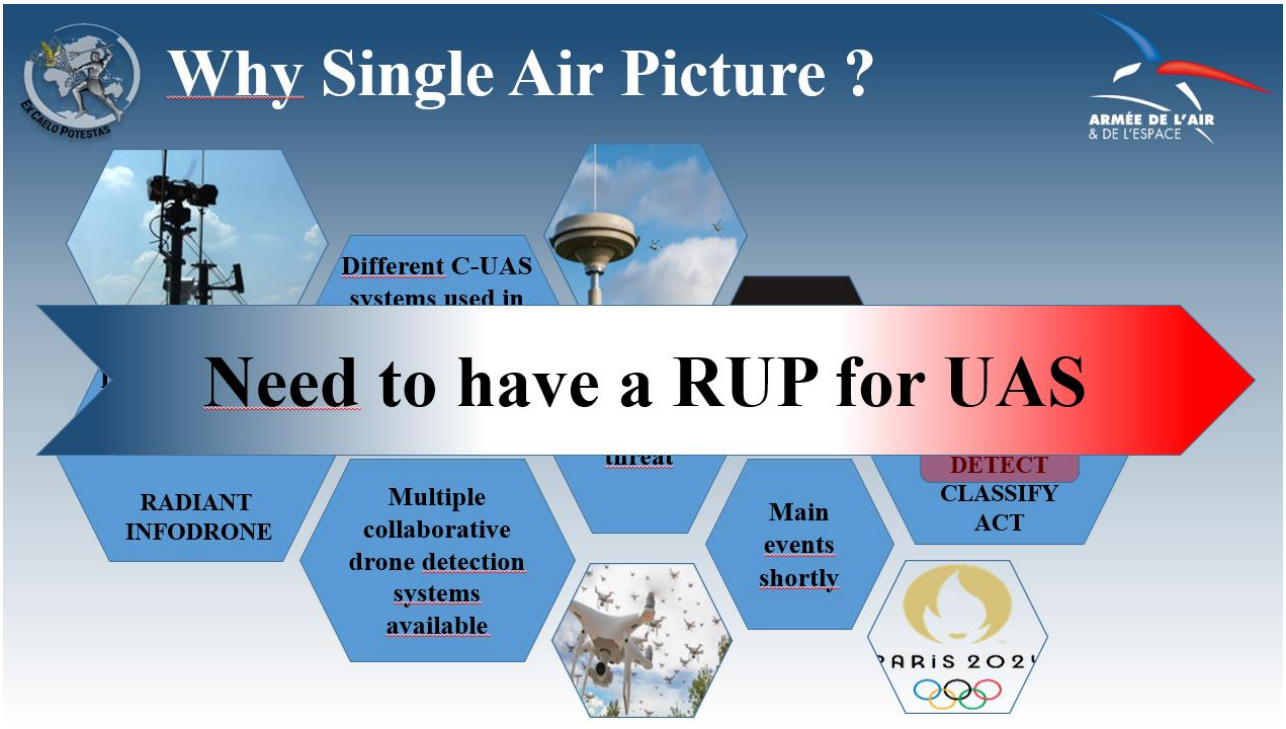
So, French civilian and military C-UAS capabilities have evolved positively over the past 5 years, from jamming guns to "heavy C-UAS Systems" whose be able to detect, identify and jam.

Both militaries' forces and police bought C-UAS systems. Today, you find 4 types of C-UAS systems from different companies but unable to connect each to other.

In addition, UAVs detection systems are available such as Infodrone, Aeroscope, and so on, which offer a cheap solution for detecting as many UAVs as possible, mainly those operated by tourists.

Finally, two main events will occur in France shortly:

- The RWC in sept 2023
- The Olympics in 2024



To fly our own drones and fight those for terrorist use, it has become necessary to connect all systems (UAV and Conter UAVs systems) and using all technologies.

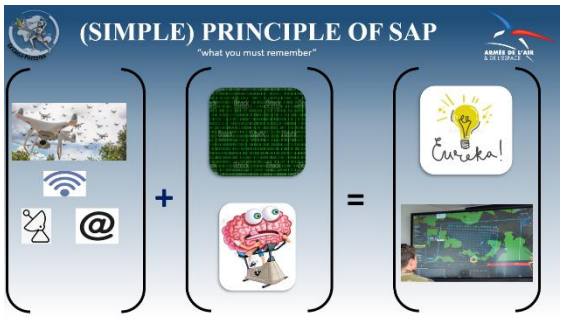
Because we are in charge of Air Defence 24 hours a day, the prime Minister have decided that the French Air and Space forces will integrate and coordinate the C-UAS of Ministry of Defence and Ministry of Interior.

The rules in C-UAS are the same of those in the air defense: you need to detect, identify, classify and shoot if it is necessary.

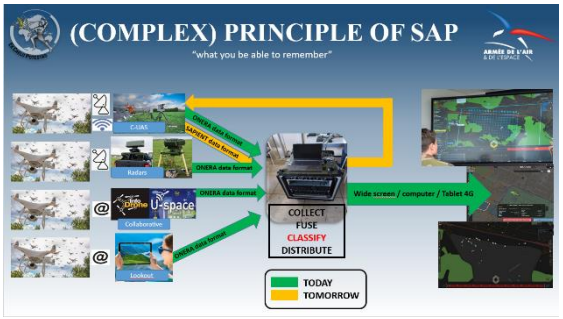
To detect, it is OK. We use many systems that are also able to identify and classify. But, until now, it was not possible to coordinate our actions. Like the RAP in the Air Defense, we need a RUP - a recognized UAV Picture. That's why we have created SAP.

To explain the principle of SAP – a simple way and a complex way.

First, the simple way: the “what you must remember”. Basically, SAP is “just” a digital hypervision tool, able to fuse data from several C-UAS and collaborative systems.



And the complex way: The “what you be able to remember”. Concretely, we collect data from “heavy systems”, from battlefields radars, from USSP (UAV Space Services Provider) and from Infodrone. Once the information is collected, SAP shares to all C2 a secured and fused picture on different human-machine interface (HMI) to facilitate the identification and classification of drones.



A few words about the data format:

For now, we use a simple data format named “Format ONERA” especially created by ONERA, a French Company, to transmit several information about a drone track and facilitate data fusion. Today, this format allows to fuse 1500 (one thousand and five hundred) tracks at the same time. In the short term, we hope that SAP will include the SAPIENT data format.

To conclude, I would insist that SAP is still in development. Our main goal is to be ready for the Olympic and Paralympic games. Fortunately, we have several milestones to test, fix and to improve SAP before this this major event. For example, now we have the Paris Air Show and, in a few days, we’ll have our National Day where we’re going to use SAP. •

Space Situational Awareness

By Thomas BOUAZIZ, Maj (FA&SF)

Space is a domain that is vital to the functioning of our society, and its security. Today, a strategic and industrial competition is taking place in the civilian (New Space), as well as in the military spaces (growing conflictuality between states), threatening French freedom of access and action in space.

As a priority in French space strategy, SSA must be reinforced on the ground, as well as in space, in order to better evaluate threats, and characterize the observed activity (effort on space-related intelligence).

It is also necessary to assess the missile threat that could cause a lot of space debris. •

A M&S Solution to wargame IAMD aspects in a Virtual Environment

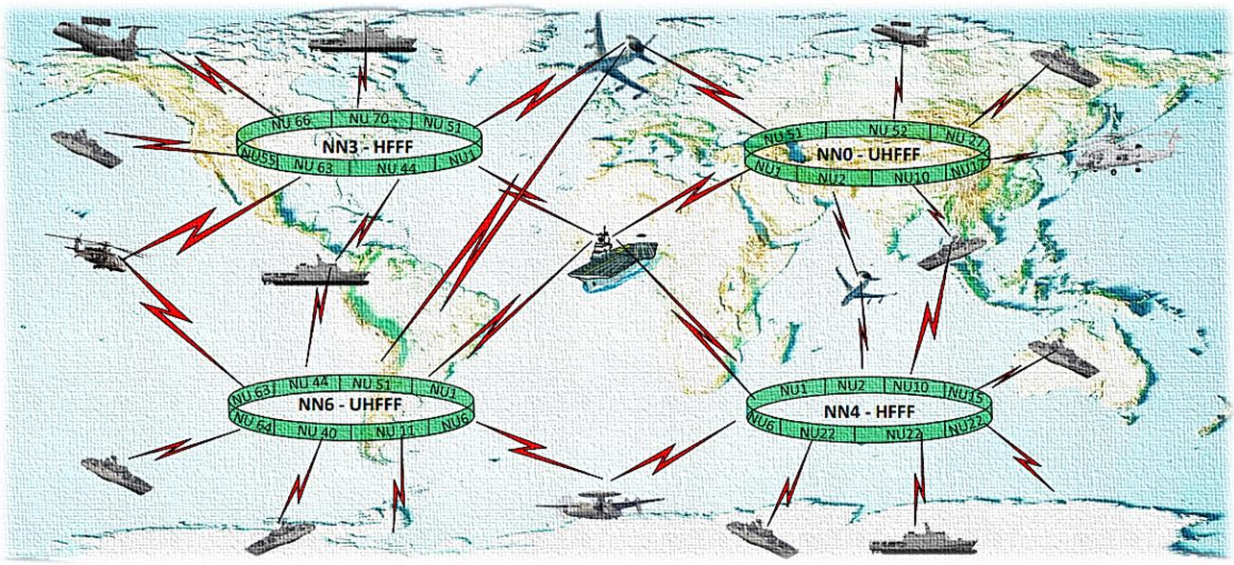
By Uwe GAERTNER, LtCol DEU A

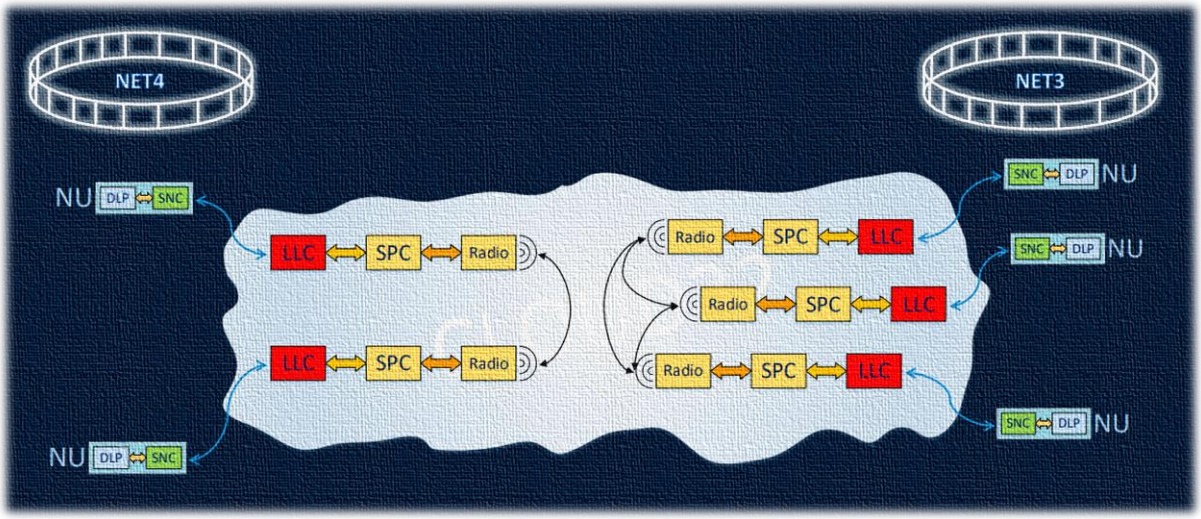
Wargaming is becoming quite popular in NATO as one method to explore certain warfighting aspects in a save-to-fail environment. The NATO M&S COE has developed a digital wargaming platform that provides virtual environments / scenarios for a wide range of applications on tactical, operational and strategic level. Which can also include IAMD. Additionally, we are working on solutions to integrate simulations into wargaming activities, which would lead to more rigor outcomes. •

Link 22 Network Emulation for Ballistic Missile Defence

By Mr Gabriele CASSOTTO

The transition from Link 11 to Link 22 is providing a completely new and enhanced capability for BLOS Tactical Data Link data exchange. NCI Agency has developed a Link 22 Emulation environment that can be used for DLP development, TDL Networks verification, Link 22 Training, etc. The core of this emulated environment is Cloud22, a software application that emulates in real time any Link 22 Networks. IAMD can greatly benefit from the use of Cloud22 to test Link 22 Networks, designed to support BMD missions. •

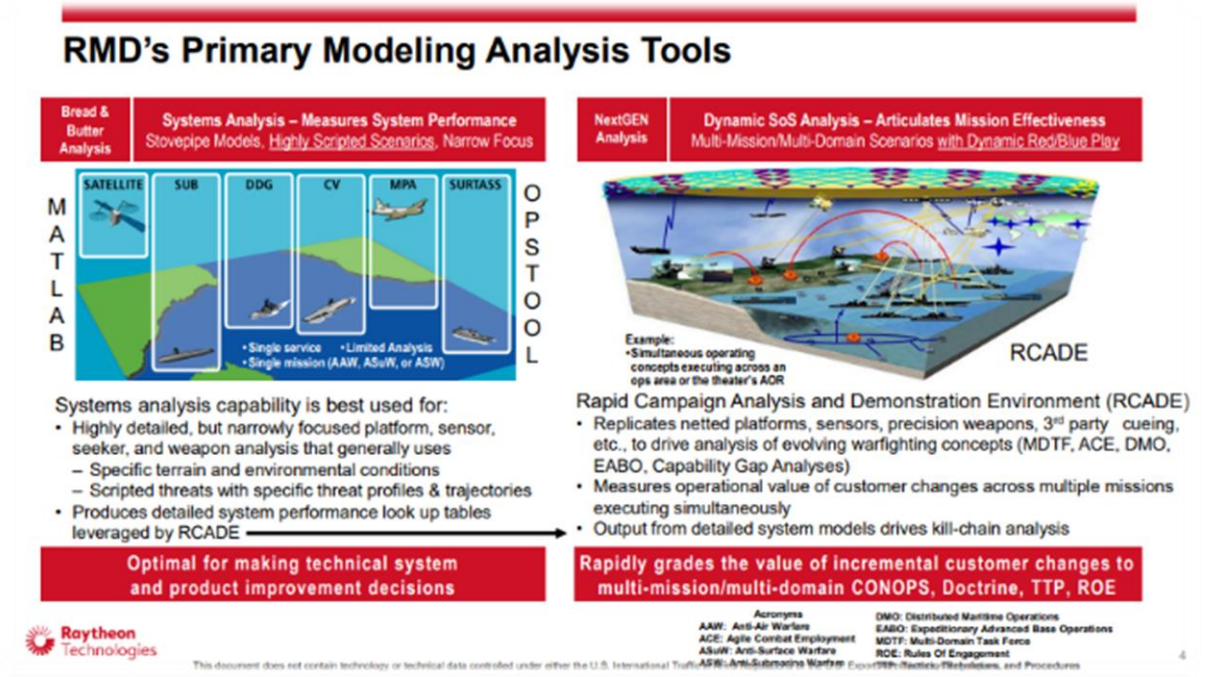


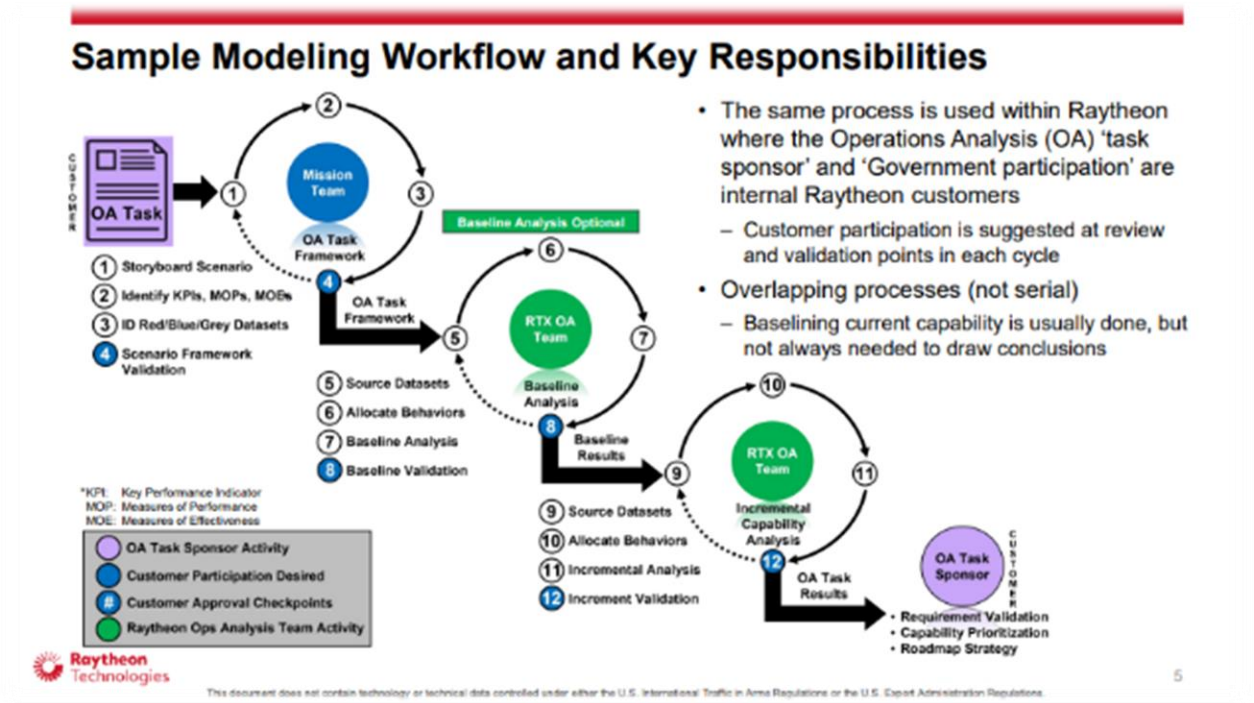


Regional and Theater-wide Integrated Air and Missile Defense Modeling and Simulation

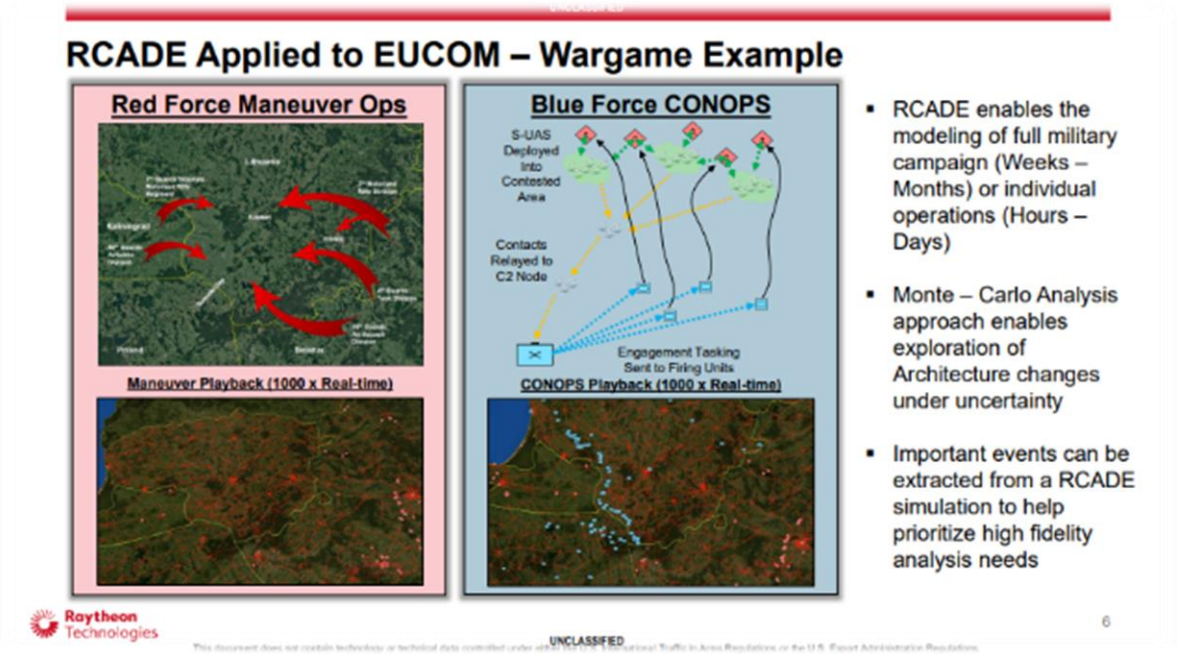
By Mr Sidney RODRIGUES

NATO members require layered, Integrated and Air Missile Defense to protect themselves against an evolving regional threat as today's complex geopolitical landscape and Ukraine conflict illustrates. Many NATO members have existing / current force capability against current threats. Effective modeling and simulation can show performance and efficacy of tactics against near and mid-term threats as well as scenarios including mass attack scenarios.





Raytheon utilizes a variety of M&S tools with a key one being the Rapid Campaign Analysis and Demonstration Environment (RCADE) that replicates netted platforms, sensors, precision weapons, and cueing all to drive analysis of evolving warfighting concepts. This tool, combined with others, measures operational value of system upgrades and / or changes across multiple missions executing simultaneously that drives kill-chain analysis.

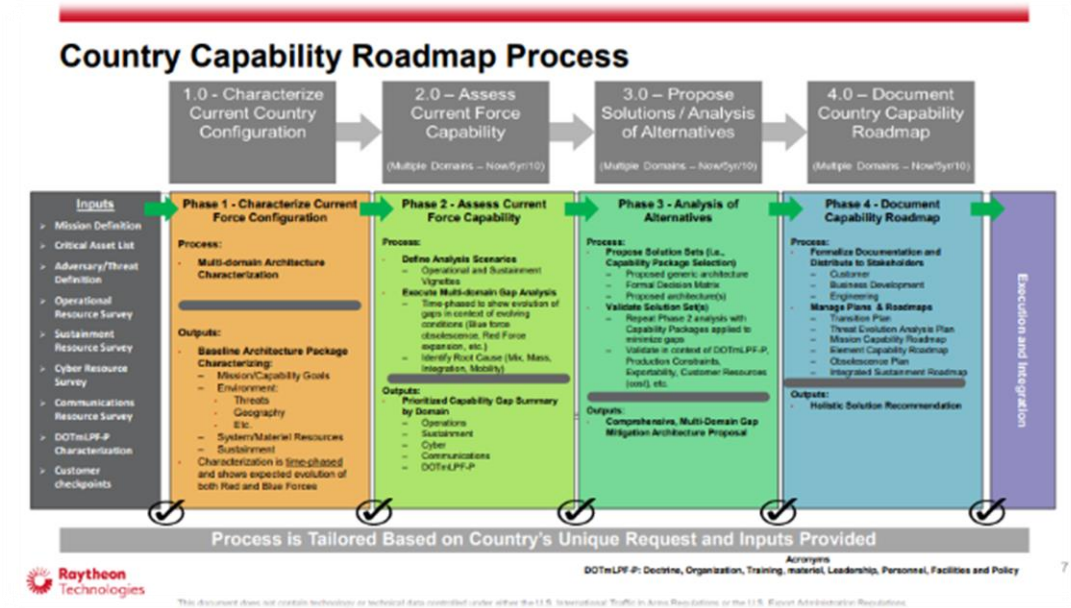


This paper will give an overview of this M&S environment and process that includes how we:

1. Characterize Current Country/Region Configuration,

2. Assess Current Force Capability and

3. Propose Capabilities with material solutions based on Modeling, Simulation, and Analysis. This presentation will address these questions and provide representative regional Modeling, Simulation, and Analysis results. •



How training and Modelling & Simulation could support Deterrence and Defence from an IAMD perspective?

By Mr Stephane GIRARDEAU

Air & Missile Defence as a basis of NATO military strategy is one of the key mission which require Modelling & Simulation in direct support of training.

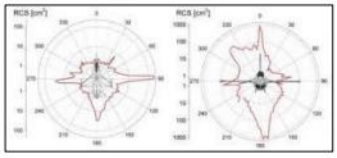
Therefore, during air and missile defence system development process, each defence company might use Modelling & Simulation key principles.

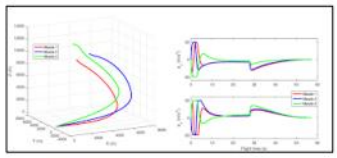
Among those principles, system architecture should be considered in order to elaborate training interface based on defined Tactics, Technics and Procedures (TTPs).

Nevertheless, as threat is evolving, defence industry might consider adaptive training models & simulator. For instance, providing tools to explore and/or experiment system TTPs shall support of the key pillar of IAMD mission, DETERRENCE.

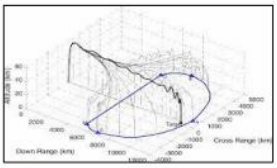
Key principles of IAMD Modelling & Simulation

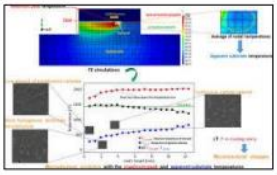
- Modelling : radar (passive, active) _ I/R
  - Detection : radar (passive, active) _ I/R
  - Interception : missiles,
  - Collect, analyse, use information : DATABASE
- Simulation
  - Simulate threat trajectories : access to information, expertise
  - Geography / Weather : influence on detection/tracking
  - Full system : from detection to interception
- Command & Control
  - Planning : AMD mission, threats
  - Wargaming : airborne / SBAMD system





- Challenges
  - Detection :
    - Current threat : ballistic missiles
    - Emerging threats : hypervelocity, glide missile, UAVs
  - Interception :
    - Current effectors : cooperative engagement (LOR, EOR)
    - Emerging effectors : direct energy weapons, C-UAVs jammer
  - C2 :
    - Integration : level of interaction between airborne - SBAMD
    - Scenario-based : basic training vs realistic CAX exercise





Modelling & Simulation in support of IAMD training

- Basic component system training
  - How to use system : 21st century learning process
  - Save resources : accelerate qualification
- Tactical weapon training
  - How to employ vs threats
  - Save resources : cost effective (maintenance, airborne availability)
  - Accelerate certification / evaluation
- Air & Missile Defence Integrated training
  - How to execute IAMD mission
  - Save resources : complexity of scenario, unique threats (ballistic missile)
  - Lessons Learned : recording, play back

Potential ways of IAMD training improvement

« from Thales industry perspective »

- Industry – warfighters interactions : EXPLORE together
  - Modelling : threats and defence systems developments
    - Short & lon terms perspectives
    - New offensive capacities
  - Simulation : current, alternate operational tactics
    - Complexity of joint operations
    - Capacity to adapt, create attack vs defence design

INTEGRATED AIR & MISSILE DEFENCE
CENTRE OF EXCELLENCE
Souda Air Base, Chania, Greece
https://iamd-coe.org/