

A New Dimension of Air-Based Threats Germany, the EU, and NATO Need New Political Initiatives and Military Defense Systems

Christian Mölling, Torben Schütz and Zoe Stanley-Lockman

The range of air-based threats is expanding with considerable speed and intensity. The main reason is the proliferation of technologies and weapons systems. Germany could play a leading role in the necessary adaptation of arms control regimes and in the development of new air defense capabilities. To this end, Germany should initiate a PESCO project on short-range air defense and an air defense capability cluster within NATO.

1 The End of Western Air Superiority

Air superiority is a key condition for armed forces to be able to act. It is needed to operate without significant restrictions from enemy combat aircraft and other airborne threats. Since the end of the Cold War, NATO countries have enjoyed clear air superiority in any conflict, being able to destroy possible enemy air forces and air defense capabilities early on. The resulting absence of enemy threats from the air has led NATO countries to dismantle most of their own air defense capabilities since the end of the Cold War.

However, given the horizontal and vertical proliferation of technologies and weapons systems in recent years, the range of air-based threats has expanded and their intensity increased. NATO forces therefore need to rethink their position on air defense capabilities.

Horizontal proliferation means that a growing number of countries have aircraft and missiles that represent airborne threats. Vertical proliferation comes in four shapes: First, there have been technical innovations or improvements in materials which were transferred to existing aerial systems. Second, unmanned aerial vehicles (UAVs) have added a new category of threats, enabling faster reconnaissance and engagement of targets. In addition, UAVs are quickly and easily available for a large number of states. Third, the military's aerial domain has become

linked to a new domain: the cyber and information space. Digitalization impacts all areas of the armed forces, creating new opportunities as well as new vulnerabilities. Fourth, due to their commercial availability, these newer technologies (UAVs and digital applications) can also be obtained by new players such as terrorist organizations.

This transformation is driven by the major changes underway in the global economy. It is nearly impossible to stop their repercussions on the military domain. Increasingly, new technology gets developed primarily for commercial reasons and global civilian markets. State-financed (armaments) programs, in contrast, have less and less influence on which technologies are available. Also, the success of the armaments industry in emerging economies means that an ever greater number of airborne weapon systems are becoming available on the world market.

1.1 Increasing Military Insecurity at All Levels

These developments create challenges at all levels of military action, i.e. in strategic, operational and tactical terms along the entire technological spectrum.

At the strategic level, the proliferation of strategic bombers with stealth characteristics or hypersonic weapon systems makes relations between states less stable. The faster and the harder to detect missiles become, the less time political systems have to react to an attack. The situation becomes even more dangerous if nuclear-armed countries are involved. Missiles moving at hypersonic speed can reduce the advance warning time of an attack between the USA and Russia from about 30 minutes to six minutes. This increases the pressure on political decision-making processes, which can lead states to adopt more aggressive doctrines – declaring, for instance, that defensive measures and counterattacks will be activated in response even to a first warning (launch on warning).

At the operational level, military action is primarily affected by the rapid progress in aircraft and cruise missile technology (stealth characteristics, higher speed) as well as by the proliferation of precision munitions. As a result, Western militaries are forced to develop new concepts of mobility, protection, deployment, and supply.

At the tactical level, i.e. on the battlefield, even very small units need to develop their own air defense capabilities in order to respond to the increasing use of small UAVs, which can serve as reconnaissance aircraft for artillery strikes, for disrupting communication links, or as weapon carriers.

In addition, cyber threats and electronic warfare permeate military decision-making at every level and jeopardize communication and coordination between and within armed forces. For example, UAVs can distort information transmissions between systems and deceive the enemy, but they can also interfere with control and signal transmission to and from other UAVs.

Germany as well as Europe and NATO should recognize that they no longer possess air superiority, at least for now. Yet the fact that many NATO countries continue to base their military operations on the misconception that they still do should be taken as an incentive to take a closer look at existing and future threats and examine possible responses and defense mechanisms.

2 A Confusing Threat Situation

In the future, more and more players will have access to technologically advanced combat aircraft and guided missiles as well as new airborne systems such as drones. Both developments make it difficult for Western armed forces to react effectively. This makes the threat situation ever more difficult to calculate.

2.1 Evolution in Aircraft and Guided Missiles

Even now, the expansion of defense industry capabilities in the aviation sector is contributing to the proliferation of airborne threats such as combat aircraft or armed drones.

In particular, emerging economies including China, India, South Korea, Brazil, and Turkey are trying to join the exclusive club of combat aircraft manufacturers in the US, Europe (especially Western Europe), and Russia. Stealth technology and the teaming of manned aircraft with unmanned systems are the two most important technological innovations for future combat aircraft. Essentially, all the above-mentioned countries are currently starting to develop modern combat aircraft.

Missile technology has proliferated in recent decades. While the political focus is on nuclear payloads (e.g. Iran, North Korea), the same technological knowledge can also be applied to missiles with conventional warheads.

In the future, long-range missile systems will be able to bypass areas covered by modern air defense systems. Also, the military value of ballistic missiles will increase over the next decade with the introduction of hypersonic gliders as alternative warheads. Extremely maneuverable in comparison to existing warheads, these gliders are better at evading increasingly powerful missile defense systems.

Today, there are also more countries that possess technically advanced cruise missiles than just a few years ago. Russia last demonstrated its progress in this area during the Syrian civil war, when missiles were fired from warships in the Caspian Sea that flew over Iranian and Iraqi territory before reaching their targets. Future cruise missiles will be developed with a focus on low detectability. They are also expected to fly at hypersonic speed within the next decade. This increases their ability to survive in the face of enemy air defense systems.

2.2 Revolution in Unmanned Aerial Systems

Unmanned systems create new military opportunities for both state and non-state actors (as summarized in Table 1). State armies can now conduct long-distance reconnaissance flights and - in the case of armed drones – make immediate use of the reconnaissance results for attacks. For most armies, with the exception of the US and Israel, this is new - especially compared to the lengthy processes of earlier analysis frequently based on the need to develop and evaluate photographs. In contrast to UAVs, aircraft carrying reconnaissance equipment can only do quick flyovers. They simply lack the fuel to observe targets for longer stretches of time.

Table 1: Use of UAVs: Missions and Actors#

		Actor	
		Non-State	State
Missions	Intelligence, surveillance and reconnaissance (unarmed)	Short reconnaissance flights (with short loitering time above target) to observe enemies in from close proximity	Short- and long-endurance intelligence gathering from different altitudes and with different payloads/sizes
	Selecting and engaging targets (armed)	Armed UAVs with small payloads: tactical ‘bombers’ (e.g. with mortar shells) and expendable suicide platforms that self-detonate	Same as non-state plus option of equipping military UAVs with heavier payloads Swarms: Decentralized operations which complicate the opponent’s identification and engagement of targets by simultaneously deploying multiple UAVs
	Other	Psychological tactics and propaganda (threat to decision-making ability of the opponent)	Similar to non-state actors, plus use in electronic warfare

More and more state armies are using UAVs: At least 90 countries have UAVs for reconnaissance missions in their arsenals.¹ Some 30 countries, nine of which are NATO states, also own armed UAVs or are in the process of developing them. UAVs have become important, too, for sophisticated armed forces beyond the US and Europe, as demonstrated by Russian-backed forces’ extensive UAV use in Ukraine. While Russia does not field any large UAVs, its armed forces seem to have developed a tactic of using small UAVs as spotters, which fits neatly into the traditional Soviet and Russian emphasis on artillery and medium-range firepower. Such artillery can be used more effectively with accurate and real-time intelligence gathered and transferred by small UAVs. These are also emblematic of Russian hybrid or ‘below-threshold’ warfare tactics: Moscow’s electronic warfare and information campaigns are aimed at exploiting US overdependence on satellites and Western spectrum superiority.

Low-resource armed forces in particular see an advantage in the use of UAVs as a comparatively inexpensive air force. Examples range from Nigerian forces deploying armed UAVs in 2016 to attack Boko Haram’s logistics bases to Azerbaijani forces using a UAV programmed to self-detonate on impact during the Nagorno-Karabakh conflict of the same year.

Yet the biggest benefits from the asymmetric advantage created by UAVs accrue to non-state actors: For the first time, they can conduct air reconnaissance and use it to coordinate attacks or guide suicide bombers to their targets. Affordable, commercially available, and user-friendly UAVs have therefore become a weapon for non-state actors. They do not require large logistical operations, space or much time to start – which many non-state actors, ranging from the Islamic State to extremists in the Philippines to drug cartels in Mexico – have come to understand.

In addition, UAVs have a significant psychological effect, regardless of whether they are armed or not. Just as fear of landmines affects the movements of armed forces

and civilians, fear of surprise attacks by UAVs limits military operations. In the battle for Mosul in 2016/2017, Iraqi troops were endangered by UAVs², even in walled-in open spaces, which changed movement patterns and made even quiet zones dangerous for soldiers.

UAV technology is still in its infancy. Future generations of drones are likely to overcome current limitations such as low speed and lack of stealth characteristics. Additional variations will be added in the future. For instance, swarms of UAVs may be able to overcome conventional air defense systems. They will overwhelm the defense because they present more targets than can be simultaneously engaged. Swarms are therefore more resilient than traditional platforms that operate alone or in smaller formations. The redundancy of abilities within the swarm allows the role of a destroyed UAV to be taken up by another.

2.3 Digitalization Makes Airborne Capabilities More Vulnerable

At the intersection of the air domain and the cyber and information space, digitalization is creating new vulnerabilities for the armed forces as well as new capabilities for the enemy. Russia used UAVs to „bomb“ Ukrainian soldiers with intimidating SMS messages. This “high-tech version of dropping leaflets on enemy battlefields”³ underscores the flexibility of UAVs. Besides using UAVs for electronic warfare in Ukraine, Russia in 2016/2017 also successfully disrupted American UAVs in Syria – despite their encrypted signals and anti-interference measures.⁴ At times, the US was unable to make use of its surveillance and reconnaissance capabilities.

More intensive digitalization makes communication, navigation, and warning systems ever more vulnerable. Disrupting or manipulating such systems can decisively influence airborne operations: In October 2007, Israel hacked Syrian air defense systems to manipulate the representation of Israeli aircraft positions. This allowed Israel to avoid detection during an operation in Syr-

ian airspace.⁵ Cyber sabotage is not only a threat to air defense networks but can also be used for attacks against increasingly digitalized weapon systems such as modern fighter aircraft.

3 Three Building Blocks: Arms Control, Air Defense Systems and Cyber Security

To respond to these multiple challenges, Europe should push for new arms control and non-proliferation measures while further developing its own defense systems.

3.1 Expand and Adapt Arms Control

A new arms control regime could address some of the strategically destabilizing effects of airborne threats such as hypersonic weapons systems. Already existing non-proliferation treaties are also helping to slow down the spread of technology, where larger UAVs, modern combat aircraft, and modern ballistic missiles and cruise missiles are concerned. However, these treaties should, at a minimum, also include other relevant states such as China and India, which currently are not members.

However, many technologies and the systems they enable cannot be adequately regulated by such measures. They are commercially available and require little adaptation for military or terrorist purposes. New defense systems are therefore also necessary.

3.2 Construct Modern Air Defense Systems

Future defense systems must be qualitatively and quantitatively capable of dealing with the new threats. Air defense is to be understood as a system of overlapping engagement ranges of different air defense systems. Moreover, when choosing defensive measures, it no longer makes sense to distinguish between „traditional“ and „new“ threats. Even traditional ground-based air defense requires technological innovations, for example in lasers and electronic warfare.

Most Western armed forces today have only a minimum of air defense systems for the medium to long range (four to 30 kilometers). Air defense systems with short ranges (up to eight kilometers) were largely dismantled over the last two decades.

3.3 Use European Cooperation to Strengthen Autonomy

Building a multi-layered, integrated air defense is a common challenge for all European countries in terms of procurement and operation. Effective defense is only possible if threats can be identified early and jointly. National systems are not sufficient.

Closer European cooperation and the acquisition of a sufficient number of systems would strengthen Europe's strategic autonomy in a key area. It would also have positive effects on transatlantic relations. A greater European contribution to air defense would relieve the burden on the United States, which is currently a major capability provider. New procurement would also strengthen industrial cooperation with the USA in some segments. US manufacturers provide essential components for today's medium- and long-range defensive systems, such as Patriot, and future tactical air defense systems such as TLVS. In addition, it is NATO that organizes air defense in Europe. For short-range air defense systems, European solutions are likely because Europe has extensive defense industrial capabilities in this area.

3.4 Germany as a Framework Nation in Air Defense

Germany could, for good reasons, assume the role of a driver and partner vis-à-vis the other European states: First, it traditionally maintains many of NATO's air defense capabilities. Second, it would like to act as a main partner in capability development for the armed forces of other NATO and EU countries in NATO's Framework Nation Concept and in PESCO. Germany could fulfil this role through the following concrete initiatives:

- PESCO project Short-Range Air Defense: As one of the next PESCO projects, Germany could propose the joint development and procurement of a short-range air defense system by several European armed forces. The need is obvious, and air defense is an EU priority in capability development. Joint procurement would ensure technical interoperability and higher life-cycle cost efficiency.
- Framework Nation for an air defense capability cluster: For existing armed forces, Germany could initiate closer cooperation between European air defense units. This could take place in the context of the Framework Nation Concept that Germany introduced into NATO. This would increase the alignment of processes and standards and thus military effectiveness. Accordingly, Germany should consult closely with its European partners when deciding on a tactical air defense system (TLVS) and prioritize the European interoperability of systems.
- EU-NATO cooperation on hardening (increasing resistance to cyber attacks and electronic warfare) of digital system components: On this issue, responsibilities and competences are shared between states, the EU, and NATO. The EU sets the standards and rules, especially for applications of civilian origin. The goal

of the alliance partners must be to secure networks and components against attacks via the electromagnetic spectrum and cyber sabotage. Germany should intensively promote the establishment of a transatlantic community of experts in addition to the existing institutional exchange between the NATO Centre of Excel-

lence for Defense in Cyberspace and the EU. To this end, the establishment of a cyber competition similar to the 'Cyber Grand Challenge' of DARPA, the US Department of Defense agency responsible for innovation, would be a good idea - and would certainly attract the interest of the partners.

Torben Schütz, Associate Fellow, Program Security, Defense, and Armaments, German Council on Foreign Relations (DGAP)

Dr. Christian Mölling, Deputy Research Director, German Council on Foreign Relations (DGAP)

Zoe Stanley-Lockman, Associate Research Fellow, Military Transformation Programme, Institute of Defence and Strategic Studies (IDSS), S. Rajaratnam School of International Studies (RSIS)

Notes

- 1 New America Foundation (2018), "Who Has What: Countries with Armed Drones", <<https://www.newamerica.org/in-depth/world-of-drones/3-who-has-what-countries-armed-drones/>>
- 2 Solomon, Ben C. (13.04.2017), "Witnessing and ISIS Drone Attack", Washington Post, <<https://www.nytimes.com/video/world/middleeast/100000005040770/isis-drone-attack-mosul.html>>
- 3 Medium (18.05.2017), "Electronic Warfare by Drone and SMS", <<https://medium.com/dfrlab/electronic-warfare-by-drone-and-sms-7fec6aa7d696>>
- 4 NBC News (10.04.2018), "Kube, Courtney, Russia has figured out how to jam U.S. drones in Syria, officials say", <<https://www.nbcnews.com/news/military/russia-has-figured-out-how-jam-u-s-drones-syria-n863931>>
- 5 Katz, Y. (29.09.2010), "And They Struck Them With Blindness", The Jerusalem Post, <<http://www.strategypage.com/militaryforums/512-40367#startofcomments>>

DGAPkompakt / Nr. 9 / June 2019



Dieses Werk ist lizenziert unter einer [Creative Commons Namensnennung – Nicht kommerziell – Keine Bearbeitungen 4.0 International](https://creativecommons.org/licenses/by-nc-nd/4.0/) Lizenz. This work is licensed under a [Creative Commons Attribution – NonCommercial – NoDerivatives 4.0 International License](https://creativecommons.org/licenses/by-nc-nd/4.0/).



Deutsche Gesellschaft
für Auswärtige Politik
German Council on
Foreign Relations

Die DGAP trägt mit wissenschaftlichen Untersuchungen und Veröffentlichungen zur Bewertung internationaler Entwicklungen und zur Diskussion hierüber bei. Die in den Veröffentlichungen geäußerten Meinungen sind die der Autoren.

Rauchstraße 17 / 18 · 10787 Berlin
Tel. +49 (0)30 25 42 31 -0 / Fax -16
info@dgap.org · www.dgap.org

Herausgeber

Deutsche Gesellschaft für
Auswärtige Politik e.V.
ISSN 2198-5936

Redaktion Eva-Maria McCormack,
Bettina Vestring

Layout/Satz Andreas Alvarez

Designkonzept Carolyn Steinbeck · Gestaltung