/M-Sec Report 2017

Aviation in Times of Global Turmoil

Living ideas – Connecting lives


AIRBUS
AIRBUS

/Content

/Foreword

These days, we are in a constant state of high alert, which has significantly increased over the last couple of years. Airports and airlines have equally been targeted by terrible terrorist attacks. This makes aviation security all the more relevant in the process of handling passengers, baggage, cargo and staff. Establishing and operating a reliable system is more important than ever. The aim is to maintain the level of success of aviation in terms of prosperity and development and – most importantly – to guarantee the safety and security of air transport.

Under the patronage of the Chairman of the Supervisory Board of Munich Airport, Dr Markus Söder, and Ambassador Wolfgang Ischinger, Munich Airport is hosting its very first Munich Aviation Security Conference, M-Sec. We have succeeded in initiating a high-ranking conference on a strategic policy level, dedicated to aviation security in the face of global threat. A debate of this kind and quality opens up new opportunities to strongly anchor the important topic of aviation security among top policymakers.

During the course of M-Sec, current challenges in aviation security will be discussed by experts in the fields of politics, military, economy, research and NGOs.

This detailed report will accompany and complement the conference and address the core topics: information sharing, cybersecurity, the protection of critical infrastructure, the opportunities and risks associated with unmanned aerial vehicles (UAVs) as well as the fight against international terrorism. Experts from various organisations will analyse and evaluate these topics in the report from different points of view, which will also be up for discussion throughout the conference.

Munich Airport is Europe's first and only five-star airport in the third consecutive year, winning the World's Best Airport Terminal Award in 2017 for its Terminal 2. Such awards not only express the quality and high performance of the airport, but also place us under obligation to continuously improve. Munich Airport aims to go one step further by living up to its local responsibilities – including in the area of aviation security – and making the protection of its customers, employees and all other guests a top priority. We are convinced that high-quality security processes are commensurate with high levels of customer satisfaction.

We wish for a successful conference full of many productive discussions, which will hopefully inspire us to find solutions to meet the challenges of our time.

Dr Michael Kerkloh
President and CEO
Munich Airport

Andrea Gebbeken
CCO
Munich Airport

Thomas Weyer
CFO
Munich Airport

/Greeting

M-Sec, the Munich Aviation Security Conference, has been developed as a new interdisciplinary and international platform for aviation security experts providing the opportunity to discuss current issues and challenges of aviation security in a political and strategical setting.

As Chairman of the Supervisory Board of Munich Airport and Patron of M-Sec, I am delighted to contribute to fostering the debate on this important topic from its various angles within such a high-ranking format. Especially in light of current threats, aviation security is of highest priority for politics and the public.

As many internationally renowned experts from the various different fields of aviation security are contributing to M-Sec, this exchange of information and best-practices offers an ideal opportunity to highlight the manifold aspects of the topic from different perspectives and at the highest level in terms of content and in-depth insights into the topic.

Munich Airport has been proven to be one of the best airports worldwide – illustrated by numerous accolades. For the second time in a row, Munich Airport has been awarded as the only five-star airport in Europe. It is therefore a natural next step to initiate with M-Sec this debate on aviation security here in Munich, supported by my co-patron Ambassador Wolfgang Ischinger, Chairman of the Munich Security Conference.

In times of a globalised world, aviation and international air traffic connecting the world have gained more importance than ever before. It is a cornerstone for economic growth and prosperity in our country and a driver of growth in the job market. World air traffic has been growing constantly for 60 years. In spite of global crises and temporary decreases of traffic numbers, the global air traffic volume is increasing constantly with a long-term perspective. This trend can also be observed in Germany: In 2016, German airports registered a total count of more than 223 million passengers. By 2030, this number will have risen by 35%. Especially Munich Airport – opened in 1992 – has shown just how important an excellent connection to the international network of air routes can be for an economic area. The economic success stories and competitiveness of many Bavarian companies on international level in the past 25 years can be attributed to a not insignificant extent to Munich Airport as a dynamically growing aviation hub. The future development of Bavaria will remain closely connected to the development of international air traffic. It is crucial that Munich Airport can play its role in this growth of international air traffic, predicted by all aviation experts. Trust in this mode of transport plays therefore an essential role – particularly talking about security.

With M-Sec, we want to contribute to keep aviation and international air traffic on its successful track – even and especially when faced with tensions and threats by the international security environment. Together with partners from politics, the private sector, military, academia and non-governmental organisations, M-Sec Conference and Report will address the most pressing challenges of aviation security – particularly questions on threat information sharing, cybersecurity, securing critical infrastructures and, last but not least, how to deal with new and unknown threat scenarios. I wish the 2017 M-Sec every success, and its participants insightful and exciting discussions as well as a stimulating debate – at the conference and beyond.

Dr Markus Söder
Patron of M-Sec; Bavarian State Minister of Finance, Regional Development and Regional Identity; Chairman of the Supervisory Board, Munich Airport

/Patrons' Statements

»Munich Airport is Bavaria's gateway to the world. Today more than ever, we consider aviation security as one of our core challenges.«

Dr Markus Söder

Patron of M-Sec

Bavarian State Minister of Finance, Regional Development and Regional Identity;
Chairman of the Supervisory Board, Munich Airport

»Not since the end of the Cold War has the world been such a crisis-torn and dangerous place as it is today.«

Ambassador Wolfgang Ischinger

Patron of M-Sec

Chairman, Munich Security Conference

Munich Security Conference msc
Münchner Sicherheitskonferenz

/Introduction of Knowledge Partners

Dimitris Avramopoulos
Commissioner for Migration, Home Affairs & Citizenship, European Commission

Marc Bachmann
Head of Aviation and Defence, Bitkom e.V. - Digital Association of Germany
Marc Fliehe
Head of Information Security, Bitkom e.V. - Digital Association of Germany

Anna M. Barcikowska
Head of Industry Relations, NATO Communications and Information Agency
Jill O'Donnell
Industry Relations, NATO Communications and Information Agency

Douglas Barrie
Senior Fellow, International Institute for Strategic Studies

Norbert Barthle
Parliamentary State Secretary, Federal Ministry of Transport and Digital Infrastructure, Federal Republic of Germany

Alexander Borgschulze
Senior Vice President Corporate Security, Munich Airport; Chairman of the Executive Board, Bavarian Association for Security in the Economy (BVSW)

Frank Brenner
Director General, EUROCONTROL

Dan Chirondojan
Director Space, Security and Migration, European Commission Joint Research Center

Prof Dr Pascale Ehrenfreund
Chairwoman of the Board of Management, German Aerospace Center (DLR)

Prof Dr Elmar Giemulla
Honorary Professor of Aviation Law, Berlin University of Technology

Dr Emily Haber
State Secretary, Federal Ministry of the Interior, Federal Republic of Germany

Prof Dr Udo Helmbrecht
Executive Director, European Union Agency for Network and Information Security

Ambassador Wolfgang Ischinger
Chairman, Munich Security Conference

Sir Julian King
Commissioner for the Security Union, European Commission

Dr Hans-Georg Maaßen
President, BfV - The German Domestic Intelligence Service

Prof Dr Peter R. Neumann
Director, International Center for the Study of Radicalization and Political Violence, King's College London; Special Representative of the Chairperson-in-Office on the Fight against Radicalization, Organization for Security and Co-operation in Europe

Brigadier General Burkhard Pototzky
Head of Operations at German Air Operations Command, German Air Force

Dr Steffen Richter
Head of Section Aviation Security, German Federal Police

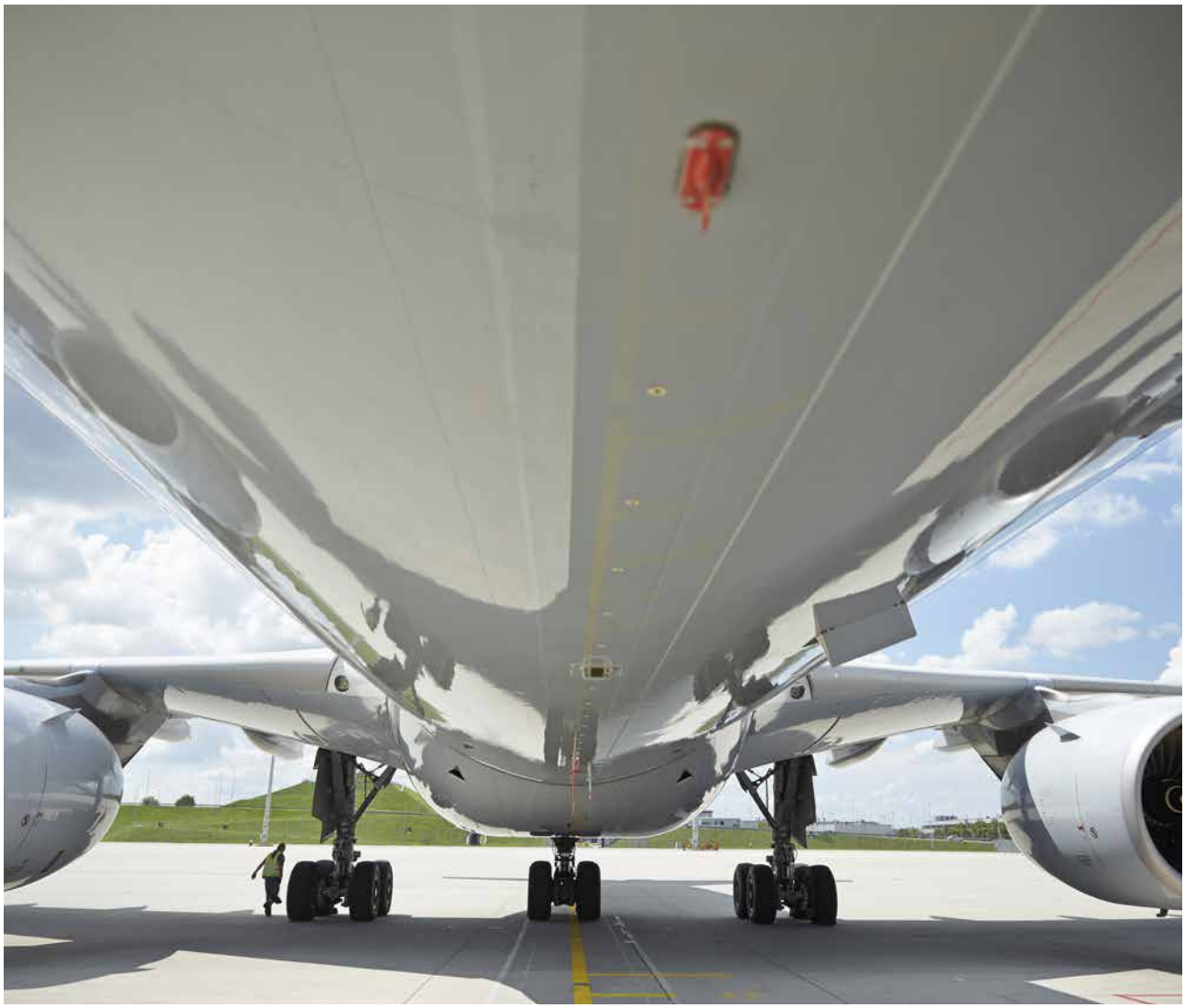
Alexander Sander
Managing Director, Digital Society e.V.

Jan Syré
Chairman, German Federal Association for Unmanned Systems (BUVUS)

Robert Viertel
Head of BDL Security Project, German Aviation Association (BDL)

Rob Wainwright
Executive Director, Europol

Sven O. Weirup
Chairman, European Aviation Security Center



/Crises, Conflicts, Terrorism – Aviation Security in a Turbulent World

Dimitris Avramopoulos
Commissioner for Migration, Home Affairs & Citizenship, European Commission

We live in volatile and unpredictable times. As our Union celebrates 60 years of bringing peace, stability and prosperity to the European continent, security remains among the top concerns of our citizens. The relevance of post-war multilateral bodies is severely tested by the multi-polarity of power in the international system. Our neighbourhood is ravaged by domestic conflict spilling over national borders and causing massive population displacements which challenge our social structures. 60 million refugees around the globe remind us of the need to live up to our legal, moral and political obligations and the fundamental values of our Union. Globalisation and increased mobility bring more opportunities but also more risks. Cyber criminality is on the rise. Terrorists are emerging both from within our societies and from our neighbourhood. Solidarity between us has become harder to ensure.

Our citizens are concerned about terrorism and the risks to their security – but equally do not wish to see their freedoms curtailed and mobility impeded. Aviation security lies at the very heart of this. It has never been easier or cheaper to travel than today, but this ease is not without risks.

On aviation security, a tightened security framework has been put in place around the world in the wake of the terrorist attacks of 9/11. EU airports are among the most regulated, controlled and secure spaces in the world. This framework serves to protect the travelling public from acts against civil aviation. It is constantly being improved and upgraded to ensure that it is up to date in terms of responding to evolving threats. But that does not mean they are risk-free. No airport is.

One thing is clear: it is no longer an option to work in silos anymore when it comes to security. We will never defeat terrorism in that way. This is why we have to continue our cooperation with key strategic partners on counter-terrorism, information sharing, police cooperation, cybercrime and cybersecurity.

Our approach has to be global. Owing also to the hard lessons of the past two years, the EU is slowly but surely going through a culture change on security, putting its own house in order, but also understanding that internal and external security are inevitably a continuum. Inside the EU, the European Commission has proposed essential building blocks towards a genuine and effective Security Union, starting with enhanced information sharing, the creation of an EU counter-terrorism centre at Europol and much closer cooperation on a range of issues - from border management, to radicalisation and terrorism financing to explosives and firearms, and even our criminal justice frameworks. Europe now has its own Passenger Name Record framework, a European Border and Coast Guard, and will soon have its own Entry-Exit System and a European Travel Information and Authorisation System at the external border.

Aviation security is no exception, with risk assessments taking place at EU level, common EU measures on mitigating the risk and a strong, united EU voice at international level both towards strategic partners and at multilateral fora.

However we still have a long way to go. Our geopolitical context will not change any time soon. As a Union, it is imperative to continue investing in strengthening our security partnerships with Turkey, the Middle East, the Western Balkans and Northern Africa.

Europe will never escape its geography. The conflicts in our neighbourhood are unlikely to dissipate quickly. We need to navigate this context with a steady compass, resolved to play a role befitting Europe's history, with a strong Security Union protecting our citizens at home, and a truly global voice in the world.

»Our approach has to be global. Owing to the hard lessons of the past two years, the EU is slowly but surely going through a culture change on security.«

Dimitris Avramopoulos, Commissioner for Migration, Home Affairs & Citizenship, European Commission

/On the Brink of Chaos – How to Deal with Global Uncertainties

Ambassador Wolfgang Ischinger, Patron of M-Sec; Chairman, Munich Security Conference

Not since the end of the Cold War has the world been as crisis-torn as it is today. The international security environment is more volatile than at any point since 1949. The liberal international order is under threat and the transatlantic partnership, which has long been one of its most fundamental and stable pillars, is facing uncertainties unseen in the Post-Cold War world.

In light of this extremely worrisome trajectory of the international order and the state of liberal democracy, this year's Munich Security Conference addressed a critical question: are we moving towards a »Post-Truth«, »Post-West« and »Post-Order« world? Three major underlying trends have become eminent. Outlining them might help us not only to better comprehend the current problems, but also to find answers on how to deal with them.

A loss of leadership

First, we can observe a distinct loss of Western leadership. In general, Western democracies have become both less willing and less able to actively shape international affairs. Syria and its horrible and seemingly infinite war is one of the most drastic examples for this.While Europeans have stood by and the US has been reluctant to engage, autocratic regimes assertively took action and created facts to which Western countries have been, more or less, impotent to react.

For decades, the United States have pursued an enlightened self-interest whose fundamental idea was simple: if the international order works and is upheld, the best possible environment for a secure and prosperous America exists. President Trump disagrees with this fundamental tenet: So far, his administration's policies have made clear that »America First« will often mean »America Only« or »America Alone«. Pulling out of the Paris Climate Agreement and the protectionist trade-policy agenda are only two major examples for this. His hesitation on NATO's Article 5 commitment is another. The British Prime Minister is completely occupied with managing Brexit and its fallout on the United Kingdom and the EU. Germany is, at this point, neither able nor willing to take up a more pronounced leadership role. Nor should it be. Instead, the EU as a whole needs to be a heavyweight in diplomacy and security policy. However, even if the necessary decisions are taken soon, this will take years to develop.

The loss of leadership goes hand in hand with a loss of international decision-making capability. In many ways, we are living in a »G-Zero world«, a phrase coined by Ian Bremmer already a few years ago. It is a world in which a relative Western decline and the rise of nationalist and protectionist policies have created a vacuum of power. In the meantime, non-Western actors have begun to assume more prominent roles and attempt to build structures in parallel or even to the detriment of multilateral frameworks which have formed the bedrock of the liberal international order since 1945. This comes at a time when the need for unified international action is, in principle, more urgent than ever before. The importance of global governance is obvious, but institutions like the UN Security Council, the G7, or the G20 are often unable to act decisively.As a result, the international order is at risk. Moreover, regional security systems are under threat: in the Euro-Atlantic area, in the Middle East – not least in the Gulf –, and in the Pacific.

»In several key geopolitical areas of the world, risks of military incidents and unintended escalations have sharply increased over the last few years.«

Losing trust

The geopolitical retreat of the West and the resurgence of authoritarian political forces are accompanied by a fundamental erosion of belief in the reliability of facts, in truth and reality. The »post-truth« trend comes with a loss of trust in democratic processes and a decreased faith in the value of democratic institutions, and even in democracy itself. A growing number of citizens in democracies express sympathies for authoritarian models and systems of government. Liberal democracies have proven to be vulnerable to disinformation campaigns, and in more than a dozen western countries, illiberal and populist parties are now part of the government. Even in countries in which populist parties receive only a small share of vote, their positions set the agenda. As a result, the demonization of globalization, multilateral cooperation and international responsibility is on the rise. When lies can win elections and facts are no longer a common base of political debates, there is a risk that illiberalism will benefit.

Lack of power

Third, a loss of the state monopoly of power is an increasingly determining factor on the national and international level. This touches upon all policy fields, but two aspects have a particularly disastrous impact on the aviation sector. International terrorism and Islamic jihadism are, on the one hand, playing a fundamental role in challenging and destroying state-structures across the Middle-East, be it Libya, Somalia, Yemen or even Turkey. Beyond that, failing states are breeding grounds for even more terroristic structures and civil-war-like confrontations. On the other hand, the high number of recent terrorist attacks in Western countries, particularly in Europe, puts those societies and political systems under pressure of securing safety for their citizens and simultaneously preserving open and free societies. On a similar level are cyber attacks and cyber warfare undermining statehood and sovereignty. Is our critical infrastructure, including aviation, safe from potentially catastrophic cyber attacks? The answer, I'm afraid, is not clear yet.

More diplomacy

Having offered a rather grim analysis of an eroding international order, there are things we can do.

»First of all we need better and more diplomacy.«

Syria, for example, has been a battlefield for more than six years now. And not only are the Syrian people suffering in a barbarous way under this confrontation between a confusing number of groups and powers, but the so-called European migration crisis is also driven and shaped by these developments in the Middle East. The EU should take united and assertive action to negotiate a ceasefire and peace-building developments. With regard to the Ukraine conflict and US-Russian tensions, classic bilateral summitry could potentially ease the confrontation. Stable peace in Ukraine, however, requires sustained US engagement in international crisis diplomacy. This willingness to step up and to shape events is currently even more important in the Asia-Pacific area, probably the most dangerous conflict zone at the moment, where the North Korean regime keeps testing missiles and rocket systems, provoking the US and her allies in the region. Finally, the Gulf region is in dire need of more diplomacy as well, as demonstrated by the outbreak of the Qatar crisis.

More Europe

An obvious consequence of the current state of international peace and security is the need to strengthen the European Union. We may be on the cusp of new momentum. The outcome of the French elections offers new hope. And President Trump and US populism seem to be seen, by many Europeans, as a warning rather than as a model.

There is today a welcome new European seriousness about strengthening the EU's joint foreign and security policy. An overwhelming majority of some 74% of the population favors a stronger European role in the world, according to a 2016 Pew poll[1]. Even Eurosceptic citizens know that they are better served if a strong, large EU defends their interests internationally – and not just their small nation state. In this area, the EU could find renewed purpose and prove to its citizens that it is part of the solution, not of the problem. That means that delivering in this policy field is essential: We should discuss qualified majority voting in foreign policy matters. We need more pooling and sharing of military assets and of procurement processes. And we need much better intelligence-sharing. Why don't we propose a European FBI?

»We have a historic opportunity for the EU to transform itself into a security provider appreciated by the 500 million citizens the EU is supposed to protect.«

More transatlantic exchange

Although transatlantic relations are under stress, they are still a fundamental pillar of the West. Europe's only good option is to engage with the US administration as much as possible – there is simply no alternative to close cooperation between the US and the EU. Dealing with critical challenges – including the relationship with Russia, the wars in Syria or Ukraine, or the jihadist threat – is only possible in an effective manner through a unified Western approach. And nobody should forget the fact that Europe remains America's most important market. 45 out of 50 US states export more to Europe than to China, and European majority-owned foreign affiliates employ more than 4.1 million US citizens.[2]

Aviation security, like international security, depends on trust, on technology, and on reliable partners. Only through comprehensive and strong cooperative relationships can tomorrow's risks be effectively managed.

[1] Top 10 Risks for 2017 (Provided by Eurasia Group)[3]

1 **Independent America:** Donald Trump will use US power overwhelmingly to advance US interests, with little concern for the broader impact. Trump is no isolationist. He's a unilateralist. Expect a more hawkish – and a much less predictable – US foreign policy. Allies, especially in Europe and Asia, will continue to hedge. Rivals like Russia and China will test. US-led institutions will lose more of their international clout.

2 **China overreacts:** The need to maintain control of the transition ahead of next fall's party congress will increase the risk of economic policy mistakes that rattle foreign investors and international markets. President Xi Jinping knows this is a dangerous time to look weak and irresolute. US-Chinese tensions, particularly over commercial disputes and North Korea, might play out to make 2017 a dangerous year.

3 **A weaker Merkel:** Strong leadership from Angela Merkel has proven indispensable for Europe, which will face more challenges in 2017 – from Brexit negotiations and complex relations with Russia and Turkey, to Greece's finances and the fallout from a series of European elections. Though Merkel is likely to win re-election, she'll emerge as a weakened figure.

4 **No reform:** Some leaders, like India's Modi, have accomplished as much as they can for now. In Russia, France and Germany, reform will wait until after coming elections, and China faces an all-consuming leadership transition next fall. Turkey's Erdogan and Britain's May are fully occupied with domestic challenges. In Brazil, Nigeria and Saudi Arabia, ambitious plans will advance but fall short.

5 **Technology and the Middle East:** The revolution in energy production undermines the stability of states still dependent on oil and gas exports. New communication technologies enhance the ability of angry citizens to commiserate and organise. Cyber conflict is shifting the region's precarious balance of power. Finally, »forced transparency« (think Wikileaks) is dangerous for brittle authoritarian regimes.

6 **Central banks get political:** Western central banks are increasingly vulnerable to the same sort of crude political pressures that distort economies in developing countries. In 2017, there's a risk that Trump will use the Fed as a scapegoat, putting new pressure on future Fed decisions.

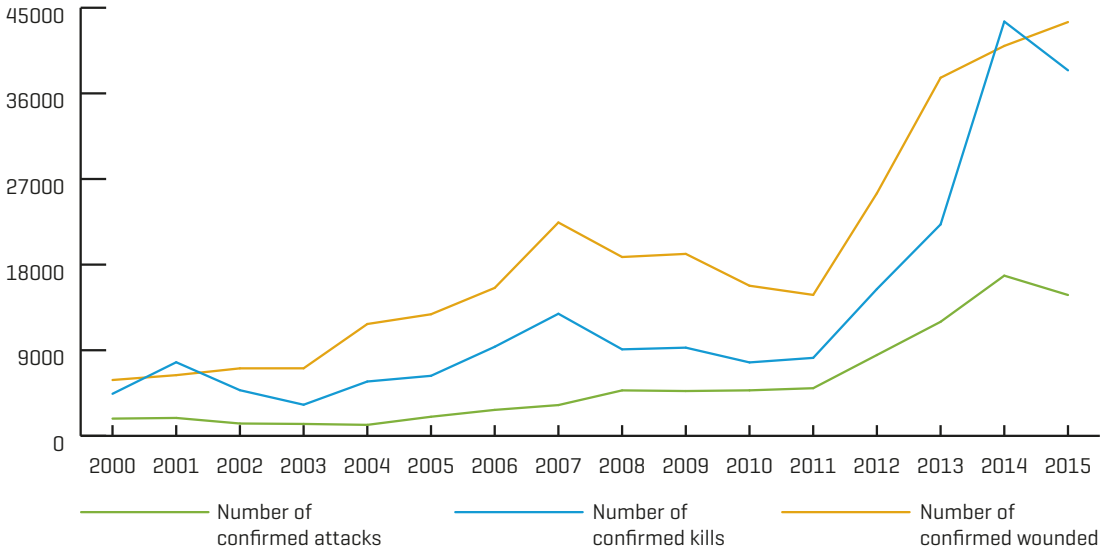
7 **The White House vs Silicon Valley:** Trump wants security and control. The tech firms want freedom and privacy for their customers. Trump wants jobs. The tech firms want to push automation into overdrive. The two sides also differ substantially on investment in science.

8 **Turkey:** In the wake of his narrow referendum victory, President Erdogan continues to use an ongoing state of emergency to tighten his control of day-to-day affairs. In 2017, he will exacerbate the country's economic problems and its tense relations with neighbours and with Europe.

9 **North Korea:** It's hard to know exactly when North Korea will have a missile capability that poses a clear and immediate danger to the US, but the DPRK appears to be approaching the finishing line at a time of deteriorating relations between China and the US. A tough Trump policy will continue to roil geopolitics throughout the region.

10 **South Africa:** Unpopular President Zuma is afraid to pass on power to someone he doesn't trust. Infighting over succession poses an obstacle to any effort on needed reforms and limits South Africa's ability to help stabilise conflicts in its neighbourhood.

[2] **Terrorist Attacks Worldwide, 2000 - 2015 (Source: START Global Terror Database)**[4]



/»The threat is very significant.« Aviation in Times of Terror

Interview with Prof Dr Peter R. Neumann, Director, International Center for the Study of Radicalisation and Political Violence, King's College London; Special Representative of the Chairperson-in-Office on the Fight against Radicalization, Organization for Security and Co-operation in Europe

ISIS is on fallback, the Trump administration and the coalition against ISIS are strengthening their military engagement in the Middle East and Europe is tightening its security measures. How would you estimate the current threat of terrorism in general and to Western countries?

The threat is very significant. We should not make the mistake of thinking that the defeat of ISIS in its stronghold in Syria and Iraq will mean an end to ISIS-related activity or terrorism. Rather on the contrary, the defeat of ISIS in Syria and Iraq may have the consequence in the short term that some of its activities spread further abroad. This will have effects in the Middle East, most probably increasing terrorist activities in countries outside of Syria and Iraq, in countries like Yemen, Libya and other places that are affected by instability and certain tensions. I also expect a continuation of terrorist activities in Western countries, especially in Western Europe, because ISIS has released various statements over the last six to eight months saying that people should no longer come to the Islamic State. Instead, they are called upon to stay in their home countries and carry out terrorist attacks and activities there. To some extent, that also explains the increasing number of terrorist incidents we have seen in Western Europe.

So-called »lone wolves« seem to be responsible for recent terrorist attacks, such as in London or Berlin. On the other hand, Manchester may have been planned by a network. How intense are ties between ISIS command structures and terrorist cells that might exist in European countries and other countries participating in the US-led coalition against ISIS?

Genuine lone wolves - people who radicalise entirely on their own and are not part of the command and control structures – are fairly rare. Even people who act on their own, lone attackers, are often members of wider networks and, in many cases, have relationships with ISIS in the Middle East. Anis Amri [Berlin attacker], for example, was without a doubt a lone attacker, but he had become radicalised as part of a network of jihadists that was active across Germany. And we know for a fact that he received instructions from ISIS networks in Libya and was in regular touch with them.

So, for me, he was a lone attacker but would not count as a lone wolf. The more we look, the more valid principles we find. What is particularly significant and what we have seen in the past 12 - 18 months is that even lone attackers are able to carry out attacks based on instructions they receive in real time via personal messaging services, like WhatsApp or Telegram, from ISIS members in Syria. These have often been referred to as »remote-controlled attacks«, »hybrid attacks« or »virtual mentoring« – members or affiliates of ISIS based in Rakka or somewhere in Libya giving instructions via personal messaging services. This was also the case, for example, in Germany last summer [attacks in Ansbach and Würzburg]. Both of these attacks were carried out by so-called lone wolves, but in fact they were both in touch with the Islamic State and received instructions in real time. This is a huge concern for security and intelligence services across Western countries because these personal messaging services are highly encrypted and very difficult to decrypt.

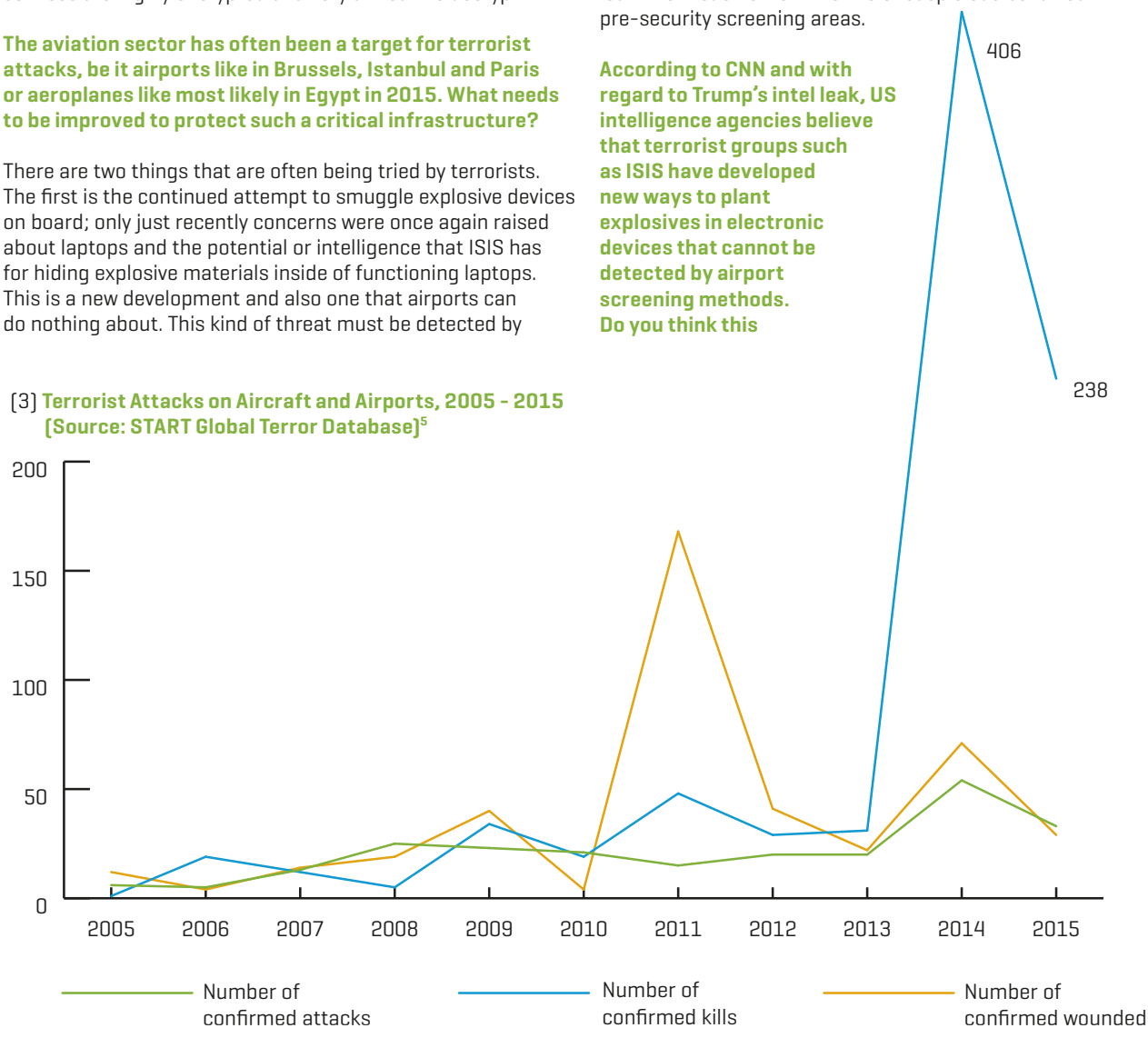
The aviation sector has often been a target for terrorist attacks, be it airports like in Brussels, Istanbul and Paris or aeroplanes like most likely in Egypt in 2015. What needs to be improved to protect such a critical infrastructure?

There are two things that are often being tried by terrorists. The first is the continued attempt to smuggle explosive devices on board; only just recently concerns were once again raised about laptops and the potential or intelligence that ISIS has for hiding explosive materials inside of functioning laptops. This is a new development and also one that airports can do nothing about. This kind of threat must be detected by intelligence services, who really need to stay up to date with whatever ISIS or Al-Qaida-related groups are developing to get explosive devices on board. These insights then have to be reported and conveyed to airports, airlines and national security agencies to safeguard against such threats.

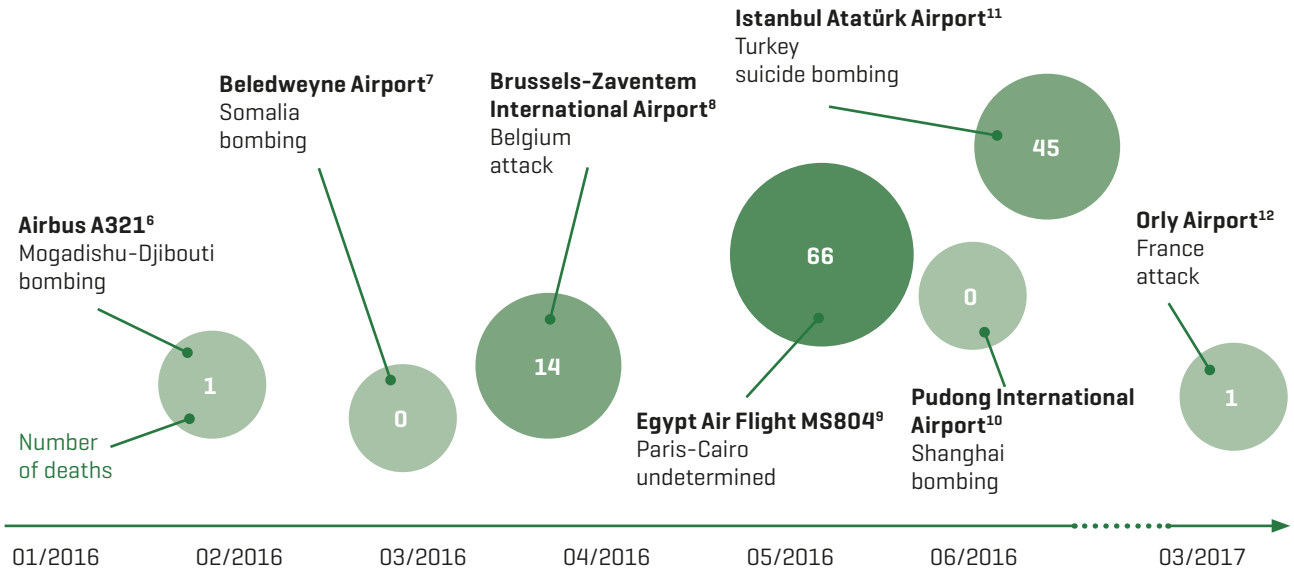
The second threat concerns suicide attackers inside the airports themselves. This is what we have seen not only in airports, but also in the case of Manchester, for example, and other similar venues. Terrorists are trying to carry out their attacks before reaching the security parameters rather than going through the security checks. At Brussels Airport, before the check-in area, in Manchester, right at the entrance of the concert hall – I think we need to be more creative in how we secure areas before the actual and formal security checks begins and in how to avoid people from assembling, since those are preferred areas of attack. We also need to learn from each other in terms of suspicious behaviour in pre-security screening areas.

According to CNN and with regard to Trump's intel leak, US intelligence agencies believe that terrorist groups such as ISIS have developed new ways to plant explosives in electronic devices that cannot be detected by airport screening methods. Do you think this

[3] **Terrorist Attacks on Aircraft and Airports, 2005 - 2015 (Source: START Global Terror Database)[5]**



(4) **Terrorist Attacks on Aircraft and Airports, 01/2016 - 05/2017**



is currently and in the future a realistic terroristic scenario? Would you agree that the US and UK decision to prohibit laptops and other electronic devices on flights starting in various Middle Eastern countries is an appropriate measure to face this threat?

I have no doubt that this is based on real intelligence and that this decision was not taken lightly. Of course we know that some bomb-makers within ISIS or Al-Qaida in Yemen are highly sophisticated and have been responsible for attacks that would have killed nearly hundreds of people in some instances. May I remind you of the bombs that were hidden in UPS packages or the attempts to hide and carry explosive devices in laptops and underwear a few years ago. These were not perceived threats, they were real. And in that sense I do think that the US and UK were left with little choice but to take this measure. Going forward we need to think more creatively about how we can overcome this and somehow make it possible to detect explosives that are hidden in laptops. Maybe the technology for this already exists or soon will, but I don't think banning laptops forever and everywhere is a good solution. As this is a serious threat, and there is nothing to suggest otherwise, it was the appropriate step to take. However again, going forward, I hope we will find a way of screening laptops for this particular threat more efficiently than banning them altogether.

How knowledgeable are terrorist groups like ISIS and their supporters in the field of cyber attacks? The German Domestic Intelligence Service stated that they were able to infiltrate an airport's energy supply system only by using publicly available information. Moreover, it seems to be possible to take control over an aeroplane by hacking the on-board entertainment system. Are those realistic terrorist scenarios?

When it comes to cyber attacks or cyber warfare, there is definitely a threat, but the threat has been largely one that has come from states or non-terrorist non-state groups – hacker collectives, for example. It's quite surprising that people have been talking about cyber terrorism or terrorist groups using cyber warfare for the past 20 years, but by and large nothing has happened. ISIS, for example, is very sophisticated when it comes to disseminating propaganda on the Internet and propaganda purposes in general, but it has not really systematically exploited the Internet in order to cause harm to its enemies. That does not mean it will never happen, I'm just saying that the evidence for cyber terrorism by ISIS or Al-Qaida is very slim. We need to prepare for this, but most of ISIS activities have been geared to actually carrying out more simple terrorist attacks, not more sophisticated ones. When ISIS speaks to its supporters, it tells them to drive cars into crowds or to take knives and attack random people on the street. Making things easier rather than more complicated is generally the way ISIS works and will continue to work. Again, it doesn't mean we shouldn't worry about cyber attacks happening in future, but none have happened so far and I do not believe it is a priority for ISIS right now.

In January 2017, ISIS published a video showing fighters using a new weapon: a drone armed with a bomb. Was this simply a single PR stunt or a new large-scale method of attack? And what needs to be done to prevent ISIS and other terrorist groups from making use of such technical equipment?

We have often seen ISIS showing off things in its propaganda videos, the use of aeroplanes, for example. It has never used aeroplanes, but the propaganda videos lead you to believe that it has a whole air force or fleet – which it doesn't, of

course. It often tries to show things in its propaganda that are not as systematic or widespread as it would have you believe. However, drones are a real issue, particularly in the West, where they are easily available, relatively cheap and not very difficult to use. I do think there is a real threat of drones being used as delivery mechanisms for explosive devices. Airports need to protect themselves from that, not only in terms of drones delivering explosive devices but also in terms of drones flying into the engines of aeroplanes. There is already a number of sophisticated technical systems out there that make it impossible to operate drones in particular areas. Those technical systems are being used at sports events, for example, and I think and I hope they are being used increasingly at airports as well.

To what extent do terrorist groups have access to missile systems that are able to shoot civil aircraft at average altitudes, such as the Russian BUK system used by Eastern Ukrainian separatists to shoot down MH17?

We know they are not being sold to terrorists. But one way terrorist groups get access to these weapons is, of course, through a number of terrorist groups operating in war zones, for example, and most prominently in Syria right now. Most of the weaponry ISIS obtained was captured from Syrian Army bases. Gaining access to this kind of weaponry is often a threat when terrorist groups hold territories and capture towns and cities from the enemy. This should always be a cause for concern and there is surely a good reason why airlines are not flying over Syria right now. It is the same with so-called stinger missiles, rocket-propelled grenades or similar systems that are either captured from enemies or, in the case of Syria, are falling into the hands of groups like ISIS because they are being joined by previous members of other groups that were supported with different kinds of weapons by certain countries. Those weapons, not BUK systems, but smaller, shoulder-held systems, were delivered to less extremist groups in the past. ISIS captured them or gained access to them by former members of those groups joining its ranks. Weapons ending up in the wrong hands is a massive risk if such weapons are being provided to war zones.

Recent data has shown that all terrorists who have carried out attacks in Europe were well known to security and police agencies. Would you say that screening passengers according to alleged risk groups is an effective preventive security measure? Given that measures such as racial profiling have been proven inefficient and costly, how would you evaluate the effectiveness of the PNR system?

In my opinion, those are two different things. Racial profiling – picking out people based on their skin colour, name, race or the assumption that someone is a member of a particular religion based on his/her name – is certainly ineffective and

the reason why there are no professionals advocating it. A lot of resources would end up being wasted on so many cases of suspicion based purely on religion or race. And, once the terrorists realise what you're doing, it will become rather ineffective. Eventually they will adapt to it and use operatives that do not typically fit those profiles. We know that 20% of ISIS recruits are converts, white people with Christian names, who converted to Islam and do not fit any racial profile. Therefore, racial profiling certainly does not work. What does work is having people who are suspected of being violent extremists based on their membership in special networks or certain behaviour in the past and who may be on no-fly lists or on lists of people being flagged up. In that sense, PNR is an important step, but it is even more important that European countries actually merge their databases. In Europe, we still have a potpourri of databases that are not connected to each other. Countries are still failing to provide all the names of the people that they consider to be a threat. That still makes it possible, for example, for someone flagged as a threat in the Netherlands to fly to Syria from Düsseldorf in Germany without being recognised as a threat by the security personnel at the airport. Security agencies are inefficient in terms of pooling names in their databases, so a Dutch person has a very good chance of flying from Düsseldorf or moving within the Schengen Area without being recognised by German or other national authorities because relevant information was never sent by the Dutch authorities. In my view, this is much more important than racial profiling. We need to get to a point where Schengen countries share their databases of named terrorist suspects, which is not yet the case.

Do you think Brexit will have a major impact on the European security architecture?

Since negotiations haven't even properly started yet, we don't know how they will end. Theresa May, the British Prime Minister, just said, security cooperation is the only area in which she not only wants to maintain cooperation with the European Union, but in which she actually wants to increase cooperation. So there is a clear recognition by the British that cooperation with the EU on security matters is vital to Britain, just as the EU benefits from the professionalism of British security agencies. I very much hope that everyone will recognise that this is not an area you should play politics with and that we can maintain the channels of cooperation that were established in the past. Also, that the UK can remain a member of Europol and will still be able to access European databases just like EU countries are able to benefit from the work of British security agencies.[13]

/Further Escalation? North Korea and the Implications for Asian Airspace

Though Asia-Pacific has been making headlines regarding its disputes in the South China Sea for years, ongoing escalations in the protracted conflict on the Korean peninsula pose ever more perilous threats for air traffic in the region.

North Korea – escalating politics

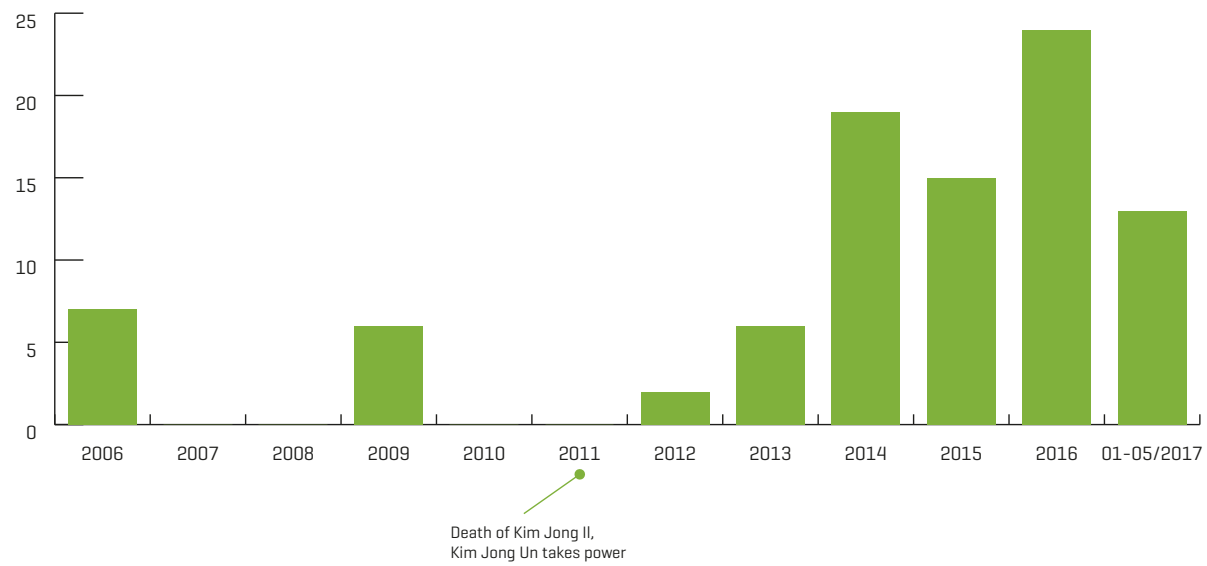
North Korea has put the world on edge. By conducting banned missile tests and promoting a weapons programme that is a »clear and present danger« to America, as James Mattis, the US Defence Secretary put it on 3 June 2017 at the Shangri-La Dialogue[14], North Korea aims to strengthen its negotiating position and its national unity at the same time. However, with thousands of rocket launchers aimed at Seoul, the international community is obliged to choose its next steps carefully. Despite international protest, North Korea is likely to advance its nuclear programme. China fears a Western-oriented, unified Korea as well as regional instability and has so far been reluctant to commit to effective sanctions in line with the international community. US President Donald Trump, on the other hand, is under increasing pressure due to the advancement in range of North Korean intercontinental ballistic missiles (see fig. 6). Even though military actions are not in anyone's interest so far, the tone of US communications has undoubtedly harshened.

Consequences for the Pacific airspace

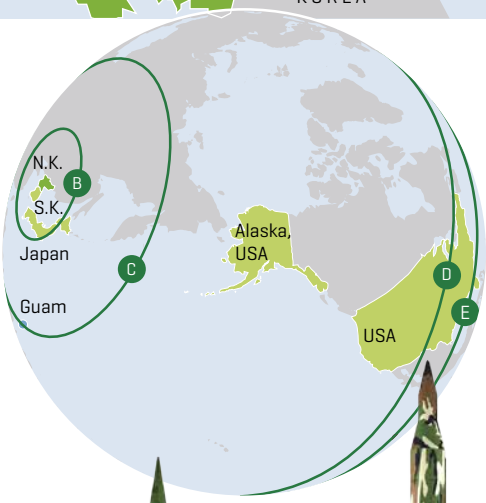
However, in light of most recent developments and statements by Chinese officials, the international community has regained hope that sanctions might be tightened with Chinese approval in the future after all. Chinese-supported sanctions have a chance of finally becoming effective in adverting North Korea's pursuance of a nuclear weapons programme. Yet, North Korea would likely be forced to retaliate and take drastic and provocative actions to compensate for the political loss of face. Harsher sanctions might therefore just as well have undesired effects on Asian airspace. South Korea and Japan would be the most likely targets. Based on existing alliance commitments, the US would be forced to intervene and a refugee crisis would challenge the whole region, escalating the conflict from a regional to a global crisis.

Seoul's Incheon Airport, one of the region's air hubs, being located just 60 km from North Korea's boarder, would be affected from the start of such a further escalation. It is likely to be considered a no-fly zone very early on. All air traffic would need to be redirected, resulting in massive implications on aviation in the entire region. In addition, all air traffic connecting East Asia to the world – be it cargo or civil aviation – would be heavily affected. Resulting disruptions and unpredictability would cause grave complications for both passengers and the supply of goods in the region.

(5) **Number of Missile Tests Executed by North Korea, 2006 - 2017 (Source: CNS North Korea Missile Testing Database)[15]**



[6] North Korea's Strategic Threat (Provided by CNS for NTI)[16]



In September 2016, North Korea tested a nuclear warhead that it claimed will arm the country's strategic ballistic missiles.

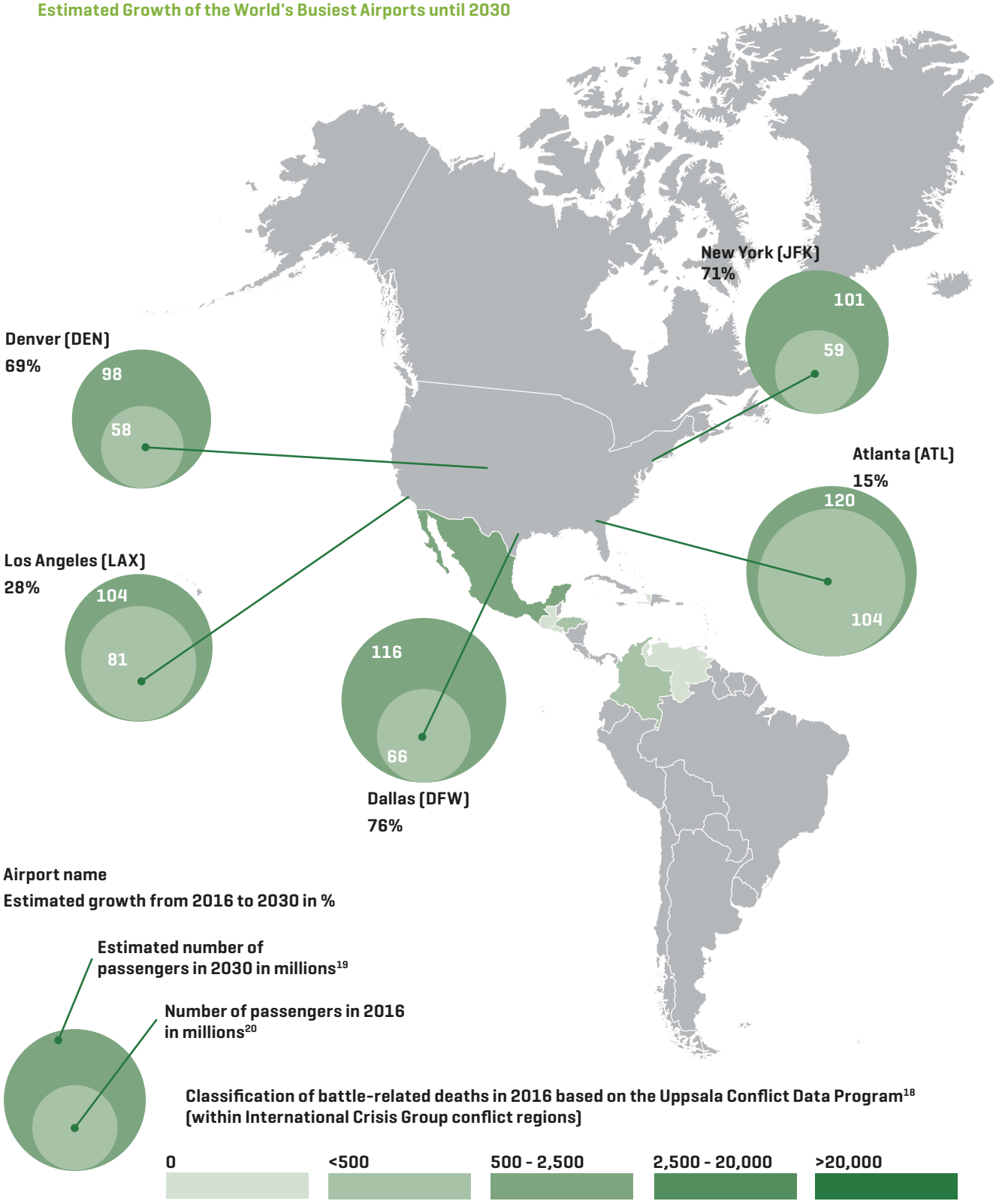
The claim is unverified but some experts find it credible based on North Korea's five nuclear tests.

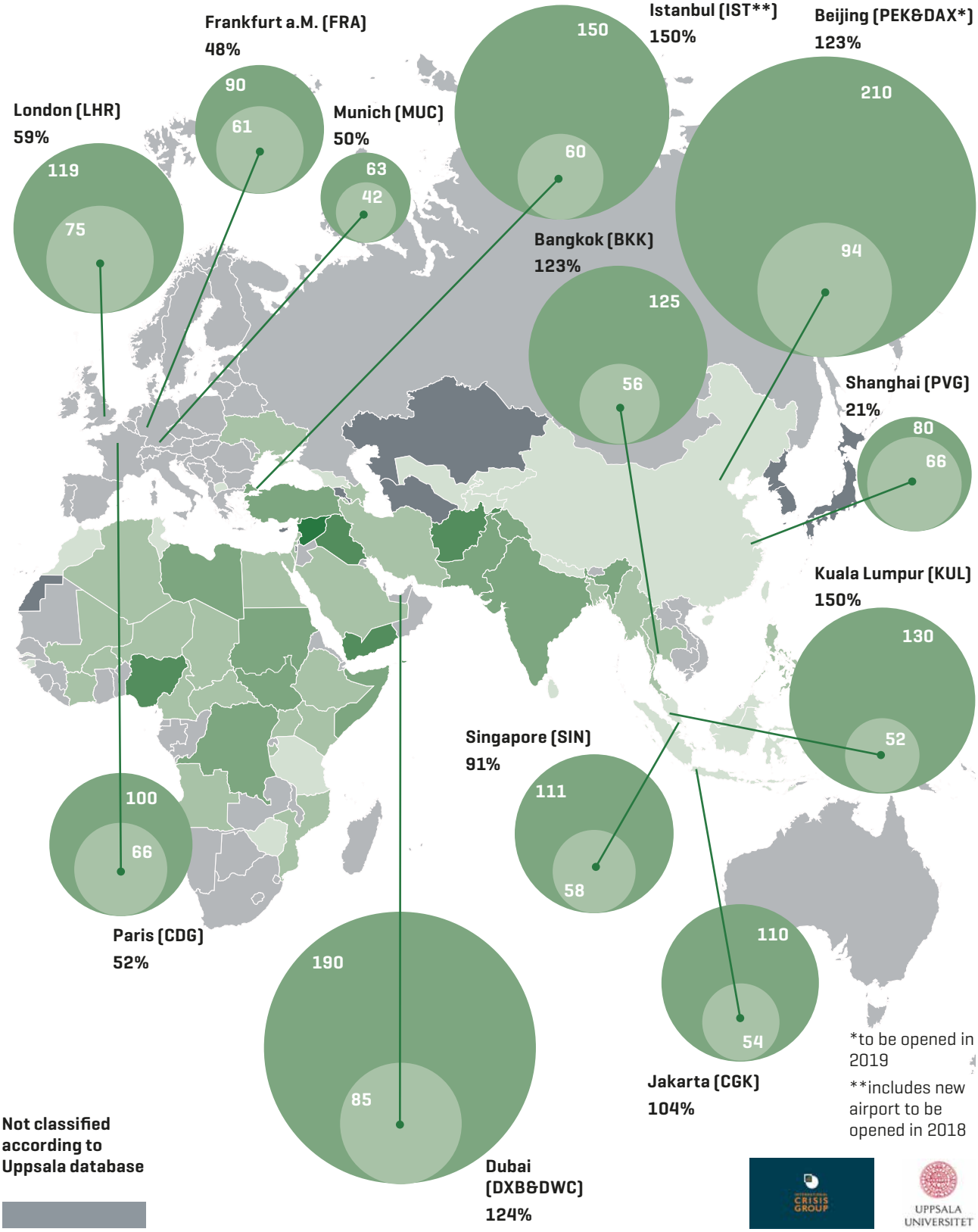
A	B	B	B	C	D	E
KN-02 120 km	Scud B/C/ER 300-1,000 km	KN-11 1,250 km	Nodong 1,300 km	Musudan 3,000 km	KN-14 10,000 km	KN-08 11,500 km
Fewer than 100 launchers		At least 1, submarine launched	Fewer than 50 launchers	Fewer than 50 launchers	At least 6 launchers, not yet tested	

Note: North Korea may have additional missiles

Created by CNS Funded by NTI BUILDING A SAFER WORLD

[7] **World Conflict Map (Source: International Crisis Group)[17] in Comparison to the Estimated Growth of the World's Busiest Airports until 2030**




Frankfurt a.M. (FRA)
48%
90
61
Istanbul (IST**)
150%
150
60
Beijing (PEK&DAX*)
123%
210
94
London (LHR)
59%
119
75
Munich (MUC)
50%
63
42
Bangkok (BKK)
123%
125
56
Shanghai (PVG)
21%
80
66
Kuala Lumpur (KUL)
150%
130
52
Singapore (SIN)
91%
111
58
100
66
Paris (CDG)
52%
190
85
Dubai (DXB&DWC)
124%
110
54
Jakarta (CGK)
104%
Not classified according to Uppsala database
*to be opened in 2019
**includes new airport to be opened in 2018

/Security in German Airspace: Inter-ministerial and Multinational Cooperation

Brigadier General Burkhard Pototzky, Head of Operations at German Air Operations Command, German Air Force

The German Aviation Security Act (Luftsicherheitsgesetz) governs the rules, responsibilities and acceptable procedures for meeting air security requirements in Germany and beyond.

Generally, the responsibility for air security lies with federal and regional aviation authorities. In the event of a lack of resources for resolving and overcoming potential or real airspace threats, the Aviation Security Act stipulates that military support may be called upon – in this case, in the form of the German Air Force. This occurs, for example, if a civilian aircraft is suspected of being used as a weapon for terrorist or other purposes and deliberately crashed.

Pursuant to the German constitution (Grundgesetz, Section 87d), air transport administration shall be conducted under federal administration. As a state-authorised company, DFS Deutsche Flugsicherung, is entrusted with assuming sovereign tasks to ensure the safety of aircraft operations and is wholly owned by the Federal Republic of Germany. Shareholder rights are exercised by the Federal Ministry of Transport and Digital Infrastructure (BMVI).

Air traffic control is overseen by five control centres spread across Germany and the Netherlands. Air traffic controllers are in constant communication with the pilots flying the civilian aircraft, guiding them safely through German airspace. If radio communications are lost, the air traffic controller is unable to carry out this task and an unsafe and possibly unsecure situation occurs in the airspace.

The reasons for this could be something like an incorrectly set frequency, but also a terrorist hijacking.

After five minutes of exhausting all options, the supervisor of the relevant DFS control centre transfers responsibility for what becomes a LOSSCOM situation over to the National Air Security Centre (NASC Germany/ Nationales Lage und Führungszentrum für Sicherheit im Luftraum (NLFZ SiLuRa)).

The NASC is an inter-ministerial federal institution in which the subdivisions Air Defence, Air Traffic Control and Internal Security/Air Security form an integral part and are permanently involved.

They include:

- from the Federal Ministry of Defence, the A3 Division of the Air Operations Command with the Air Force Operations Centre (AFOC/OpZLw),
- from the Federal Ministry of Transport and Digital Infrastructure, the branch office of the BMVI, represented by Deutsche Flugsicherung GmbH (DFS), and
- from the Federal Ministry of the Interior, the Airspace Security branch of Federal Police headquarters.

All other measures are now coordinated and monitored by the NASC. The duty controller first reports the incident internally and then initiates a set of procedures consisting of information gathering, situation assessment, documentation and reporting. An immediate information sharing with the NATO command post responsible for military airspace surveillance and Quick Reaction Alert (QRA) deployment in Northern Europe, i.e. the Combined Air Operations Centre (CAOC), then takes place.

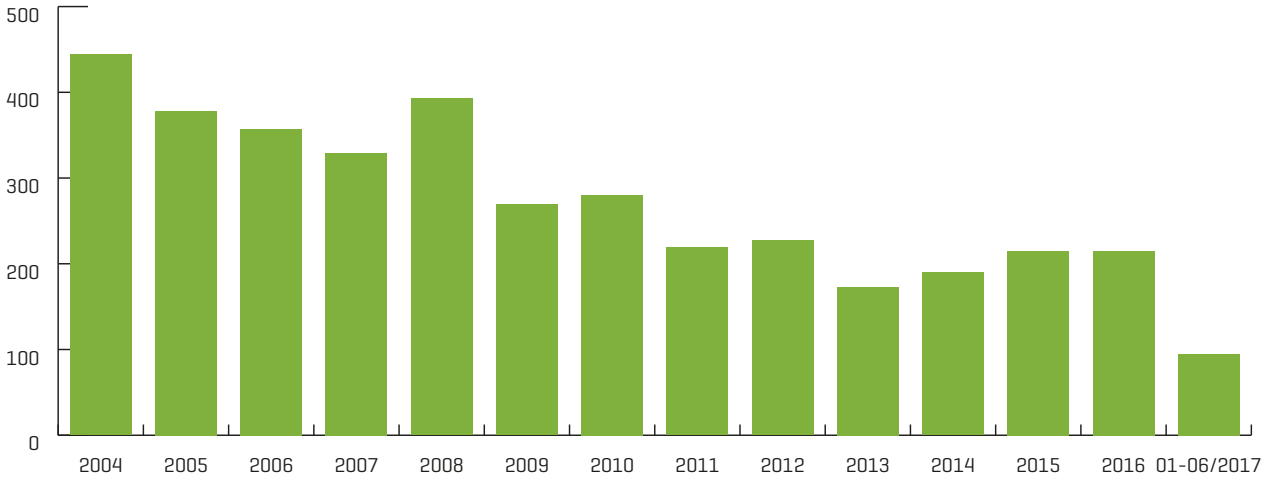
The national airspace status is based on constant surveillance by the German Air Force. For this, two Control and Reporting Centres (CRC) have access to a multitude of military and civil radar devices, engage in data exchange with the CRC in neighbouring countries, and also maintain permanent contact with German air traffic control.

In addition to airspace surveillance, the CAOC is responsible for NATO Air Policing and generally also for German QRA interceptors assigned for this purpose.

Depending on how critical the situation is estimated to be, the CAOC can give the command for one or more QRA interceptors (in Germany or in neighbouring countries) to be on high alert or immediately order an Alpha Scramble[21].

If all attempts to establish contact from the ground are unsuccessful, the objective is to resolve the situation in the airspace in question.

[8] **LOSSCOM-Incidents in German Aerospace Reported to the National Air Security Center by the German Air Traffic Control (Provided by the German Air Force)[22]**



Only the armed forces respectively the air forces with their fighter jets are able to intercept a high-flying, fast-moving aircraft, visually identify it, and, if necessary, use visual signals to communicate with the crew. Such aircraft interceptions occur under the command of an aircraft controller from one of the CRCs. This aircraft controller also conveys reports from the QRA pilots about the intercepted aircraft to the command centres, CAOC and NASC, and in turn, passes on their commands to the QRA interceptors.

Within German airspace, the QRA interceptors are deployed for such LOSSCOM cases as per Section 15 of the German Aviation Security Act in administrative assistance for the air traffic control organisation.

Provided the situation remains a LOSSCOM and does not intensify, missions carried out in the airspace of Germany and some neighbouring countries are generally left under NATO command, who can respond much more flexibly, especially in the case of virtually daily cross-border incidents, by drawing on the support of QRA interceptors from all NATO neighbours.

The NASC monitors the mission in German airspace, coordinates the proposed measures with the CAOC following visual identification, and keeps all relevant centres in Germany informed about the course of progress until completion of the mission.

In the event of a LOSSCOM situation escalating to the suspected misuse of a civilian aircraft for a terrorist or similar attack, the situation becomes a RENEGADE threat and full responsibility is directly transferred to the state as a matter of national security; as in neighbouring states too.

Further QRA deployments are then carried out under national command and the necessary forces and resources are temporarily reassigned by NATO to national control in the course of a Revoke Transfer of Authority (RTOA).

Any measures related to the use of force against a civilian aircraft, such as forcible re-routing, a forced landing or even the firing of a warning shot, have to be applied in accordance with the relevant national jurisdiction.

In German airspace, the air forces then act in administrative assistance for the authorities for the interior and any use of forces have to be with the collective decision of the federal government.

In terms of national responsibility in the case of RENEGADE threats, a cross-border cooperation to deal with such incidents through the relevant national governmental authorities (NGAs) specifically set up for this purpose is only possible on the basis of bi- and multilateral treaties. Such treaties are already in force or under way.

The main role of the NASC, as part of the German NGA, is to maintain control of the general situation and to offer the best possible advice to political decision makers with regard to sweeping defence measures. This role is assumed by superior authorities – for the air force, this is the German air defence commander.

Air force soldiers and federal police officers – as representatives of the sovereign tasks performed by the polices of the federal states – as well as air traffic control operators and employees of the Federal Office of Civil Protection and Disaster Assistance therefore work hand in hand, round the clock, on compiling a detailed status report on German airspace security and the handling of threats.

/Europe's Airpower: Matching Demands and Supply

Douglas Barrie, Senior Fellow, International Institute for Strategic Studies

IISS

Post 9/11

The events of 2001 that fundamentally shaped the US-led wars of the early 21st century had an inevitable effect on European air forces. While the hijacking of commercial aircraft was nothing new, the suicidal and murderous use of a passenger aircraft as a flying bomb placed an even graver challenge on the air forces of nation states faced with such a threat.

Up until the 2001 attacks on the US, the defence of national airspace had become an area of benign comparative neglect for European air forces. The perceived lack of a credible state threat coupled with reductions in force size resulted in a reduced focus on the protection of domestic airspace. All this would change after September 11, 2001.

The issue was no longer of intercepting and escorting a hijacked aircraft to an airfield where the security authorities could then deal with the situation. Instead, the threat had become far uglier. Air forces and administrations were faced with having to deal with an improvised cruise missile, a vehicle that could include tens or hundreds of people, domestic and foreign nationals.

In the aftermath of the September 2001 attacks, policy decisions were taken by the US and some European governments regarding the procedures and command chain for dealing with a hijacked aircraft deemed to be a threat. Rules of engagement were established that would – as a last resort – result in the destruction of a commercial aircraft in the air were it deemed to be being used as an improvised weapon. Authorisation to engage would require approval from the highest levels of a government. At the same time, the combat aircraft aircrew tasked with providing 24-hour Quick Reaction Alert (QRA) were profiled and supported to ensure that, if faced with the awful responsibility of engaging a commercial aircraft, they would be able to cope.

Not all European nations, however, have 24-hour QRA. A widely publicised incident in 2014 required French combat aircraft to escort a hijacked Ethiopian Airlines Boeing 767 into Swiss airspace to land at Geneva Airport since the Swiss Air Force did not provide 24-hour coverage due to resource limitations. Following the incident, the government decided to work towards establishing a round-the-clock response capability by 2020.

Security concerns

The growth in NATO membership also brought with it additional air policing activities. The Baltic states became alliance members in 2004, but neither Estonia, Latvia nor Lithuania had an air force able to fulfil this role. Instead, other NATO member states provide this capability on a rotational basis. This activity has taken on greater importance as relationships with Russia have deteriorated over the past decade. Traditional air defences are now once again unfortunately a key element of NATO air power and are intended to provide reassurance to Eastern European alliance members and to deter any potential aggressor state.

The re-emergence of the risk of state-on-state warfare, though still remote, has not simply replaced the threat of a suicidal attack using a commercial aircraft. The two disparate demands now exist side by side, placing further demands on European air powers.

Russia has become not an awkward and sometime irascible strategic partner but a strategic competitor willing to exercise or threaten to exercise military force in pursuit of what it views as its legitimate territorial aims or security concerns over the Russian diasporas in the »near abroad«.

»While this is not a return to a Cold War, Europe is faced once again with the possibility, thankfully still remote, of state-on-state conflict on its eastern flank.«

Matching demand and supply

European air forces remain a critical asset in terms of national defence while continuing also to provide a flexible and effective military tool when governments wish to exert military power.

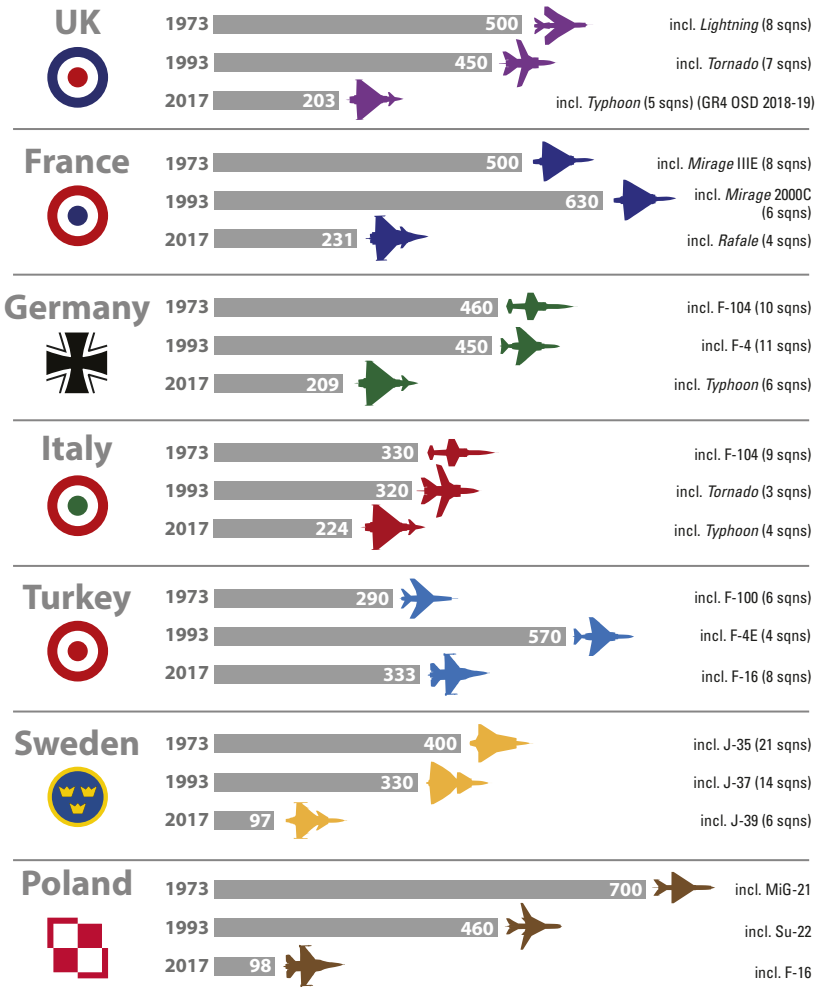
Increased demand, however, does not necessarily equate to improved resourcing. Since the end of the Cold War and super-power confrontation in 1989, European air forces have reduced in size considerably. Compared to the early 1990s, France, Germany and the UK have cut combat aircraft fleets by roughly a half. Only in the past few years has this

downward spiral stopped, accompanied by indications of a modest increase in future. This reversal is the result of Europe's security environment being at its poorest since the early 1980s. In the UK, a decision was taken in 2015 to extend the service life of early versions of the Eurofighter Typhoon combat aircraft to provide an additional two squadrons, while there are also ambitions to introduce a second squadron of the Lockheed Martin F-35B Lightning II into service more quickly than originally planned.

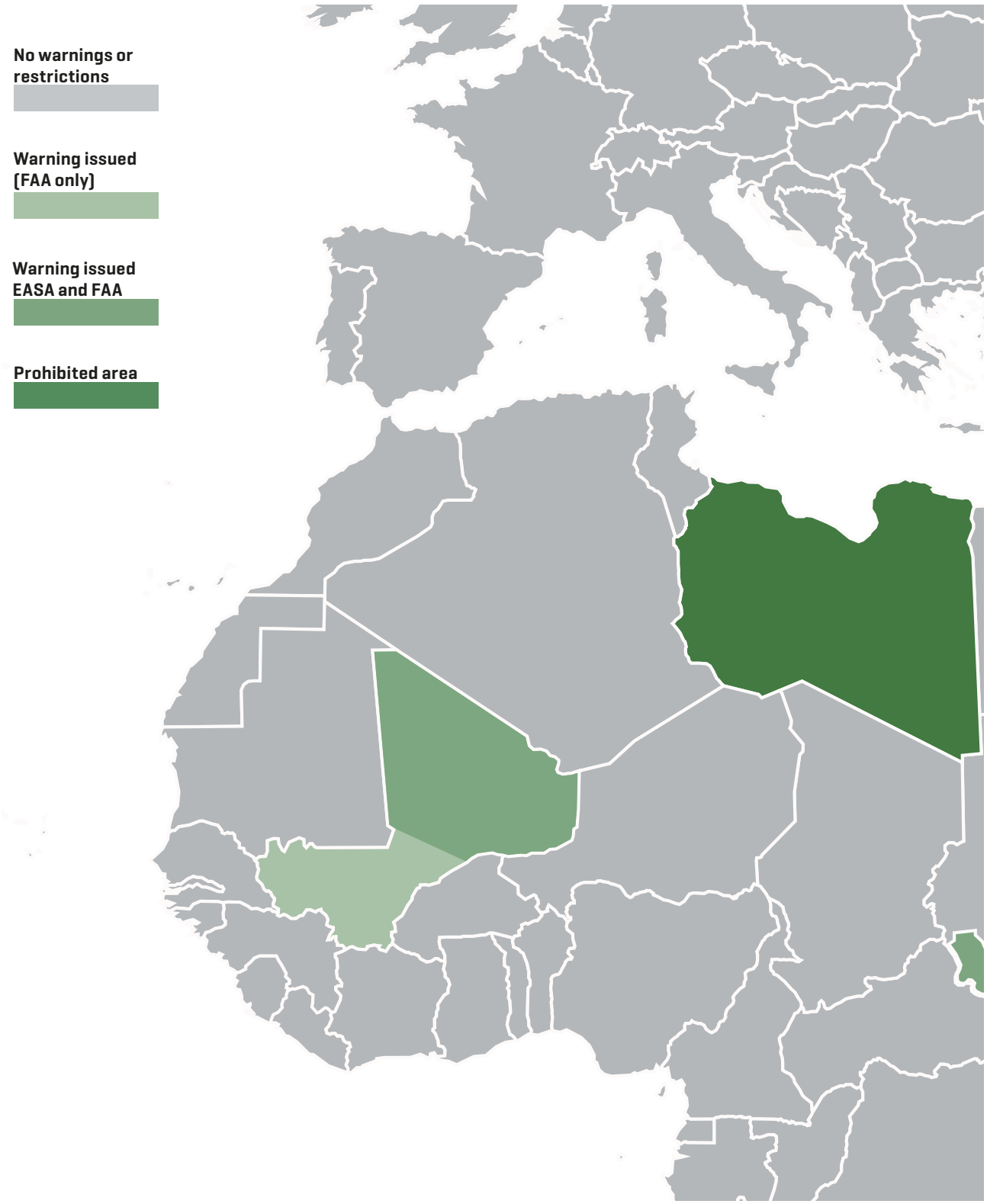
The present generation of combat aircraft now in service with Europe's air forces include alongside the Typhoon, the Dassault Rafale, and the Saab Gripen. These so-called fourth-generation fighters are considerably more capable on a like-for-like basis than the types they replaced. But capability comes at a cost.

While the collapse of the Soviet Union removed during the 1990s the risk of full-blown state-on-state conflict in Europe, several of the continents' air powers nonetheless have been involved in combat operations on a near permanent basis over the past three decades. Beginning with the first Gulf War, some European air forces have undertaken commitments in the Middle East on a near constant basis since 1991. The 2001 - 2014 war in Afghanistan, the invasion of Iraq in 2003, and the continuing campaign against Da'ash in Iraq and Syria have involved European air forces including Germany, France, Italy and the UK. Shorter duration operations such as the Libyan air campaign also drew heavily on European air forces while national-level commitments such as France's ongoing operation in the Sahel region of Northern Africa require air force resources.

(9) **Fighter Jets in Europe (Provided by IISS)**[23]



[10] **Worldwide Flight Restrictions According to EASA[24] and FAA[25], 06/2017**



/Sharing Information on Conflict Zones

Frank Brenner, Director General, EUROCONTROL

The tragic loss of flight Malaysia Airlines MH17 over eastern Ukraine in July 2014 highlighted the risk of flying over conflict zones, even at an altitude of over 30,000 feet. In its aftermath, a task force was formed by ICAO to consider what might be done to help prevent such events in future. A key finding of that task force was the value of sharing information so that states and airspace users can make informed decisions on what areas should be avoided. It was proposed that an ICAO repository of information on conflict zones should be set up and made available publicly.

EUROCONTROL supports the principle of sharing such information. Its Network Manager Directorate acts as a widely-used information source for aviation in Europe; a key tool it uses is the Network Operations Portal (NOP)[26], which is made available both to the public and also, in a version with more information and functionality, to 7,500 aviation professionals across Europe. There are several million 'hits' on the site daily.

As a result, it was felt that it would be useful to set up an area (the »Crisis Management Portlet«) in the protected version of the NOP, providing information on which airspace in or near Europe was affected by either closures or warnings related to conflicts. This could be achieved rapidly and then reviewed once other tools such as the ICAO[27] Conflict Zone Repository became available.

The portlet went live on 21 November 2014 with both a map and a list showing closures and warnings. The information comes from state authorities and also the European Aviation Safety Agency (EASA), typically through Aeronautical Information Publications (AIP), Aeronautical Information Circulars (AIC), Conflict Zone and Safety Information Bulletins (CZIB/SIB), Notices to Airmen (NOTAM) and ICAO State Letters. It is kept current through frequent updates; the NOP Headline News function also helps to make sure that aviation professionals have access to the very latest information.

The response from our users has been very positive, with airspace users appreciating how the information is presented, the fact that it is kept up to date and also that it is maintained on a secure site. It is seen as having real value, especially at a time when so much of the airspace on the periphery of Europe is affected.

EUROCONTROL Network Manager does not originate content for the portlet but instead presents available information, H24, in an accessible format. Unfortunately, however, the ICAO Conflict Zone Repository has unfortunately only had a limited number of state authorities contributing to it. As a result, there is a strong demand from our airspace users for EUROCONTROL Network Manager to continue with its portlet, which is also seen as being supportive to its role in the European Aviation Crisis Coordination Cell.

/Knowledge is Power – The Importance of Threat Information Sharing

Dr Emily Haber
State Secretary, Federal Ministry of the Interior, Federal Republic of Germany

Bringing the right information to the right people to do the right thing – this is one of the challenges we have to face in many fields. The Federal Ministry of the Interior covers a wide range of topics where information is shared: starting from eGovernment to protecting public security.

In Germany, protecting public security is organised along federal lines. It is the 16 federal states making up the Federal Republic that are primarily responsible for this task. By contrast, the federal government is responsible for central law enforcement issues, with which it has tasked the Federal Criminal Police Office (Bundeskriminalamt, BKA), as well as for border control, railway policing and aviation security – tasks performed by the Federal Police. Owing to this federal structure, we need to make sure that the stakeholders involved have the information they need when they need it, which is a particular challenge. Nowadays, neither crime nor crime control stop at national borders. In a globalised world, no nation can single-handedly guarantee a sufficient degree of security. Security networks must be used to fight criminal and terrorist networks.

This is also true within the European Union. In Europe, too, we can take effective action against organised crime and terrorist violence (and manage migration and travel) efficiently and appropriately only if we share and connect available information. However, our authorities also need to be able and allowed to effectively tap specific resources.

Europol, the European Union's law enforcement agency, is intended to assist and strengthen the work of the relevant member state authorities and their cooperation in preventing and fighting organised crime, terrorism and other forms of serious crime. To this end, Europol stores and analyses information from the member states, making it easier for them to share information. The relevant authorities in the member states can query the Europol information system, where member state data on crimes and criminals is stored. The database shows links between investigations conducted in the individual member states. Using analysis work files, Europol can clarify connections between crimes and provide member states with operational and strategic analyses.

In addition, we need to fill existing gaps in Europe's information landscape, for instance with regard to the processing of passenger name records (PNR). Under the EU's PNR Directive, member states are required to establish Passenger Information Units (PIUs), to whom air carriers must transmit specific PNR data. The Directive must be transposed into national law within two years of its entry into force, i.e. by 25 May 2018. Germany has already met this requirement by adopting the PNR Act, which took effect on 10 June 2017. We are now taking the organisational and technical steps to put the envisaged PNR data information system into operation. In line with the EU Directive, the aim is to run the PNR data against police databases (e.g. the Schengen Information System) to identify known criminal offenders who have been flagged by security authorities on account of arrest alerts. Also, pattern recognition should enable us to identify persons linked to terrorism and organised crime who have not yet come to the attention of the security authorities.

The EU's PNR system follows a decentralised approach and places a major focus on information networks: firstly, within any given member state, the PIU and the relevant national authorities must coordinate their actions smoothly; secondly, the PIUs of

»The recent tragic attacks in Europe have highlighted the importance of effective information sharing between Member State authorities.«

Sir Julian King, European Commissioner for the Security Union[28]

»The value of our security information is maximised when our systems talk to each other. The complex and fragmented systems we have today make us vulnerable. Actionable information is not always available for the law enforcement officials that need it.«

Dimitris Avramopoulos, European Commissioner for Migration, Home Affairs & Citizenship[29]

the European Union must make sure that, in cases where intelligence gathered by one member state is also relevant for others, such intelligence is actually shared (Europol has been given a central role here); and thirdly, the information may also be shared with third countries if certain conditions are met, in particular an appropriate level of data protection.

In addition, the architecture of the EU's major information systems needs to be improved noticeably, in order to overcome the fragmentation of information that should be grouped together because it concerns related facts or phenomena. The authorities must be enabled to systematically tap and retrieve related information, as the Justice and Home Affairs ministers demanded in their Council conclusions of June 2017. Based on the results of a high-level expert group, the Council and the Commission concluded that the existing systems must be connected through a common identity repository, merging and linking (identity) information. In this context, security and data protection are not opposing factors, but go hand in hand: having a common identity repository means that, wherever possible, data are collected only once, that their quality is continuously maintained and improved, and that they are ready for multiple use. That would enable us to systematically detect persons with false or multiple identities, and to consolidate or otherwise clarify such identities. These proposals need to be implemented swiftly in legal, operational and technical terms.

I believe that further developing this issue will be essential to set the course for future security and freedom in Germany and Europe.

/Cooperation Across Borders and Sectors

Rob Wainwright, Executive Director, Europol

Cybercrime, people smuggling and other forms of serious and organised crime have developed into significant and truly pan-European threats with major impact on the aviation sector. As for terrorism, the sector has been facing this threat for decades, but terrorist tactics have evolved rapidly in the last few years. Feeding on a world that continues to interconnect and to accelerate, and on technological developments that fundamentally change the criminal landscape, the complexity, scale and internationalisation of crime and terrorism are ever increasing.

To enable law enforcement to keep up with its international criminal adversaries, the essential ingredients are fostering global information sharing, facilitating multinational investigations and providing in-depth, state-of-the-art criminal analysis. These tasks form the core of Europol's mandate. Assisting EU member states in their fight against serious international crime and terrorism, Europol is the hub for the exchange of law enforcement information in the EU and it provides key operational support for member states' investigations. Working closely with international partners, institutions and the private sector, Europol in many cases is the central platform for these partners to reach out to European law enforcement.

For several years now, cooperation with and through Europol has been on the increase. Key areas like counter-terrorism, for example, saw a tenfold increase in information provided to Europol since the beginning of 2015, allowing for major successes in disrupting the funding of terrorist organisations or their destructive online propaganda. Regarding the aviation sector, three areas of strategic concern stand out that deserve close attention and impetus for enhanced cooperation.

Airline ticket fraud – huge monetary losses and facilitation of serious crimes

Though seldom in the limelight of public attention, airline ticket fraud threatens security worldwide by potentially facilitating the international travel of terrorists and criminals involved in a range of criminality, including illegal immigration, human trafficking, and drug smuggling. The airline industry is estimated to lose over one billion dollars per year as a result of the fraudulent online purchase of flight tickets.[30] Since 2013, Europol has held Global Airline Action Days targeting the individuals attempting to travel on these tickets.

This activity brings together representatives from airlines, online travel agencies, payment card companies and the International Air Transport Association (IATA), who all work together with experts from Europol's European Cybercrime Centre (EC3) to identify suspicious activity and relay information to law enforcement officers deployed in airports globally. The last day of action in October 2016 took place in 189 airports in 43 countries and involved 75 airlines and 8 online travel agencies. It resulted in over 190 individuals being detained, and highlighted the importance and huge impact that law enforcement can have when it comes together with industry and shares information in an environment of trust.

Vulnerability of the aviation sector to cybercrimes

Airline ticket fraud is of course only one cyber-related aspect of how malicious actors can affect the airline industry. Across all industries, both criminals and state-sponsored actors are flexing their technological muscles, looking for new opportunities to cause damage or create profit.

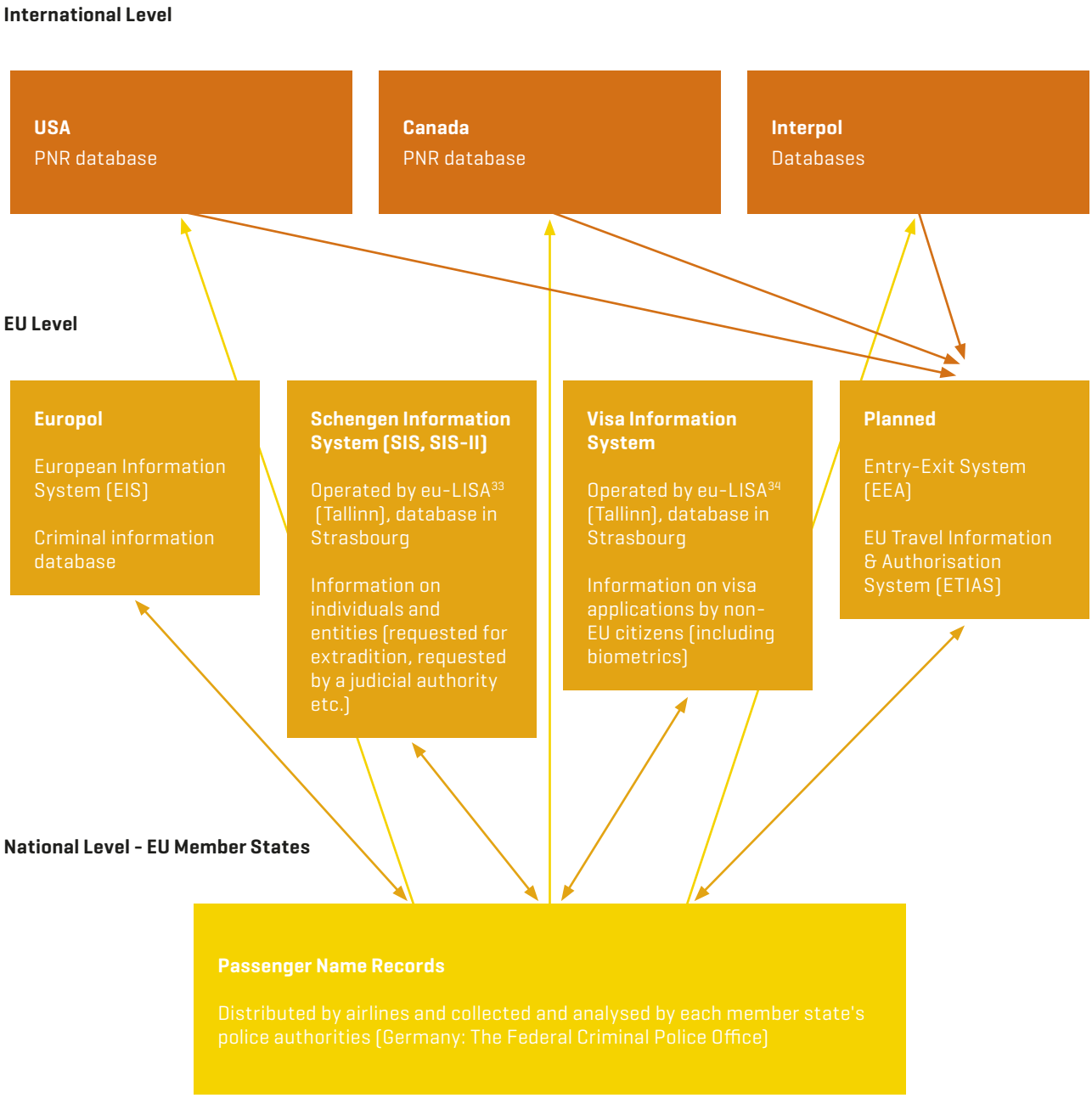
In 2015, a Distributed Denial of Service (DDoS) attack grounded more than 1,400 passengers at Warsaw's Frederic Chopin Airport. This attack was the first of its kind, but demonstrated how a relatively simple attack, which is readily available to hire on the digital underground, can cripple an airline.

»The airline industry relies heavily on computer systems in its ground and flight operations. Each of these is potentially vulnerable to some form of cyber attack.«

Ransomware - malware which encrypts the data on a victim's system unless a ransom is paid to decrypt it – has become the leading malware threat in the EU. With it, criminals have sought victims atypical to the usual financial targets - hospitals, law enforcement agencies, governments. The unprecedented global »WannaCry« attack in May 2017 exposed the vulnerability of public and private infrastructures and highlighted that cyber security must be a major strategic concern across all sectors. Given the reliance of airlines and airports on numerous, distinct computer systems, a ransomware attack on them could be devastating. As with all forms of cybercrime, this is an area where Europol works closely with industry to share tools and prevention advice through the »NoMoreRansom« campaign.[31]

Of course, most airlines will have robust physical and technical security measures in place to deter a direct cyber assault. This is why the most complex and

[11] **Aviation-related Excerpt of the European and International Information Exchange Environment**[32]



sophisticated cyber attacks usually rely on breaching the 'human firewall', using social engineering to bypass internal security measures. It will therefore become ever more important that the industry, in addition to technical measures, ensures that its employees are properly trained to recognise and react appropriately to such threats.

Enhancing security through travel data: systems alone are not sufficient

Numerous legislative initiatives with significant impact on the airline industry aim to give European law enforcement, including Europol, access to relevant travel data. Among them are the European Passenger Name Records Directive, which is in the process of implementation in EU member states, as well as the European Travel Information and Authorisation System (ETIAS) and the Entry-Exit System, which are currently being negotiated in Brussels.

All of these initiatives highlight a significant and long-standing intelligence gap, namely information related to passengers travelling to, from and through the EU and the borderless Schengen Area not being available in adequate fashion in advance of the travel taking place. This gap was already made apparent in relation to the Jewish Museum attack in Brussels in 2014, when a foreign fighter known to law enforcement authorities was able to return to the EU from a conflict zone undetected using air travel, and subsequently move across the EU for months until the moment of conducting the act of terrorism. Addressing this gap and enhancing security in the EU can help muster crucial support for safeguarding the right to free movement within the Schengen Area.

Yet, though all those data systems alone are relevant, it is only their combination that will unveil the full added value and benefits. Achieving interoperability between the various systems is a strategic aim for the EU, in order to allow maximum efficiency in combating serious crime and terrorism while safeguarding high data protection standards. Europol has extensive experience in the handling of large sets of data while adhering to strict data protection protocols, which it will contribute to the upcoming discussions on enhanced travel data analysis.

Innovative solutions that strengthen intelligence-led policing without compromising safeguards for the handling of sensitive personal data, and which limit the economic and administrative burden for the industry, are typically the result of a close partnership of law enforcement, industry and the research sector. The central common denominator running through all areas of strategic concern is that a structured exchange and the sharing of expertise and tools between these sectors is more important than ever.

EU Reform Process on Information Sharing and Interoperability[35]

In 2016, the European Union set up a High-Level Expert Group on Information Systems and Interoperability, aiming to

- give advice and assistance to the Commission in order to achieve the interoperability and interconnection of information systems and data management
- develop an overall strategic vision on the interoperability and interconnection of information systems on a more effective and efficient data management for border management and security in the EU
- establish cooperation and coordination between the Commission and member states on questions relating to the implementation of Union legislation on the interoperability and interconnection of information systems

In their final report, published on 11 May 2017, the high-level experts conclude that it is possible and necessary from a technical as well as a data-protection perspective to establish the three following instruments:

- a European search portal
- a shared biometric matching service
- a common identity repository

The interconnectivity of systems is recommended only to be considered on a case-by-case basis while evaluating if certain data from one system must be systematically and automatically reused to be entered into another system.

/Brexit: Security Risks for European Aviation

In terms of the consequences for aviation, much of the Brexit debate has focused on the problems it will cause carriers. For example, whether or how British carriers will still be able to participate in the common air transport market, which strategies they can pursue to ensure market access, and what consequences Brexit will have for the EU–US Open Skies Agreement.

Little has been discussed, on the other hand, about the consequences of Brexit on aviation security and how Brexit – especially a »hard Brexit« – could have a major impact on progressive developments in the European security architecture.

In the fight against terror and organised crime, Great Britain plays an important role. EU member states can access British intelligence through several databases. As a result of Brexit, however, these sources could dry up. Similarly, Britain may no longer be able to rely on these sources for its own investigations.

This applies, for example, to the European search database Schengen Information System (SIS II). The security authorities of 26 Schengen countries as well as Europol, Eurojust and the national public prosecutors have access to these databases. Through a special opt-in clause, the UK participates in SIS II, but Brexit will terminate the validity of the opt-in clause.

Other non-EU members, such as Switzerland, have access to SIS II. However, the prerequisite for this is that they are part of the Schengen Area. The UK is not a member and a future Schengen membership of Great Britain is currently unimaginable.

Similar problems arise when accessing other databases. Access to the Eurodac database with fingerprint data is available only to EU member states or Dublin countries taking part in the so-called Dublin-Regulation, such as Norway. The likelihood of Britain becoming a »Dublin« state, however, is currently just as remote as Britain becoming a member of Schengen.

This means that Europol's Executive Director Rob Wainwright is right in saying Brexit runs the risk of creating a »dangerous security gap«, especially in the fight against terrorism in Europe.

/PNR and the Risk-Based Approach to Aviation Security

Sven O. Weirup, Chairman, European Aviation Security Center

People evaluate risk. Everywhere, all the time. Proper risk assessment has been key to mankind's survival throughout the millennia of evolution.

Every passenger a suspect ...

Everywhere, all the time? Well, without exception in aviation security. In aviation security, we declare every passenger a suspect and hence subject every passenger to identical security searches and procedures. Aviation security as we know it focuses on dangerous objects only, not at all on dangerous people. A truly awkward approach; no police, customs or internal revenue officer would work that way. In all other walks of life it is assumed and accepted that security measures are triggered and guided by clues or patterns of suspicion.

Evasive tactics or a strategic response?

A kitchen knife in the hands of an innocent person remains just that, a household utensil. It is the ill intent that forms the risk. Unfortunately, not all dangerous objects are as easily detected as a kitchen knife. New threats may very well defeat the technical capabilities of contemporary airport security equipment. It is dangerously naive to assume that future attacks will trail the pattern of past attacks. Today's strictly tactical response prepares for the modi operandi of previous assaults, not necessarily those of the future. We eagerly follow the misguided promise that non-discriminatory checkpoint technology will detect each and every threat for us in the most politically uncontroversial way. Surely this approach is an easy one; but to protect innocent lives, is a politically convenient approach truly the more ethically justifiable path?

In modern AVSEC, risks can no longer be mitigated by tactical responses alone. A sustainable strategy will aim at identifying potential assailants first and dangerous objects second. Myriads of perils are unidentified today; so-called black swan scenarios. Black swans cannot be countered by predefined and predictable technologies and procedures, however rigid these may be. Only data intelligence and scientific methods of pattern recognition can do that.

The EU's choice

The EU Commission, at least after the Paris terror attacks in January 2015, has acknowledged this fact and decided to revive an initiative from 2011; originally blocked and now passed by the EU parliament: Directive (EU) 2016/681 of April 2016. At the latest on 25 May, 2018, all member states will need to use a data-based intelligence tool to counter crime and terror: Passenger Name Records, in short PNR.

PNR

PNR are unverified sets of data that airlines generate to facilitate booking processes and to enhance service. PNR contain several different types of information, such as travel dates, travel itinerary, ticket information, contact details, the travel agent at which the flight was booked, means of payment used, seat number and baggage information. Some member states (e.g. the UK) already have a PNR scheme in place, others now produce and enforce corresponding national PNR legislation (e.g. the »Fluggastdatengesetz« in Germany). States will obligate air carriers to forward PNR data of all passengers on their flights between the EU and third countries to a Passenger Information Unit (PIU), established at domestic level for this purpose. In Germany, the Federal Criminal Police Office (Bundeskriminalamt, BKA) has been designated to act as the responsible national PIU. To ensure an optimum of data protection, Germany has decided to keep the implementation of the PNR infrastructure separated, and therefore to have the BKA delegate the task of data collection, storage and processing to the Federal Office of Administration (Bundesverwaltungsamt, BVA).

Predictive policing

PNR data are different from and should not be confused with the Schengen Information System (SIS), the Visa Information System (VIS), or Advance Passenger Information (API), which may, however, be part of some airlines' PNR. Even though PNR are passenger data linked to travel, they are used as a criminal intelligence tool rather than as a border control tool. More commonality will be between PNR and the emerging methods of predictive policing. Both use big data techniques to criminologically recognise and analyse all sorts of suspicious patterns. The aim is to »identify persons who were previously unsuspected of involvement in terrorism or serious crime« and require further clearance by the competent authorities.

The airlines' predicament

Authorities may use PNR data reactively, proactively and in real time. For PNR to be effective, the focus on prevention is paramount. The individual risk assessment of passengers prior to their travel applies predetermined criteria and facultative cross-checks with existing police intelligence and information systems. Airlines and authorities will need to provide, validate

[12] Development of Handling Passenger Name Records (PNR) in Europe

11 September 2001
The terrorist attacks in the US lead to a strongly increasing amount of data/PNR exchange between the US and the European Union.[36]

2006
The European Court of Justice criticises the lack of legal base for personal data exchange between EU member states and the US - the first agreement fails.[37]

2007
The European Union adopts the second agreement between the US and the EU to create a legal base for data/PNR exchange. The European Parliament and civil rights groups start a number of lawsuits at national European courts and the European Court of Justice.[38]

February 2011
The European Commission proposes a draft for a European PNR directive and starts the legislative process. The EU Parliament immediately declares to fight this directive.[39]

2012
The agreement between the EU and the US about PNR data exchange is finally in force.[40]

June 2014
The second agreement between the EU and Canada to PNR data exchange is adopted. Again, EU parliamentary groups and civil rights groups start legal resistance.[41]

April 2016
After more than five years since the legislative process has began, the EU Parliament adopts the European PNR Directive.[42]

September 2016
The European general attorney at the European Court of Justice declares that the PNR agreement between the EU and Canada most likely violates European law. The Court usually follows his recommendations. A decision is expected in 2017.[43]

April 2017
The German Bundestag adapts the »Federal Act for Handling PNR Data« to transform the European Directive into German law. This law also includes PNR data of intra-Schengen flights. Civil rights groups declare to fight this law at German courts.[44]

May 2018
Final deadline for all European member states to transform the PNR Directive into national law.[45]

processes, and disseminate huge amounts of data very fast, efficiently and at a high integrity. Not a trivial task, and for airlines a potentially costly one. Some 180 airlines are operating in Germany alone. Many still need to adopt the current IATA passenger and airport data interchange standard PNRGOV. It remains to be seen when and how airports and the IT industry will be called upon to assist the implementation, testing and certification of these processes and hence enable technical compliance and fulfilment of the legislators' timescale. For public acceptance of industrial partners, these will need to verifiably operate under national or EU jurisdiction and to physically perform all data processing and storage strictly within these boundaries.

»I explicitly appreciate the decision of the European Parliament to adopt the PNR Directive. After years of troubling discussions, we now finally have a further important instrument to fight international terrorism. Security agencies in Europe now finally get the possibility to identify the travel routes of potential terrorist offenders and to take appropriate measures against them by analysing their PNR data. This is essential for preventing attacks as well as for uncovering networks.«

Thomas de Maizière, Federal Minister of the Interior, Federal Republic of Germany[46]

»PNR is an important step. But it is even more important that European Countries actually merge their databases.«

Prof Dr Peter R. Neumann, Director, International Center for the Study of Radicalisation and Political Violence, King's College London; Special Representative of the Chairperson-in-Office on the Fight against Radicalization, Organization for Security and Co-operation in Europe[47]

Civil and digital rights?

EU and national PNR legislation prohibits any data storage and processing on grounds of race, ethnic origin, religion or belief, political or any other opinion, trade union membership, health or sexual orientation. The gathering, processing and storing of PNR data shall be transparent and strictly protect citizens' data and fundamental rights. Still, PNR will raise both serious and valid privacy concerns. These are rightly and exhaustively being addressed in other contexts and hence require no further mention in this short essay.

PNR expanded

Member states are given the liberty to extend PNR to intra-EU flights, or to a selection of them. Most member states have declared their intent to make use of this option. Driven by the terror attacks of March 2016, the Belgian Chamber of Representatives even approved a draft law to apply comparable methods to the data of train passengers.

Secure identities

A much neglected, even ignored prerequisite for the full implementation of PNR will be the establishment of a secure identity for every passenger. Today, ID checks are rare and airline passengers travel more or less anonymously; at least on most intra-Schengen flights. Technology, as used in EasyPASS or similar automated border checkpoints, would use convenient and rapid biometric identification measures to give future passengers a secure identity, authenticate their PNR data, and make subsequent data processing valid and meaningful.

The risk-based approach

Even if this is not its entire purpose, PNR will make air travel less vulnerable to hitherto unidentified threats, and accordingly, keep passengers more secure. Resources available to security will always be limited. PNR will allow these limited resources to be focused precisely and on target. Experts call this the risk-based approach to aviation security.

For the vast majority of passengers, PNR and its risk-based approach will bring back pleasure and convenience to air travel. The scope of physical security screening will be minimised or eventually reduced to random checks. Future stand-off sensor technologies may perhaps augment this approach, but only a minute number of passengers will show indications that lead to a closer inspection. And again, most of these passengers will be cleared and understand that certain non-discriminatory criteria may have prompted a more thorough check. A risk based approach simply implies screening different passengers in different ways.

The airports' dilemma

Global air travel tends to double every 15 years. A little more in Asia, a little less here, but the demand keeps growing. Unfortunately, air capacity does not. Space at European airports is tight. It is this limited capacity that could seriously restrict the advance of aviation and consequently even national economies. If doubling the number of passengers would

require a doubling of security checkpoints, the consequential collapse of airport infrastructures would seem a certain fate.

Today's luxury of wasting precious airport infrastructure to perpetuate an overcome security model will neither be sustainable nor justifiable. Checkpoint processes need speeding up. Equal attention cannot be given to all passengers all the time.

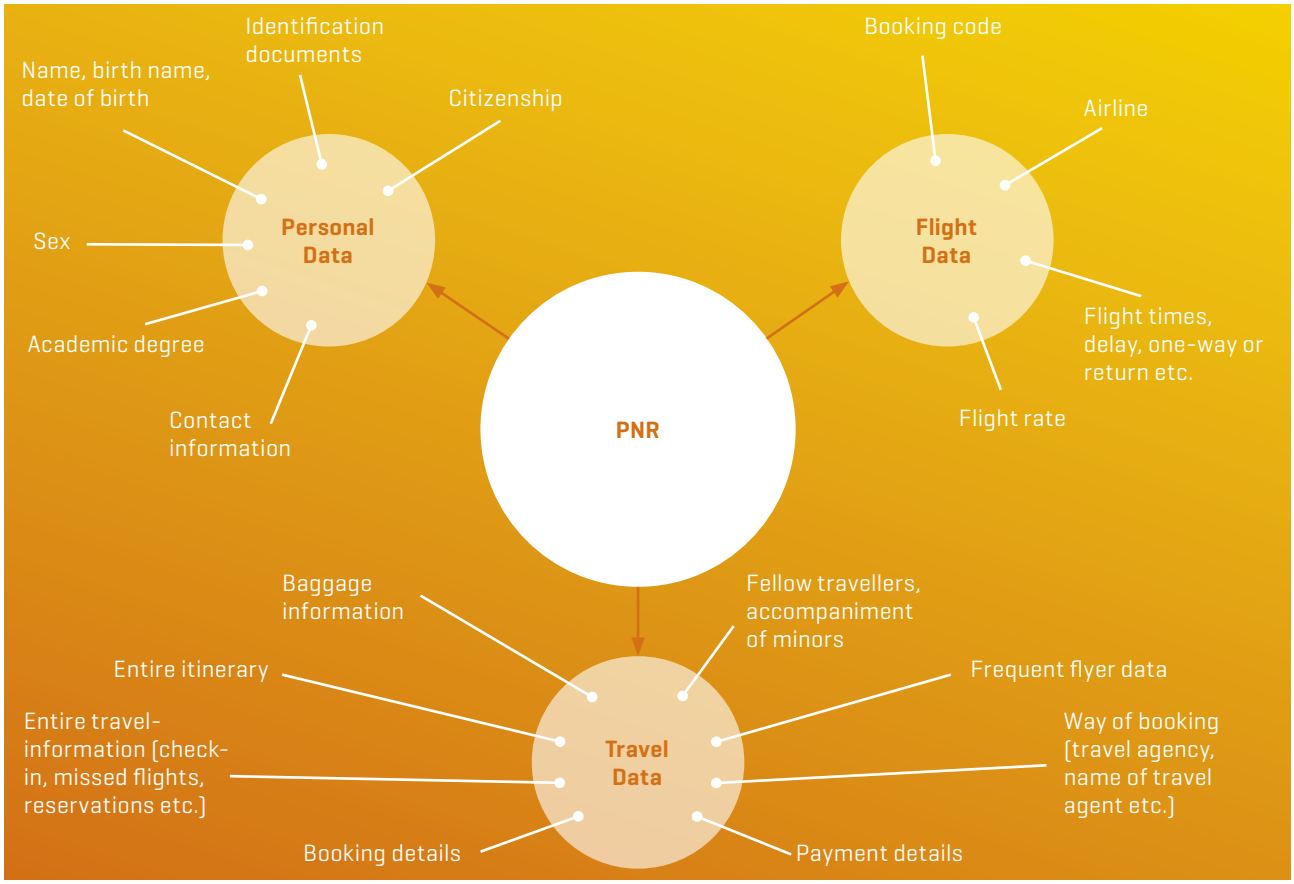
Bonafide security

Modern terrorists are masters of resourcefulness and creativity. They will eventually find ways of defeating our predictable checkpoint technology. Future attacks may use unconventional weapons produced by 3-D printers, subcutaneously implanted IEDs, chemical agents, or any other means that conventional detection technology was simply not designed for. Only a risk-based approach will provide the redundancy to detect the assailant, if not his weaponry. Security agents themselves may fail, be it because of inability or neglect, or at worst due to ill intent, extortion, reward or persuasion. PNR as an automated method will reduce the dependency on the human factor in security screening.

Summary

Only a strategic and thus risk-based approach will ensure adequate levels of passenger security and convenience while allowing existing airport infrastructures to adequately cope with future demands. PNR will provide the means to accomplish this goal. Member states must make prudent and determined use of the new PNR Directive's enormous potential while adhering to the EU's high standards of data protection and civil rights. Airports, airlines and security providers should be encouraged to actively participate in making their industry smart and resilient against the menaces to come.

[13] **Schematic Overview of PNR Data Collected in Germany (Based on the German Federal PNR Act)**[48]



/Ineffective, Wasteful and Overly Intrusive: Why PNR Will Not Help in the Fight Against Terrorism and Serious Crime

Alexander Sander, Managing Director, Digital Society e.V.

DIGITALE GESELLSCHAFT

In the aftermath of the 9/11 attacks, some countries like the US started introducing the collection, sharing, retention and analysis of flight data, the so-called Passenger Name Record (PNR). In 2018, a new EU-PNR system will enter into force: PNR data of all travellers flying from, to or within the EU will be retained and used for five years for the purpose of fighting terrorism and serious crimes. This system will affect nearly one billion travellers every year. After five years, five billion datasets will have been fed into the EU-PNR databases. On the one hand, this massive, non-targeted and indiscriminate collection of individuals' data will affect millions of unsuspicious passengers. On the other hand, recent attacks in the EU have shown, that the threat of terrorism is real. Taking into account that many of the attackers have been travelling back and forth prior to their attacks, it comes as no surprise that a considerable number of members of the security community hope to combat terrorism more effectively by falling back upon the retention and analysis of PNR data. But on closer inspection, is PNR really a useful tool to fight terrorism?

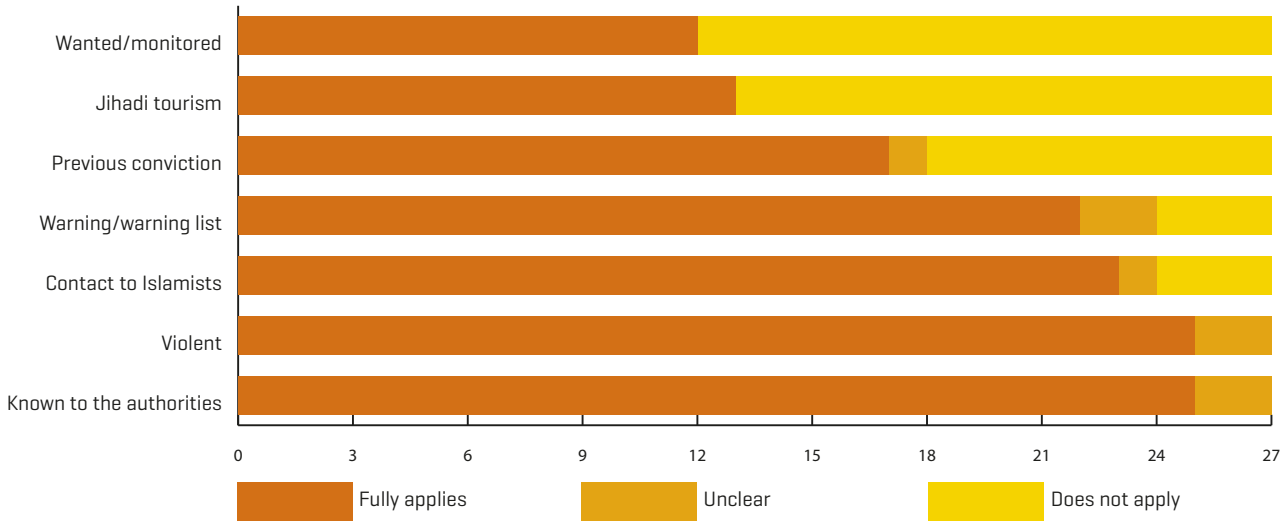
Known and unknown suspects

The EU-PNR system, originally proposed by the EU Commission, is supposed to find »unknown suspects« in order to strengthen the fight against terrorism and serious crime. With the aid of big data analysis and profiling measures, the system is expected to help law enforcement and intelligence authorities identify potential terrorists and felons. However, recent terrorist attacks in various European member-states have revealed all the drastic shortcomings of information sharing between different security authorities and automated data analysis. Even without the retention of PNR data, in most of the cases the perpetrators have been on the radar of police and intelligence authorities for years. These authorities were reluctant to share their information with other authorities and, mostly due to a lack of resources, were not able to conduct targeted surveillance on the suspects in question. At the same time, the security community keeps asking for more databases and measures of indiscriminate mass-surveillance, like the introduction of a costly PNR system. Until today there is no evidence for an increase in security through the implementation of a PNR system. Until today the only argument to justify the retention of PNR data is that most serious crime and terrorism involves travelling. Until today not a single country which has made experiences with the retention of PNR data (some of them – like the U.S. - even for several years) is capable of effectively demonstrating the usefulness of such data collection for the prevention of terrorism and serious crime. Until today it remains unclear how more data about perpetrators or suspects would have enabled law enforcement authorities to prevent any of the attacks. But not only is the benefit of a PNR system for the prevention of terrorist acts or serious crime questionable. Apart from anecdotal reports, no empirical evidence exists for any sort of advantage which indiscriminate data retention could possibly have for the prosecution of such serious offences. Quite to the contrary, the Danish Ministry of Justice has found in an evaluation of their national system for the retention of metadata from electronic communications that the amount of data generated by the system was so large that it in fact hampered effective criminal prosecution. After all, more data does not equal more security. If one's intend is to find the needle in the haystack, it does not make any sense to increase the size of the haystack. What's even worse: if authorities had used their resources properly in order to individually monitor known suspects and effectively share information on them, they would have been able to prevent at least some of the attacks. From all we know today, such a strategy promises to be far more effective than wasting money on the automated spying on millions and millions of travellers.

You need to know who is coming to your country

Advanced Passenger Information (API) data have been collected for decades in order to monitor who is travelling from where to where. API data are also part of the PNR data set, but a PNR includes much more information, such as for example meal preferences, information about the medical condition of travellers, luggage information, data about people travelling together and payment information. A PNR even contains a text box into which airline staff or travel agents can insert whatever they like, i.e. if they find travellers annoying or stressful. Up to 60 pieces of information can be collected per flight and individual in a single PNR. A tangible reason for the expansion of the pool of data collected has not been presented yet . In order to meet the standards of necessity and proportionality laid down in the European Charter of Fundamental Rights, there should have been an assessment whether a less

[14] **Authorities' Awareness of Terrorist Attackers in Europe, 2014 - 06/2017 (Source: Sascha Lobo, Spiegel Online)**[49]



Graph includes the 27 identified attackers of Islamist terror attacks (= at least 1 innocent person was killed) in the EU and their status with the authorities. The total number amounts to 29, however, 2 suicide bombers of the Paris attack have not yet been identified. Some borderline cases were not included, such as Villejuif (04/2015), Saint-Quentin-Fallavier (06/2015) and Manchester (02/2016).

intrusive measure, like the collection and analysis of API data, might help combat terrorism and organised crime. But this assessment has never been conducted. As a consequence, an already running system for the collection and retention of API data capable of letting countries know who is travelling to their country, is being extended to a massive data retention of sensitive passenger data without any evaluation of existing measures and without any evidence that PNR contributes to higher level of security.

The risk of profiling

Thanks to the EU-PNR system there will soon be a database with information on millions of innocent individuals which is continuously being profiled and cross-referenced with other databases. Therefore the data of individuals who are in principle neither subject to criminal investigation nor subject to any security measures will be analysed and evaluated for years. The only reason for putting them through this security scan is the simple fact that they have booked a flight. With a threshold this low, the quality of the ensuing profiling measures comes into focus. At this point, one has to realize that all the data analysis within a PNR system is carried out by algorithms. This means that PNR inherits all the defects and problems that typically come with automated decision making. Even though many people do think of digital technology as being entirely objective, there is actually no such thing as an unbiased algorithm. A bias can already lie in the identification of the problem that the algorithm is supposed to solve. Moreover, a bias might be built into the decision which data to collect and in which way to correlate it. When used for crime-prediction, for instance, such bias could result in racial profiling or other discriminatory practices. One of the main problems when using algorithms to find suspicious patterns in PNR data are positive and negative false alerts. Even an entirely innocent person is always running an increased risk of becoming the target of a criminal investigation. This fact alone can be enough to stigmatise even entire groups of people, for example persons from a specific country or with a particular religious background. The German Federal Constitutional Court stated: »For those persons whose constitutional rights it affects, data profiling means a higher risk of becoming the target of further official investigative measures. This has been demonstrated to a certain extent by the outcome of the data profiling implemented since 11 September 2001. [...] Furthermore, the very fact of police data profiling having been carried out according to certain criteria – if it becomes known – can have a stigmatising effect on those who meet these criteria. [...] It is relevant, with regard to the intensity of the effects of the data profiling carried out since 11 September 2001, that it is targeted at foreigners of certain origins and Muslim beliefs, which always involves the risk of spreading prejudice and stigmatising these population groups in the public perception.«[52]

The risk of unverified data

In contrast to API data, airlines collect PNR data for commercial purposes. They want to ensure that passengers will meet their connection flights or want to cater to special service needs of passengers. Travel and airline agents can access and change travellers' PNR without any access logs and without any proof that this data is correct. If there are mistakes in the API data or if the data is incomplete or inaccurate, it may

lead to more or less annoying situations for the travellers, but they won't have to face any serious consequences. But now, as this unverified data is used for crime prevention and law enforcement purposes, it might lead to travellers having to answer probing questions at the customs, having to tolerate special security checks at the airport or even ending up on a no fly list or worse. At the same time, it will be hard for affected travellers to ask for a correction of incorrect or inaccurate data as they don't know where the data has come from in the first place. This deprives travellers of the option to clear false data sets as they don't have a chance to correct them. From the perspective of the security authorities it means that valuable resources are being wasted on the investigation of completely innocent travellers.

Alternatives

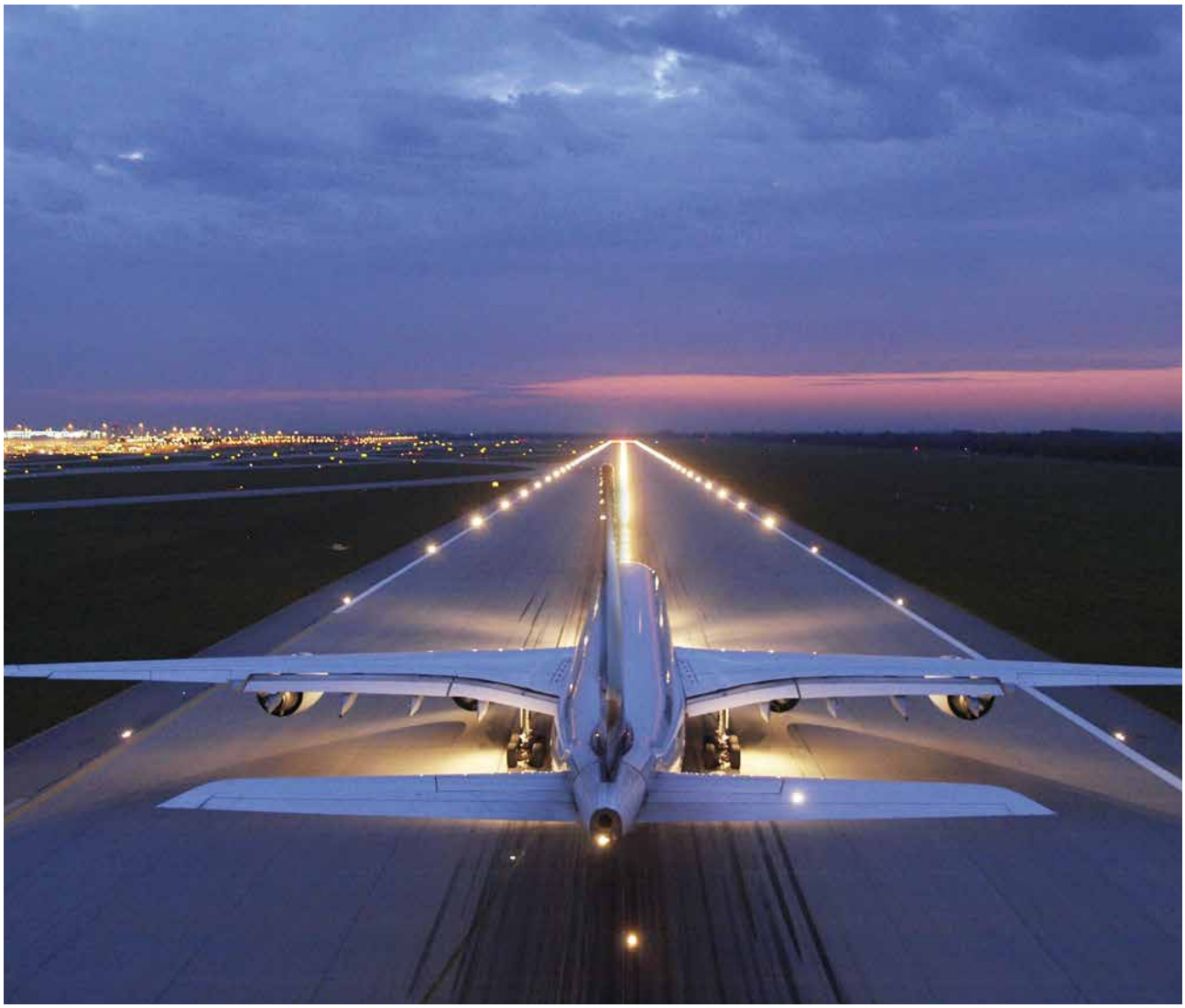
The retention of PNR data is just a first step towards a total collection of all (of a traveller's) movements. An extension of the system to a collection of PNR from trains and ships is already being discussed. In the face of the system's immense cost and its entirely unproven effectivity and therefore unproven efficiency, this cannot be the right path. Instead, a thorough evaluation of already existing measures, including the retention of API data, should be conducted. Resources – which are typically limited - should rather be used to focus on already known suspects instead of trying to create a plethora of new suspects with the aid of automated decision making. When it comes to combatting terrorism and serious crime, targeted surveillance will be more effective than a blanket profiling of all travellers. Big data technology comes with the promise of endless scalability, which might sound tempting to those with a fiscal perspective. On closer inspection, such systems will turn out as a huge disappointment when it comes to the prevention and prosecution of serious crime. Useless and wasteful surveillance of false positives will be only one of the many problems that come with this type of automated mass-surveillance.

»The PNR Directive continues a wrong policy of mass data collection that endangers security and freedom in Europe. Following the terrorist attacks in Paris and Brussels, we now know that information regarding the terrorists was available to the police and security agencies, but was not used for surveillance and exchange. […] The additional amount of data resulting from the collection of PNR data will not support police in their work, but instead increase the data haycock.«

Jan Philipp Albrecht, Vice-Chairman of the Committee on Civil Liberties, Justice and Home Affairs, European Parliament[50]

»If the [German] law [implementing the EU PNR Directive] is adopted by the German Bundestag, the PNR data of more than 170 million people will be collected indiscriminately and be stored for more than five years. Being such a far-reaching intervention, it is essential to make sure that rules and regulations for PNR data collection are consistent with European fundamental rights.«

Andrea Voßhoff, German Federal Data Protection Commissioner[51]



/The Invisible Enemy – Aviation Under Cyber Attack

Sir Julian King
Commissioner for the Security Union, European Commission

It's possible that Friday, 12 May 2017 will turn out to be a landmark date in our attitudes to cyber attacks and a turning point for what we are prepared to do to protect ourselves.

The WannaCry ransomware attack hit 150 countries, with victims including British hospitals, the German railway network, Spanish telecoms, a US logistics giant and the Russian Ministry of Interior.

Some time ago, I published an article saying that the first thing I do in the morning is check if I have any pending updates to install on my smartphone. I don't know if 66 days have elapsed since then, but that is the timespan which psychologists say it takes to form a habit. And making a habit of small cybersecurity-related actions like this is what we all have to do to play our part in the battle to make ourselves safer.

We appear to be entering a new phase in our relationship with technology - in particular the »smart« variety, which is rapidly altering our interactions with everything from our laptops to our fridges and cars. Technology has the potential to make our lives easier, but with cybercrime rising at a faster rate than the use of the Internet, the capacity for it to touch the lives of us all has never been greater.

As Europol's recent Serious and Organised Crime Threat Assessment[55] highlighted, the scant detection rates and chances of prosecution mean that cybercrime has never been more widespread, profitable and low risk from a criminal's point of view.

The UK's National Crime Agency[56] noted last year that cybercrime surpassed all other kinds of crime combined, with computer misuse and computer-enabled crime accounting for 53% of all crimes committed. In some countries like Italy, physical bank robberies are on the verge of extinction – down by 90% over the last decade – while online crime has soared by 67% in the last year alone.

Globally, the cost of cybercrime is estimated to range between $375 billion and $575 billion dollar annually. But if the scale of business losses is alarming, just consider the threats that we now face to the integrity of our democratic institutions. France's presidential election suffered an 11th-hour drama when President Macron's campaign team announced it had fallen prey to a »massive and coordinated hack« which resulted in a flood of leaked material, including fake documents, being spread on the Internet with the clear intention of influencing the result.

In March, the Dutch government took the decision to hand count all ballots in the general election[57] to prevent potential hackers from influencing the outcome.

»While the aviation security sector was not affected by the 12th of May cyber attack it remains a very attractive target for cyber criminals and cyber terrorists, and a possible strategic target in the hybrid war.«

»Cyber weapons can damage a physical object as badly as a traditional weapon.«

Eugene Kaspersky, CEO and Founder, Kaspersky Lab[53]

»Collaboration and exchange between states and other stakeholders is the sine qua non for the development of an effective and coordinated global framework to address the challenges of cybersecurity in civil aviation. Cybersecurity matters must be fully considered and coordinated across all relevant disciplines within state aviation authorities.«

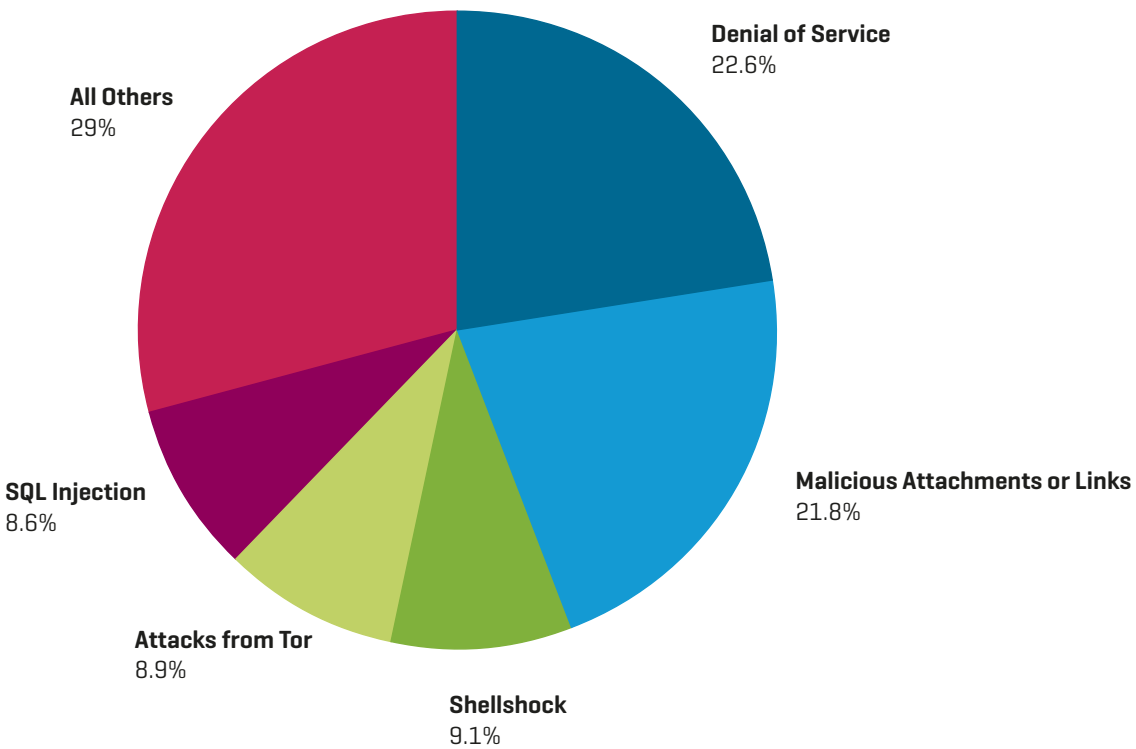
Luc Tytgat, Director of the Strategy and Safety Management Directorate, European Aviation Safety Agency[54]

As in other industries, airlines and airport operators are concerned with the theft of sensitive customer or company data. But an additional vulnerability is the technology being used to improve the connectivity of flight operations systems with ground crews and air traffic systems. The Next Generation Air Transportation System will rely upon the Global Positioning System, which is software-based and Internet-connected. This will bring with it greater potential vulnerability, which must be eliminated. While this enhanced communication and integration is essential to the improvement of financial and operational performance, advances such as these provide more opportunities for cyber criminals in ransom attacks or terrorists aiming to hit the civil aviation sector - which is still considered an attractive target for its symbolic value and high impact on public opinion.

We now need to develop a comprehensive response not only based upon prevention and building resilience, but also upon reinforcing detection and deterrence. We need to look at the security of devices and systems, and increase awareness of cybersecurity and the importance of cyber hygiene. Only by increasing the likelihood of getting caught and punished with appropriate penalties can we diminish the allure and profitability of cybercrime.

In May 2017, the European Commission published the mid-term review of the EU's digital single market (DSM), reporting on the progress made in the last two years on creating the right conditions for Europe's digitally powered and enabled future. The DSM has the potential to unlock €415 billion of growth annually and to revolutionise the way we work, shop and live. But as well as the advantages, we need to be clear-eyed about the accompanying risks. That is why the Commission is accelerating its work on the review of the EU's 2013 Cybersecurity Strategy. Four years may not sound like long ago, but in cyber terms it is a lifetime and in an area where every day has the potential to turn up something new, planning ahead, being prepared and being proactive must be central to our response.

(15) **Most Prevalent Cyber Attack Vectors in the Transport Sector, 03/2015-05/2016 (Source: IBM)[58]**



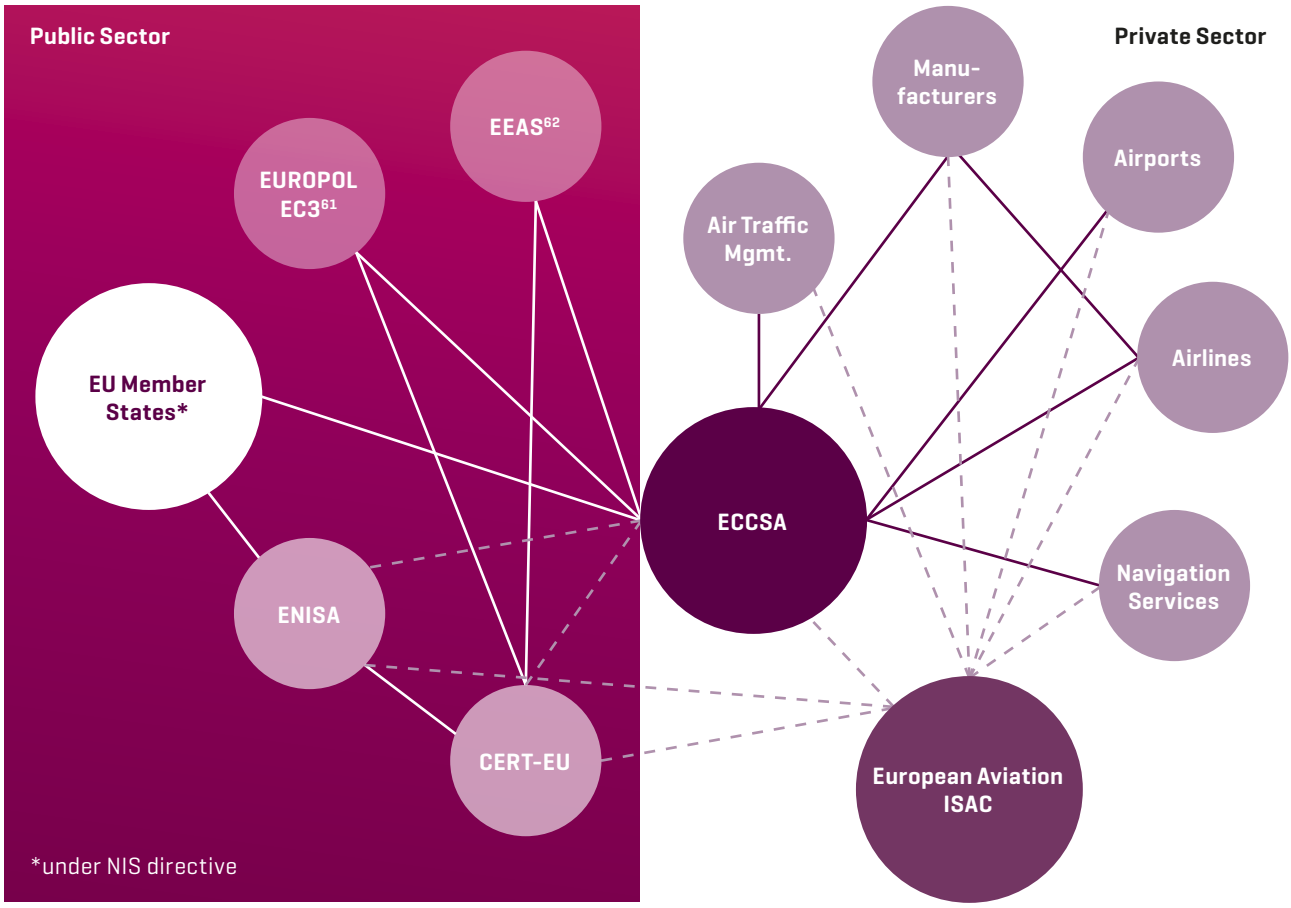
/European Centre for Cyber Security in Aviation

The EASA »Cybersecurity roadmap« presented in 2015 has been considered a basis for implementing a cybersecurity framework for aviation.[59]

An important part of this roadmap is the implementation of a European Centre for Cyber Security in Aviation (ECCSA), which foundation was laid down in a jointly presented »Memorandum of mutual Cooperation« between EASA and CERT-EU (Computer Emergency Response Team) in February this year. ECCSA will primarily serve as a platform for sharing and managing information - a key enabler for implementing a resilient aviation cyberspace. ECCSA will provide secure means for aviation stakeholders to exchange domain-relevant cybersecurity information such as vulnerabilities, i.e. weaknesses that can be used for malicious purposes, as well as events and incidents that might be worth sharing with the aviation community. ECCSA's operational team of analysts will provide additional input to the information shared by the participants, with the aim of facilitating a knowledge and risk profile of aviation cybersecurity threats. The first implementation phase foresees the development of the following tools and services in the period 2017-2018:

- A public website reporting cybersecurity news and ECCSA initiatives
- Open source intelligence services for members
- A collaboration platform for members to exchange sectorial cybersecurity information

[16] **Institutional Framework of the European Centre for Cyber Security in Aviation (Source: EASA)[60]**

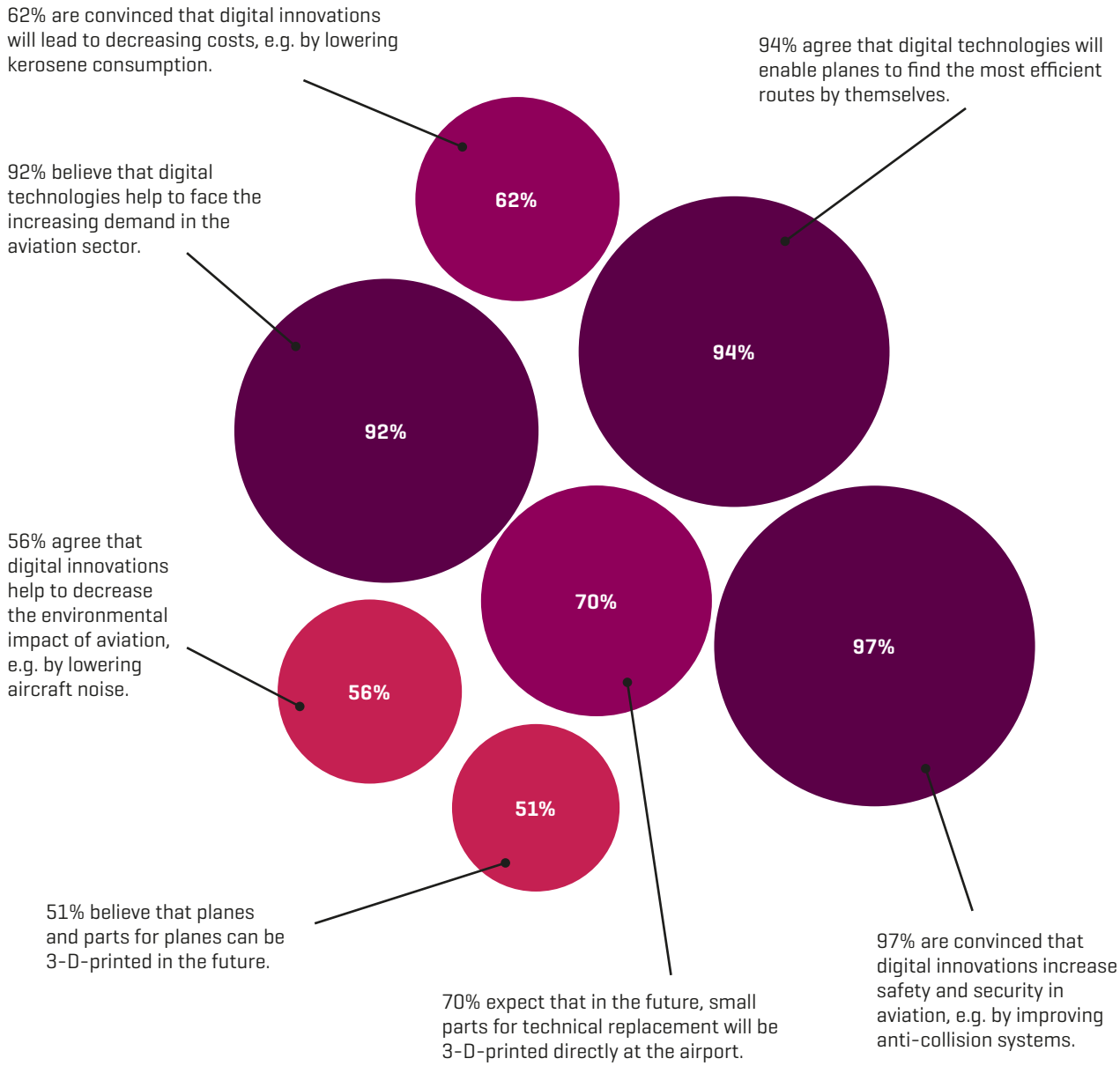


/A Hacker Is Not Needed

Marc Bachmann, Head of Aviation and Defence, Bitkom e.V. - Digital Association of Germany
Marc Fliehe, Head of Information Security, Bitkom e.V. - Digital Association of Germany

bitkom

[17] **Selected Results of a Survey on Digitalisation among Airline and Aviation Industry Representatives (Source: Bitkom e.V.)**[63]



The potential stemming from digitalisation confronts companies with extensive and dramatic changes in the field of aviation. The challenge is to anticipate and mitigate future risks – whether of a technical or organisational nature. It is important not only to face known risks, but also to prepare for unknown and unpredictable risks, which may pose a potential disruptive threat to the whole industry in the future.

The connectivity derived from widespread digitalisation, including mutually reinforcing or even multiplying effects, must take into account the consequences for safety and security. This issue is also being tackled through legislation: with the first German IT security legislation in 2015, large parts of the aviation industry were defined as critical infrastructure (KRITIS). The focus is on defining and implementing industry-specific security standards.

Observing IT security solely in the context of office environments and simple IP-based networks, it can be seen that IT security risks (including all hazards from more open networks) are already being managed quite well. Security concepts focus on three aspects: integrity, confidentiality and availability. The hazards are known or the change patterns of abnormalities follow a predictable course, the group of users is mostly limited; the interaction with other persons, networks and devices is known or observable.

Market expertise in this area is (relatively) broad and profound, and can easily be found. The same is true for external technical support (also in cases of damage or loss). High-tech products (such as intrusion detection and intrusion prevention systems) offer optimum protection and providers have a vast experience and global infrastructures to support users. Software and security patches are provided within a few hours or days.

The prerequisites from office IT cannot simply be transferred to aviation and cyber security. The challenges are much more significant and the conditions are fundamentally different. From an aviation perspective, this means facing the following challenges:

1 The infrastructures that need to be secured have long product life cycles with direct consequences for development and innovation cycles. Often, aircrafts that need to be secured against hackers are over 20 years old – or even older. Software updates are only possible with distinct lead time (and after passing the necessary quality testing). New software could possibly lead to the loss of existing certifications, which would lead directly to further complications and thus additional expenses.

2 Long development times and product life cycles make the principle of »security by design« all the more important. Software developments must take into account that the installed products need to be resilient against cyber attacks in 20 years or more. Therefore today's knowledge and current industrial standards need to be refined into security architectures and implemented in further software developments. The ability to update, hardware security modules, digital signatures and certificates, virtualisation and sandboxing should provide the basis for this.

3 There is a serious lack of IT security experts on the HR market. Profound expertise and industry know-how in the technicalities of infrastructures, protocols and processes are crucial in the aviation and aerospace industry. Comprehensive and industry-specific training including current digitalisation trends is needed to secure the future of the HR market.

4 Many of the infrastructures used in aviation need to be open to different participants – the focus here is on availability and interoperability. Due to the criticality of these infrastructures, subsequent adjustments are difficult and only possible in the long term. Security features need to be implemented with a view to the future.

5 The conflict between safety and security needs to be researched intensively and their importance in practice needs to be discussed. In many infrastructures, for historical reasons, the focus is on functional safety, which can be undermined in the case of a lack of IT security. IT security should not be the »trade-off« for safety. Both components have to be seen as a whole and should complete each other.

6 We need a risk management that focuses on smart attack scenarios based on the complexity of infrastructures, processes and how they interact with each other. These scenarios can be used to develop countermeasures and training on how to handle cyber attacks – for example simulator training.

7 In the future, defending against cyber attacks will not just be the task of supporting resources and processes, but also part of a pilot's skill set. It is especially important to detect and understand such attacks, e.g. against the integrity of flight data, or at least take them into account in abnormal flight situations.

Aviation can only stand up to its responsibility if the system and the acting persons in it (e.g. the pilots) not only use the technologies available, but also control them.

The »principle of hope«(»It won't hit me«) will not work anymore. The challenges outlined do not even require the creativity and intelligence of a hacker to be exploited; they are conditioned by the architecture. Blaming the providers is not the solution: the new challenges are a product of the digitalisation – and the result of a lack of demand by the industry in the past. We need a change of mindset. We need to stop being digitalised and start actively shaping digitalisation. The experiences of other industries, e.g. in the context of the Internet of things, could help us find the right path.

/The NATO Industry Cyber Partnership: Strengthening Collective Cyber Defence

Anna M. Barcikowska, Head of Industry Relations, NATO Communications and Information Agency[64]
Jill O'Donnell, Industry Relations, NATO Communications and Information Agency

During an informal gathering in April 2015 in The Hague, business executives representing IT, financial and security and defence sectors and NATO officials discussed how they could work together to bring to life the new NATO Industry Cyber Partnership (NICP), endorsed by NATO allies at the Wales Summit the previous year. Since that time, cyberspace has come to play an even larger role in NATO's deterrence and defence posture. NCI Agency - responsible for providing cybersecurity and information assurance throughout NATO - defended NATO networks against an average of 500 cyber incidents per month last year, a 60% increase over 2015. Also in 2016, alliance leaders at the Warsaw Summit officially recognized cyberspace as an operational domain along with air, land, and sea. That decision will allow the alliance to integrate cyber into training and military planning in order to better protect its missions and operations.

»Our defence posture must be able to deal with rapidly evolving cyber threats, so our job is never done«, said Koen Gijsbers, General Manager of NCI Agency. »That sets a high bar for cyber resilience. It also means that partnerships—including new ways of partnering with industry—are critical. As the cyber threat increases, so does the opportunity for NATO and industry to improve our collective cyber defence by working together to better understand and counter cyber threats.«

The very idea for the NICP illustrates the recognition that when it comes to cyberspace, NATO and industry are in the same fight. Fast-moving cyber threats and rapid technology evolution are the new normal for defence organizations and companies alike. Working together - especially through threat information sharing - strengthens collective cyber defences. The earnest discussion in The Hague generated a level of momentum that reflected the gravity of the cyber threat. Two years later, the NICP is helping to keep NATO and industry networks safer.

As NATO has increased the depth and scope of its collaboration with industry partners on cybersecurity, one lesson has been paramount: successful cooperation requires high levels of trust. Working together with industry on cybersecurity requires an intensity of information sharing and ongoing communication about common threats that is more characteristic of relationships between allies than relationships between defence organizations and industry. And yet, cooperation with industry is absolutely essential: this may be the first time in history when industry input is so crucial to building a more complete picture of the threat. Information sharing may be the single highest-impact, lowest-cost, and fastest way to implement capabilities NATO already has in hand to enhance cyber resilience, improve incident handling and mitigate vulnerability to attack. Allied Heads of State and Government recognized this at last year's Warsaw Summit when they highlighted the importance of information sharing with industry to improve understanding of cyber threats.

NATO and industry partners share cyber threat information through a NICP Malware Information Sharing Platform (MISP). The NICP MISP combines a community of members and a web-based information sharing platform that facilitates information sharing between NATO cyber defence offices and industry on cyber threats and relevant malware and incidents. It aims at breaking down the barriers that prevent information sharing by enabling exchanges of technical characteristics of malware within a trusted community without having to share information about the context of the attack. It combines a searchable knowledge base repository with a multidirectional information sharing tool, providing an automated mechanism to enable the import and export of data and an interface with other systems. The aim is to speed up the detection of incidents and the production of defensive countermeasures. Examples of information categories that are exchanged on the one-to-many basis include:

- Vulnerabilities (Webapp exploits, zero-day vulnerability information before public disclosure)
- Information on botnet command & control and associated IP addresses
- Malware and Advanced Persistent Threats (command & control infrastructure, dropzone, compromised devices)

- Indicator of Compromise info from incident investigations affecting the corporation (not the customers)
- Indicator of Compromise of new or new variants of malware
- Zero-days on 3rd party software
- Anonymized Industrial Control Systems (SCADA) related vulnerabilities and incidents and patterns of attacks

The use of information exchanged in the community is governed by the Traffic Light Protocol, and in general requires that information is not used for commercial purposes but for increased knowledge, internal research, implementing signatures, infrastructure protection, internal security operations centers and trend analysis.

(18) **Cyber Threats to NATO (Provided by NATO Communications and Information Agency)**

Wide Range of Cyber Threats

Opportunistic attempts	Cyber crime	Insider threat

Potential Damage of a Cyber Attack

Loss of life	Destruction of sensitive data	System unavailability	Reputational damage

Number of Attacks

550 million
cyber events per day processed by NATO security sensors

16-17
cyber incidents raised per day that require immediate action (<0.000004% of all attacks)

7 Stages of an Attack

1	2	3	4	5	6	7
Re-connaisance	Weaponization	Delivery	Exploitation	Installation	Command & control	Actions on objectives

Defence Against Cyber Attacks - 6 Stages of Defence

1	2	3	4	5	6
Detect	Deny	Disrupt	Degrade	Deceive	Destroy

[19] **NATO Partnerships: Key to Cyber Security (Provided by NATO Communications and Information Agency)**

Cooperation

Industry
Wales Summit 2014
NATO Industry Cyber Partnership
Multiple signed partnership agreements

European Union
02/2016: NATO and EU sign technical arrangement on cyber defence cooperation
Threat information sharing

Ensuring NATO's Cybersecurity: Multi-Layered Approach

Network-based

Host-based

User-based

Upcoming Investments in Cybersecurity

NIAS Cyber Security Symposium 2017: defining NATO's future cyber requirements

Invitation for bids in 2017, first investments in 2018

Approx. 70 million EUR investments planned between now and 2019

For one-to-one information sharing with industry partners, NCI Agency has in place 12 Industry Partnership Agreements (IPAs). These allow for timely information exchanges on cyber threats, so both parties can enhance situational awareness and better protect their networks. Hundreds of indicators of compromise have been shared, and the pace of exchanges continues to grow. The Agency also shares other technical information with industry through the NICP portal. This includes a »hardening guide«, which lists technical configuration settings and recommendations for operating systems and applications in use in NATO to render them more secure.

NATO and industry partners are also pooling their expertise through a series of Threat Vector Analysis (TVA) workshops focused on identifying cyber threats as well as techniques, practices and procedures to counter those threats. To date, five TVA workshops have considered a diverse array of attack vectors, including Distributed Denial of Service (DDoS) attacks, the insider threat, and the challenge posed by mobile devices.

TVA workshops have resulted in several significant outcomes that are directly bolstering NATO's and industry's cyber defences. For example, TVA participants quickly discovered that a common taxonomy of cyber threats was lacking, so they developed one - now in place on the NICP MISP - to improve communication and share information more efficiently on cyber threats. Other TVA discussions resulted in decisions to share NCI Agency's hardening guide for mobile platforms on the NICP portal as well as technical characteristics of DDoS attacks against NATO infrastructure.

When NCI Agency surveyed industry executives last fall about the benefits of participation in NICP, »trust« and »understanding« were keywords that appeared repeatedly. They valued the opportunity to build trust with NATO and improve understanding of each other's perspectives on cyber threats. Since the initial meeting in The Hague, the discussion has evolved from how NATO and industry should cooperate to how they can cooperate better. Trust will remain key to this effort.

The NICP is effective because NATO and industry are co-equal partners. The benefits are mutual, decisions are taken together, and everyone involved is genuinely committed to strengthening NATO's cyber defences so it can focus on what it was created to do: defend allies.

/Cyber Sabotage and Cyber Attacks Staged by Foreign Intelligence Services

Dr Hans-Georg Maaßen, President, BfV - The German Domestic Intelligence Service

Up until 20 years ago, newspapers, radio and TV broadcasts as well as phone conversations, facsimiles and standard mail predominated our daily communications. In the early 1990s, computers, the Internet, emails, mobile phones and other forms of digitalisation came into our lives bit by bit.

This digital development has rapidly changed our world over the past few years, modifying our society's communication patterns and multiplying the scope of information that is readily available. The advantages gained through these technical capabilities are evident. However, it cannot be denied that they also bear risks when abused.

At present, not a single week goes by without reports about a cyber attack being staged against a public or private institution in Germany. The German Domestic Intelligence Service (BfV) is aware that extremists and terrorists are exploiting new technologies for their own purposes and adapting their activities and organisational concepts to suit. Especially for foreign intelligence services, the advancement of information and communication technologies provides manifold opportunities for data spying and espionage or for political disinformation, modifying data and computer sabotage. Non-governmental protagonists also get the chance to conduct sabotage and to spread propaganda.

In recent years, espionage through cyber attacks in particular has become the main tool of numerous intelligence services, posing a high risk to potential or actual victims.

In this context, the Federal Republic of Germany is of particular interest to foreign intelligence services due to its geopolitical position, its role within the European Union and NATO, and due to many high-tech companies based here. Germany's open-minded, pluralist society makes it easier for foreign powers to gain intelligence - either overtly or covertly.

The intelligence and security services of the People's Republic of China and of the Russian Federation in particular massively engage in spying activities directed against Germany. Their respective focus depends on the political intentions and orders of their governments, including the governmental order to support companies with information gained in an intelligence context.

Various incidents in recent years have demonstrated how successful such cyber attacks can be. In particular the attacks against the German Bundestag in the summer of 2015 and 2016 as well as attempted attacks against political parties show that there is a general intelligence interest in elected representatives and their organisations in Germany.

The risk for critical IT security systems posed by cyber sabotage became dramatically clear to the general public in 2010, when information on the Stuxnet virus first emerged. Stuxnet was a sophisticated and successful cyber sabotage directed against the Iranian nuclear programme. German interests were not directly affected, but the incident clearly demonstrated that there is a potential risk of national German infrastructures possibly being targeted by such attacks.

Even though there have been no established serious cases of cyber sabotage in Germany, the risk is not to be underestimated. The reason is that malware which has so far been used for cyber attacks particularly aimed at gaining intelligence or at spying can be modified so as to be potentially used for sabotage purposes, too. As soon as an attacker has gained full access to an IT system, he/she will be able to freely start operations, including activities affecting the integrity or availability of the system.

For the time being, there is no direct risk to critical German infrastructures emanating from extremists, terrorists or foreign intelligence services. But serious political or foreign relations developments and an actual or presumed involvement of Germany in, for example, war-like conflicts bear the risk of cyber sabotage activities being staged against German interests in this context.

»Airports are other possible targets: sabotaging their power supplies, for example, would have unpredictable consequences for the operation of different areas of the airports and even beyond.«

Attackers first collect information and monitor their targets before taking action – which is easier than one would expect. Much of the required information is freely available on the Internet. In a test scenario, members of BfV's cyber defence team put this particular point to the test with a German airport: It did not take long to gain an overview of the technical facilities of the airport, concrete plans, employed service providers, information on the professional and private backgrounds of certain airport employees possibly being good targets in an attack, and intelligence on the IT and operating systems used. With a collation of all these pieces of information, it would have been possible to gain access to the airport's IT system via the identified persons with an email infected with malware, and to turn off the airport's power supply.

That scenario was only a test, a comparable cyber attack against this airport has not become known so far. Nevertheless, BfV has spoken to the airport operator in order to raise their awareness for such potential risks, and the operator has responded accordingly: identified weak points have been eliminated and sensitive documents have been removed from the Internet.

Moreover, it is necessary to counter the existing threat situation with lasting fast and efficient defence and intelligence collection mechanisms related to potential and actual cyber attacks. Hence, it is indispensable to realise, continually update- and review organisational, technical and legal measures aimed at a stronger cyber defence for all the institutions concerned or potentially exposed.

To strengthen cybersecurity and supplement the expert reports of IT service providers that mainly focus on the fast elimination of present IT security incidents, BfV can supply information resulting from its intelligence collection and revealing certain IT infrastructures used for attacks (so-called indicators of compromise, IOC). With this information, exposed entities are given the chance to identify whether they are affected, to stop these IT infrastructures in advance from potentially accessing their IT networks, and thus to increase protection against cyber attacks. Furthermore, BfV has introduced a new format with its »Cyber Letter«, which regularly forwards alert messages and reports to authorities and the industry.

There are manifold risks emanating from cyber attacks. Hence, the authorities are not the only ones in charge. We will only be able to protect our community in the long term if the state and the industry jointly counter this growing threat with a close and trusting co-operation. Security agencies like BfV can advise the industry on this topic discreetly and free of charge.

Threat Scenario: Cyber Attack on the Energy Infrastructure of an Airport

Cyber attacks pose an imminent threat to the economy, politics and critical infrastructures. The potential use of cyber attacks ranges from espionage to sabotage; even the slightest form of carelessness may provide a gateway to attackers. The German Domestic Intelligence Service (BfV) deals with these risks and has developed a test scenario.

By means of publicly accessible sources, a lot of information such as personal details, technical background data and even information on the energy management of an airport can be collected on the Internet within a short period of time. For example, information on the manufacturers and type designations of industrial control systems used in the field of energy supply could be found. In particular, websites of service providers such as manufacturers and engineering offices very openly share information. Details such as »horizontal and vertical data consistency« or »continual data coupling to the office network« reveal information on the access points to the control systems. In single cases, even layout plans of the control systems including room information have been found.

Manuals and demo versions of basic control systems can be easily downloaded from the Internet. Hence, a hacker does not need an expensive full version to »practise«. Current security gaps can be found by using specific search engines.

One of these search engines is SHODAN, which makes it possible to search for already known vulnerable systems connected to the Internet or, specifically, for weak spots. In March 2016, BfV was able to point out to a big European airport a control system accessible via the Internet; it was possible to log on to the system online using default settings. SHODAN, but also other search engines, even provide the option of searching for codes to take advantage of known weak spots. The attackers do not necessarily have to be able to programme themselves; codes ready for use can be directly downloaded.

The manufacturers often know about these weak spots and therefore patches are swiftly provided. The main problem, however, is the users' behaviour when it comes to installing patches: quite often, the principle »never touch a running system« seems to be of priority to the users. Moreover, industrial control systems can also fall into the hands of

attackers through weak operating systems. This is why sensitive control systems only ought to be operated in a secure, isolated environment – that is physically separated from all other networks such as the office network.

Cyber sabotage does not only have an economic but also a psychological and political effect: a successful cyber attack on an aeroplane or an airport can undermine trust in the industrial sector. While technical failures or attacks by individuals are still perceived as single cases and countermeasures taken can be presented to the public, measures in cyberspace, which is not visible, are much harder to understand for many people.

Incidents such as Stuxnet in Iran or BlackEnergy in Ukraine show that cyber sabotage carried out by states is a realistic scenario. Furthermore, vulnerable machines are often targeted by encryption Trojans: most recently, for example, the ransomware WannaCry was able to infect more than 200,000 systems and encrypt their data. The victims included transport and logistics companies but also private individuals. BfV has been tasked to protect Germany's economy from cyber espionage and sabotage by foreign states. Please do not hesitate to contact us – we guarantee you absolute confidentiality!

/Securing Smart Airports

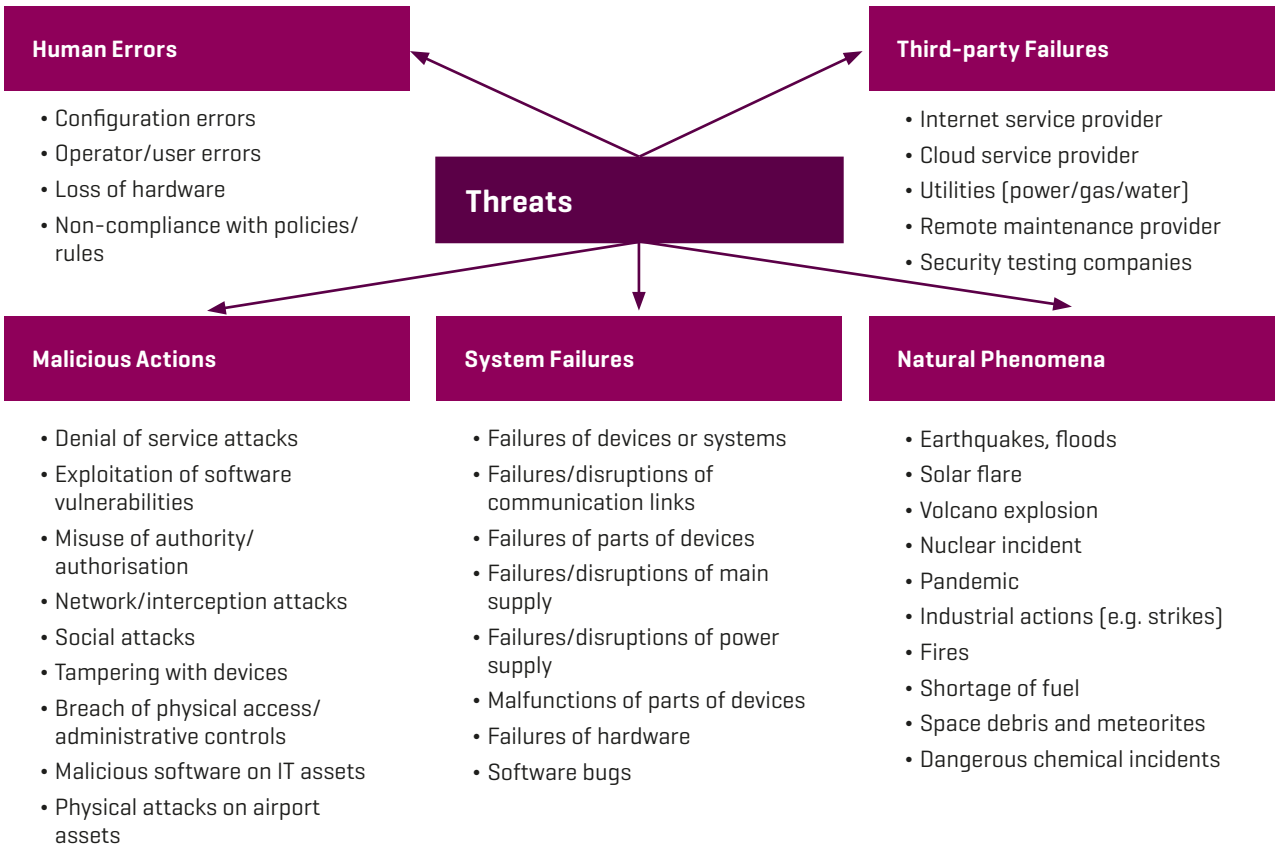
Prof Dr Udo Helmbrecht, Executive Director, European Union Agency for Network and Information Security

ENISA, the European Union Cybersecurity Agency, has been working on aviation cybersecurity since 2010, closely collaborating with relevant stakeholders both regarding studies and cyber exercises. In 2016, ENISA published a study on »Securing Smart Airports«[65], providing airport decision makers and security personnel with a start-up kit to prevent possible attacks and implement available good practices in order to safeguard passengers and operations. ENISA's future work in the field is aimed at enhancing the security and resilience of air transport in Europe together with all relevant key stakeholders and agencies.

ENISA aims to help airports make use of integrated Internet of Things (IoT) components on top of the legacy infrastructure. These airports are implementing these new smart components to offer travellers a portfolio of services that spans from self or automatic check-in, baggage and document check, flight booking management and way-finding services to automated border control and security checks. While enhancing the user experience, these components also pave the way for new attack vectors and expose airport assets to a larger attack surface.

Smart airports have the potential to deliver important improvements in overall security effectiveness, operational efficiency and passenger experience and safety. However, the increased flow of information, data processing and connections among devices and systems also bring risks

[20] **Overview of Threats (Based on the ENISA Report »Securing Smart Airports«)[66]**



[21] **Layers of Stakeholder Interaction (Based on the ENISA Report »Securing Smart Airports«)**[67]

Airport Organizational Boundary Shows the limit of what is controlled by airport management	**Integration Layer** Allows data and information sharing among applications			**Airport Service Boundary** Shows the airport supply chain and support services that lie outside direct management control of the airport
	Application Layers Stakeholders' interactions			
Customs & immigration Air traffic control Aircraft servicing, maintenance and re-fueling Food & drink, accommodation and retail Building management Passenger Information Unit (PIU) Passenger security Car parking Airport operations data centre Perimeter security Local roads Baggage handling & sorting Baggage screening	Best practices, guidelines	**International Organisations** IATA, ICAO	International pax regulations (Chicago Convention)	Aircraft manufacturers Airline operations centre Central flow management unit ATM information management Network security management services Equipment suppliers Floor-space management Consulting services Airport administrative duties Building maintenance Legal and financial services National rail, underground, bus and highways
	ISMS/ISO standards	**EU Organisations** European Commission, EASA, EUROCONTROL	European data & information management and distribution	
	Regulations	**National Government** National CAAs, border control	National airspace management	
	Planning, governance	**Local Government** Transport and planning authorities, local communities	Planning, procurement	
	Businesses, service provision	**Industry** Third-party providers industry /manufacturers, network service providers	ADS-B, ground stations (VHF, VDML), beacons, GPS	
	Service experience	**Passengers/ Travellers**	Passenger safety	
Airport management and operations database Airport IT infrastructure	**Networking Layer**			VHF, VDML voice and datalink, ADS-B, ACARS[68] Host IT infrastructure
Cable infrastructure Fibre optic infrastructure	**Physical Layer**			Radar Beacons and ground stations

that need to be addressed. Vulnerabilities can be exploited by malicious actions, but also human errors, system or third-party failures and natural phenomena can occur. The Airport Cooperative Research Program (ACRP, 2015)[69] has identified a trend towards greater interconnectivity as airports and their stakeholders leverage digital technology to optimise resources and work together more efficiently. Airports are also becoming increasingly reliant on computer services delivered via the Internet, with some airports allowing passengers and staff to use their own hardware (smartphones, tablets and computers/laptops) to access airport data, systems and network resources. A report by the UK Centre for the Protection of National Infrastructures (CPNI)[70] identifies the consolidation of IT systems and Internet-based solutions in civil aviation management and operation as a major reason for increased vulnerability to malicious cybersecurity attacks. This introduces further vulnerabilities that can give rise to cyber attacks and subsequently risk the safety and performance of civil aviation. The challenge is to address security issues not only to enhance security, but also to ensure safety. For this reason, ENISA has decided to perform this study with the aim of helping asset owners and all stakeholders involved to enhance cyber security for the safety of European passengers.

The approach taken follows the methodology based on the ENISA threat landscape approach and involves:

- Mapping assets and developing a threat taxonomy that covers possible attacks.
- Validating and/or identifying further gaps through interviews with security experts working in the field of airport information security.
- Enumerating possible attacks that target or affect smart components in airports.
- Mapping available good practices and describing in detail three attack scenarios and related mitigation actions to provide practical examples of implementation.
- Performing a gap analysis of the current situation.
- Proposing recommendations for future steps in cyber-security for airports in Europe.

After analysing the core functions and assets, ENISA presents a taxonomy of cybersecurity threats to smart components within the airport perimeter followed by the attack vectors and actors involved. The threats are mapped to categories of assets they relate to. Finally, specific attacks are highlighted against target elements, illustrating the threats to smart airport assets.

In order to give a complete overview of all possible attacks, the study offers a list of potential incidents and provides a proof of concept for three specific attack scenarios. The three attacks have been selected by the interviewed experts as the most important:

- Tampering with airport self-serving e-ticketing systems
- Network attack on baggage handling
- Drone jamming and spoofing aircraft - airport and traffic control - airline communications

These scenarios were developed to underline the increased attack surface and challenges when smart components are integrated in the traditional airport IT systems. The attack scenarios are presented in detail: the type of attack; a detailed description of the scenario; the domains where those scenarios have been or could potentially be applied; their likelihood; and the key users and stakeholders that actively take part in each scenario. Additionally, security parameters are mentioned such as cascading effects, recovery time and efforts, assets involved, criticality, and existing good practices that could be deployed. To complete the study, all available good practices for smart airports are presented and arranged according to three main groups: technical/tool-based; policies and standards; and organisational, people and processes. The goal is to provide an easy and comprehensive guide for airport decision makers to implement available good practices, in order to safeguard passengers and operations.

Finally, eight recommendations for enhancing the security and resilience of smart airports in Europe are presented in the report, tailored specifically towards decision makers, airport operators and industry.

Recommendations for airport decision makers (CISOs, CIOs, IT directors and heads of operations) and airport information security professionals:

- Prioritise cybersecurity for safety
- Establish a clear airport cybersecurity stance and allocate adequate roles and resources
- Revise cybersecurity policies and practices based on good practices monitoring
- Implement network-based, holistic risk and threat management policies and processes for cybersecurity

Recommendations for policymakers:

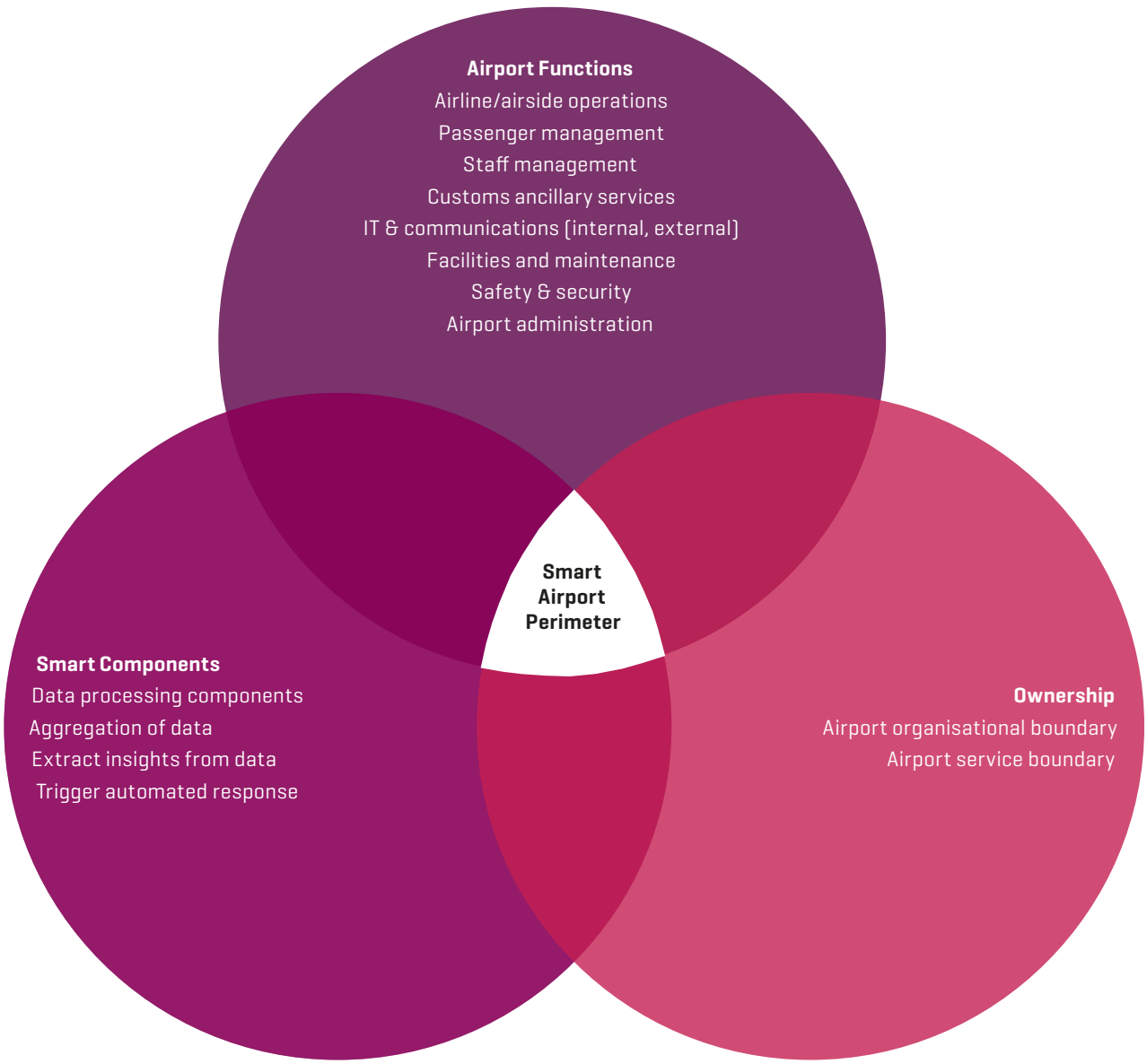
- Promote and facilitate the development of common guidelines, standards, metrics, awareness and knowledge exchange on cybersecurity for smart airports
- Facilitate the development of accreditation and third-party auditing for cybersecurity in smart airports

Recommendations for industry representatives:

- Collaborate with key stakeholders in the development of specific standards for cybersecurity products and solutions
- Work with airport operators to develop products and/or solutions that are aligned to their cybersecurity requirements.

ENISA's future work in the field is aimed in enhancing the security and resilience of air transport in Europe together with all relevant key stakeholders and agencies. In the context of the NIS Directive[71], ENISA will assist member states and the European Commission by providing expertise and advice, as well as developing and facilitating the exchange of good practices, with the ultimate goal to enable a higher level of security for Europe's air transport infrastructure.[72]

[22] **Smart Airport Perimeter (Based on the ENISA Report »Securing Smart Airports«)[73]**



/Preparing for the Worst - Airports as Critical Infrastructure

Alexander Borgschulze
Senior Vice President Corporate Security, Munich Airport;
Chairman of the Executive Board, Bavarian Association for Security in the Economy (BVSW)

The world is once again facing major security challenges. Many of today's crises are widely considered a breeding ground for international terrorism. Through spectacular attacks, such as 9/11, terrorists aim to unsettle society and instil fear. Due to its great symbolic power, aviation has been and continues to be a target of international terrorism and must therefore be adequately protected. Despite having already implemented a variety of measures to hinder terrorists from carrying out an attack on air traffic, the aviation sector remains a preferred target. Such terroristic attacks generate lots of media coverage and impact society in its most vulnerable areas: the freedom of movement and the importance of air transport for the global economy.

Are airports really critical infrastructures?

Airports are generally considered »critical infrastructures«. But are they really? Based on different existing definitions, another conclusion can also be drawn.

It is important to note that the term »critical infrastructure« is not precisely defined by law. According to the »European Programme for Critical Infrastructure Protection (EPCIP)«, it can be defined as »assets or systems essential for the maintenance of vital social functions, health, safety, security and economic or social well-being of people«[74]. The German airport network is decentralised to a large degree. With its hubs and secondary as well as tertiary airports, which represent a corresponding importance for the different regions, it is ensured that airports – no matter where in Germany – can always be reached in a relatively short time. Due to this interchangeability of airports, they are therefore not to be regarded as critical infrastructures in the European sense.

On a national level it is a very different story. Within the framework of the »Strategy for the Protection of Critical Infrastructures defined by the German Ministry of the Interior (KRITIS)«, critical infrastructures »are organisations and institutions with an important role for the community, which would in the event of a failure or impairment lead to sustained supply shortages, disturbances of public security or other dramatic consequences«[75]. Thus, within the transport sector, aviation is considered a critical infrastructure. Nevertheless, as airports are not individual infrastructures, the entire network should be considered when evaluating the security of supply for the population. As bad as the failure of an individual airport would be, its role to ensure continuous supply can be assumed by other airports within the network. The example of the fire at Düsseldorf Airport in 1996 illustrates this: air traffic in Düsseldorf had to be stopped for a few days, but the supply for the population was not at risk at any point in time, as neighbouring airports handled the traffic to a large extent until a resumption of traffic in Düsseldorf was possible.

There are also arguments claiming that airports are covered as critical infrastructure by the »IT-Security-Act«. Following the same line of thought, these claims are also not valid. Nevertheless, aviation and in particular some airports as well as German Air Traffic Control are among the affected sectors and must now incur increased efforts – despite the fact that own standards exist and much is already regulated in the air transport sector.

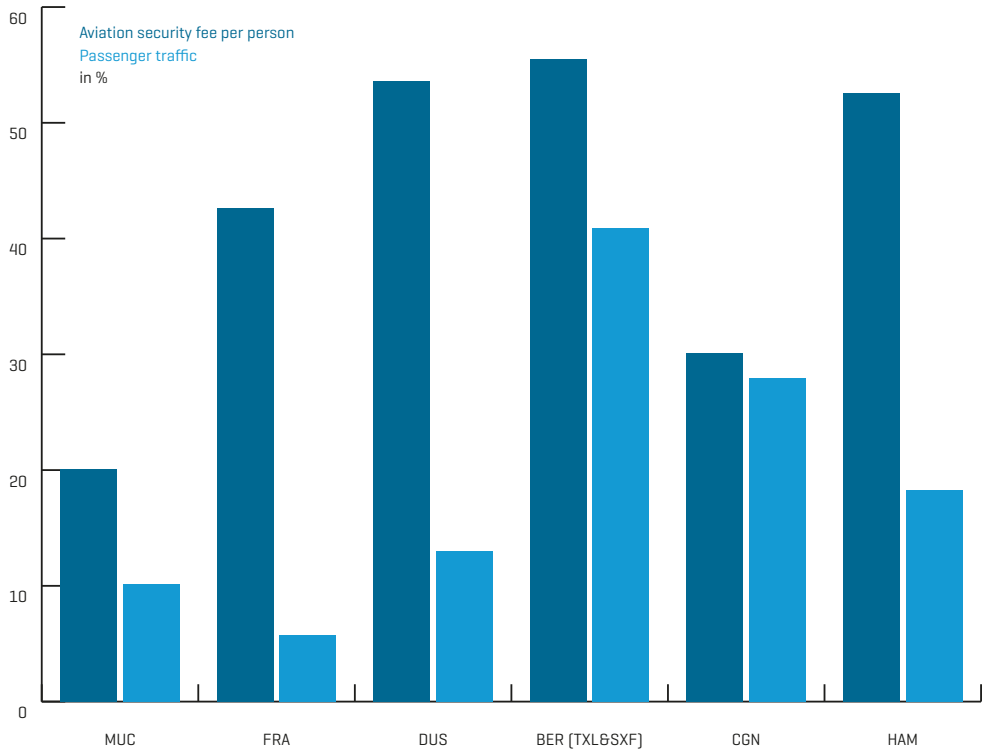
Much is regulated in aviation security, but are responsibilities correctly allocated?

The example of critical infrastructures shows how legal regulation pursues the right approach, but often leads to over-regulation for individual sectors by generally imposing requirements without further differentiation.

»Airports are generally considered »critical infrastructure«. But are they really? Based on different existing definitions, another conclusion can also be drawn.«

Alexander Borgschulze, Senior Vice President Corporate Security, Munich Airport; Chairman of the Executive Board, Bavarian Association for Security in the Economy (BVSW)

[23] **Growth Rates of Aviation Security Fees vs Passenger Traffic in Germany, 2012-2016**[76]



Looking at the regulatory framework, aviation security is designed in a cascade system. Due to its international scope, the regulations of the International Civil Aviation Organization (ICAO) are globally applicable. However, these regulations are not legally binding, as the ICAO is subject to international law, which is based on a system of consent-based governance. By joining the Chicago Convention, the Federal Republic of Germany has committed itself to applying the ICAO regulations. Within the European Union, uniform legal requirements for aviation security have been in place since 2002. Following the attacks of 11 September 2001, the EU was given the authority to define EU-wide basic standards. Since then, a large number of regulations and non-public decisions have been adopted which regulate aviation security in the EU. In Germany, national responsibilities for aviation security measures are laid down in the Aviation Security Act adopted in 2005 and amended in 2017. This national aviation security law is, in principle, based on three pillars: governmental responsibilities, security measures to be taken by airport operators and measures to be taken by air carriers.

Taking a closer look at authorities entrusted with responsibilities related to aviation security in Germany, it becomes clear that a multitude of appropriate authorities is tasked with the job. At federal level, the Federal Ministry of the Interior (BMI) and the Federal Ministry of Transport and Digital Infrastructure (BMVI) enjoy the highest regulatory power concerning aviation security. However, the BMVI has delegated the execution of its supervisory duties to the Federal Aviation Office (LBA) as a subordinate authority. The LBA oversees the security responsibilities of air carriers as well as the certification of operators tasked with securing the supply chain for airfreight and in-flight supplies. Federal aviation authorities, on the other hand, supervise airports within the framework of the Federal Executive Administration. Including all subordinate authorities, the Federal Republic of Germany thus counts well over 20 appropriate aviation security authorities. This raises the question of efficient administration and uniform implementation of legal requirements.

The distribution of security tasks on the part of the industry must also be critically questioned. Can industrial operators, freight forwarders and hauliers really ensure that freight is securely transported to an airport and then onboard aircraft? Is it reasonable that individual airlines act as airport operators in certain airport areas while the airport operator has no influence whatsoever on the way or quality in which security measures are implemented in this area?

For this reason, the question of responsibilities and the distribution of tasks should be discussed in a constructive and

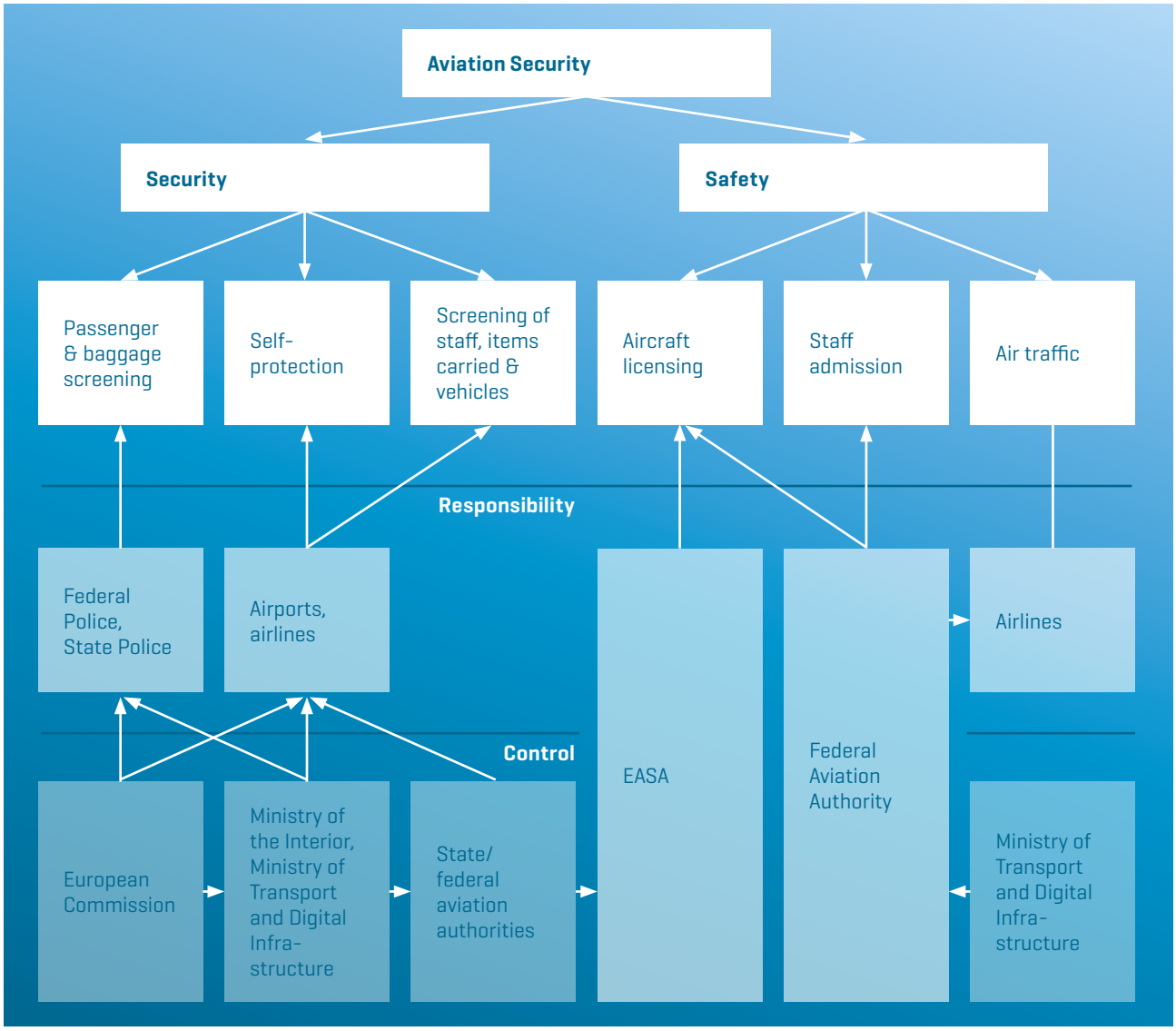
fruitful manner in the near future. Above all, this discussion must be guided by the spirit of high-quality security, since only if trust in aviation remains, it can perform its task successfully.

Are security and economic efficiency mutually exclusive?

An answer to the previously raised question is closely linked to the question of costs and debtors in the field of aviation security. Airports, like air carriers, compete. In contrast to air carriers, airports cannot change their location in difficult circumstances, but have to bear rising costs themselves, since these cannot be passed on to the customers. Air transport operators have so far borne these costs themselves or passed them on to the passengers. Because of the huge increase in security-related costs, the question is whether the state has to take responsibility, as the threat is not directed against aviation as such, but against it as a symbol of the free world and community of values.

The aviation industry is willing to continue making its contribution to security. However, measures should always be threat-oriented, constantly reviewed and, whenever possible, able to be withdrawn. Under these premises, security and profitability are not mutually exclusive, and a road to an effective and efficient security system in the aviation sector can be paved.

[24] **Aviation Security in Germany (Source: German Airline Association)**[77]



Optimising Security Screening Through Network Knowledge and Service

Dr Steffen Richter, Head of Section Aviation Security, German Federal Police[78]

BUNDESPOLIZEI

The trends in aviation and the challenges to safeguard its security could not be more conflicting. International air traffic is increasing despite framework conditions being less than conducive to aviation: economic impacts, noise reduction, night flight bans, distortion of competition by states, infrastructure limitations – and the very special threat to aviation.

Airbus' Global Market Forecast 2016–2035 predicts a growth of 4,5% p.a. for passenger traffic, meaning traffic will more than double in the next 20 years.[79]

Although the distance between Munich and New York will remain the same over the next 20 years, the concentrations of passengers - especially at the bigger hubs – will increase significantly and noticeably. Connecting time will increasingly become a key factor in the competition between airlines as well as between airports.

With regard to the continuing threat to aviation, this development will lead to many more passengers being screened in a shorter space of time.

But how? Back to the present.
»When two people quarrel, the third one rejoices.«

Parallels can be made between daily life and airport life when it comes to airports, airlines and aviation security authorities discussing the quality of passenger screening.

However, it is not simply a case of aviation security authorities, airport operators and air carriers discussing the quality of passenger screening. In recent years, it has been repeatedly confirmed that if only two of the three parties were to discuss the issue, it is quite clear to both who would be responsible in the event of a critical situation - the third. While each party can immediately name many reasons for something not working as it should and quickly provide suggestions for improvement, they each deal with a different area of responsibility, rarely their own. This can very quickly lead to arguments. These »selective dialogues« more or less guarantee that any future problems are, at best, successfully aired but not solved.

In order to achieve sustainable solutions, there is no alternative to an honest and constructive trilogue between the aviation security authority (including the service provider), airport operators and air carriers - at least none that would be good for Germany as an air transport location.

This is the only way to reconcile security, costs and service. Only with such a cooperative approach can weaknesses be identified and analysed, suggestions for solutions developed and tested and lasting improvements in the screening process achieved. Of course security is paramount. This is the legal order. This is what travellers expect. Air transport lives on trust in its security. If travellers have no trust, they will not board an aircraft.

Germany is being targeted by Islamic terrorism. The seven attacks in 2016 are tragic evidence of this. The situation includes a specific and immediate threat to civil aviation: Berlin Breitscheidplatz is just seven kilometres from Tegel Airport, which was spotted by the terrorist al-Bakr as a possible target.

»Security is therefore not an end in itself, but an essential prerequisite for successful commercial aviation. Again, if passengers have doubts about their safety, they will not fly.«

However, recognising this priority must not lead to the authorities losing sight of the cost and service aspect. German aviation security authorities are not exempt from the obligation to provide economical financial management. All expenditures for passenger screening are initially to be paid by the federal or state governments. The aviation security fee is only used to refinance these tasks. Airports and airlines get transparent insight into the planning and spending of these expenses.

The majority of expenses for passenger security checks are incurred by the control staff. The aviation security authorities and their security companies can only deploy these personnel efficiently if solid data are available for effective and flexible deployment planning. The flight schedule dictates demand. However, the flight schedule is not based on uniform and economic staff utilisation but on the available slots for arrivals and departures. The desire of air carriers to provide global connections with short transit times has resulted in a complex, complicated and therefore fragile system that requires efficiency and process consistency among all parties

involved. In this respect, aviation security is made for aviation.

Aviation security also provides a service to the traveller. Long queues and the unfriendly presence of screening staff do not contribute to a relaxed atmosphere at the checkpoints. This is not the way to enhance performance. Rigorous screening can still be carried out in a friendly manner.

The security authorities therefore have good reason to continually check their own screening processes and to implement recognised improvement potentials. However, there should also be a consensus amongst all parties that no side will optimise its processes unilaterally at the expense of another site. Thus, it is not easy to demand faster checks for passengers and hand luggage while passengers are almost forced to take more luggage into the aircraft cabin. More hand luggage will inevitably result in more baggage being screened at the passenger checkpoints. This takes a while.

Due to time constraints, many passengers simply cannot afford to wait long for their checked baggage at their destination airport so try to cram the essentials into their hand luggage and take them on board: clothes, cosmetics, laptop etc. All this also has to be screened in accordance with the now required additional checks by means of explosive trace detection technology. This takes a while.

The need for action is obvious – both now and in the future – as forecasts for air transport indicate. Projected world growth will lead to more and more passengers being screened in even shorter periods.

How can aviation security authorities and their service providers, airport operators and airlines be better prepared for these developments?

The Federal Ministry of the Interior and the German Air Transport Association have agreed on a joint project: »Process optimisation of passenger and screening procedures«. The Federal Police is also committed to this project, working together with its service providers, airport operators and airlines to optimise passenger guidance prior to screening and security screening procedures. Out of 589 ideas, 43 fields of action were identified that are directly related to one another. Three subprojects with different areas of focus were initiated at the airports of Cologne / Bonn, Hamburg and Berlin-Schönefeld.

On the 9th Aviation Security Day, representatives of the Federal Police and aviation industry presented all three subprojects. At Hamburg Airport, the lines of communication between the parties were examined in detail in order to improve the allocation of screening staff. Where and when are which data available? How can these data be used to place personnel from the contracted company I-Sec? Only a few people decide to travel by air spontaneously. The airline a traveller has booked knows hours, days, weeks before, when they will fly. This information can be used for personnel planning in a much better way.

In Berlin-Schönefeld, Federal Police, Securitas and the airport operator have developed ways in which to simplify and speed up the planning process. Far too many officers are being tied up with these tasks by the Federal Police. In addition, the prerequisites for a new billing model are being tested. What incentives can be created for efficient staff deployment if the security company is not remunerated per screening hour, but for every check that has been carried out?

Both subprojects deal with planning and guidance before actual passenger screening. Cologne / Bonn Airport has provided a large area in Terminal 1 to develop a new type of passenger screening lounge. Here, too, the Federal Police and the commissioned company Kötter, airport operators and airlines as well as the company Scarabee, which is responsible for the design of many control points at European airports, work closely together. The Airport Innovation Lab of the Potsdam Hasso Plattner Institute also lends its support. All substeps of the passenger and baggage screening process were analysed, and ideas were developed, rejected and rethought. The screening assistants themselves had the most important role. Their experiences as well as their desires and expectations for an optimal workplace, were immediately taken into account, and their active participation encouraged. This provided the basis for building a model of cardboard boxes. In this way, the basic essentials of a passenger screening centre (preparation areas for the hand luggage, X-ray machine, workstations for monitor evaluation, manual follow-up and checks of footwear, security scanner, explosive trace detection systems) were flexibly configured. The configuration is based on the principle of »form follows function«. Which subprocesses must be changed in which manner? Are the distances and the height of the elements more comfortable to work with? After many changes a wooden model was built. This gave a clearer idea of the future workplace. The next step was to refine the subprocesses.

On 15 November 2016, the CEO of Cologne / Bonn Airport, top management of the aviation industry, the security industry and the Federal Police presented the new »EasySecurity« passenger screening centre to the public. »EasySecurity« is the way forward for passenger screening in Germany. Now it is important to thoroughly test how these expectations can be fulfilled. The feedback from passengers and the screening staff is very positive. The configuration and relaxing atmosphere allow it to be called a screening lounge. But we are still at the beginning. Screening assistants have to master the sophisticated new processes, and new elements and technology have to function reliably to demonstrate the performance of this new screening solution.

/Selected Pilot Projects

In the following pages, the M-Sec Report presents three pilot projects that have already been executed recently or are in the actual testing phase right now. All of these projects aim to improve security processes and procedures at airports on different levels.

FLYSEC is a research and innovation project that aims to develop an end-to-end security screening process. »Easy Security« has already been established at airports and improves security screening, while explosives trace detection (ETD) sets new standards for explosives detection procedures.

Process Optimization of Passenger Control Management and Security Control

Robert Viertel, Head of BDL Security Project, German Aviation Association (BDL)

BDL
Bundesverband der Deutschen Luftverkehrswirtschaft

In the context of a joint approach by the German Ministry of the Interior and the German Aviation Association and following productive discussions, both project partners have decided to sponsor and launch a unique project involving stakeholders from the authorities and the industry.

The purpose of this project is to ensure an ultimate and efficient level of security by identifying potential for process optimisation and the evaluation of future technology and automation. To achieve a best practice recommendation, a cooperation on behalf of all stakeholders is required for a comprehensive process review, starting from a passenger's booking through to boarding.

Participants from the Ministry of the Interior, the Federal Police, the airports Berlin, Cologne / Bonn, Düsseldorf, Frankfurt, Hamburg, Munich and Stuttgart, as well as from the airlines Lufthansa, Condor and Eurowings and the associations ADV, BDF, BDL and IATA, contributed to the initial project phase. After conducting various workshops and comprehensive analysis, almost 600 ideas were raised and consolidated into 43 areas of possible improvements. The results clearly identified significant interdependencies between stakeholder processes. Transparency and trust appear to be the key success factors in this project. The adopted collaborative approach is second to none in terms of achieving improvements.

During a subsequent presentation of the results and a discussion involving the management boards of both project sponsors, a subset of the identified ideas was selected for the launching of three pilot projects at the airports Hamburg, Berlin-Schönefeld and Cologne / Bonn.

Hamburg

At Hamburg Airport, the focus of the pilot project was on the planning and management of passenger flow, as well as the planning of manpower, stakeholder communications and selected activities at the checkpoint. With the support of an

Easy Security – Benefits for Passengers

- Spacious environment
- Passenger needs are focused
- Flow principle – bypassing of co-travelers if they require more time
- Appealing environment – modern, bright, overview

Easy Security – Benefits for Staff

- Workspace environment
- Stowage area for personal belongings
- Optimised workflows and processes
- Appealing environment – reduced noise, enhanced overview, more relaxed passengers

IT solution developed in-house for passenger forecast, the required data is collected from the airlines, the airport and the Federal Police. Joint access and a common event calendar support this activity, along with dedicated training activities. With a jointly developed and approved reporting system, including key performance indicators, it is used to support various levels of onsite communication – from the day-to-day operations up to management level and vice versa, thus ensuring consistent information. Furthermore, selected trials at the checkpoint with the support of the security service provider have been performed, such as, for example, the use of different tray sizes, traffic light systems, lining managers or single hand luggage lanes.

Berlin-Schönefeld

The pilot project at Berlin-Schönefeld focuses on the contractual cooperation between the Federal Police and the security service provider. In a simulated environment, the remuneration method »payment per performed passenger security check« is under evaluation. For this purpose, an additional amendment - including a service level agreement with a bonus-malus system - to the existing contract was signed. For the implementation of the trial scope, full responsibility for the manpower planning process is assigned to the security service provider, whereas the Federal Police focuses on its core responsibilities. To enhance the efficiency of planning and communication processes, the airlines agreed to supply more comprehensive data and a joint security report, including KPIs. This consolidated information contributes to an open and trustful discussion amongst all stakeholders.

Cologne / Bonn

The purpose of this pilot project at the Cologne / Bonn Airport is to focus on the preparation area and the security checkpoint. Inside Terminal 1, the airport provided a dedicated area for the physical implementation of a joint, newly designed security checkpoint environment. With the support of a company with dedicated process knowledge and integration capabilities, all stakeholders jointly developed this new layout in various workshops, while focusing on many aspects such as workflows, process optimisations, procedures, ergonomics and technology. Due to the importance of the assignment, representatives of the security service provider actively and intensively participated in creating their own future working environment based on their requirements and expectations. The first step involved designing a checkpoint layout with cardboard boxes, as an initial test of the developed process enhancements and procedures. Subsequently, a wooden mock-up was assembled to assess the results, including a stress test involving a large group of colleagues, based on actual collected passenger data from Cologne / Bonn airport.

Thus, having convinced all stakeholders, project partners and finally the sponsors, the decision was taken and approval was given to build and implement this new environment in Terminal 1.

The newly designed preparation area for passengers, the state-of-the-art technology of the security scanners and baggage screening X-rays, as well as the separate centralised image processing, separate secondary search opportunities, spacious baggage reclaim area for passengers and a dedicated recheck area enhance the effectiveness and efficiency of a modern design with the available state-of-the-art technology.

With the support and expertise of the Airport Innovation Lab, the new concept was presented to the colleagues of the security service provider and training and redesign activities were launched. The trial of the pilot project is still ongoing and the initial results are quite promising.

Easy Security

Innovation Project: FLYSEC

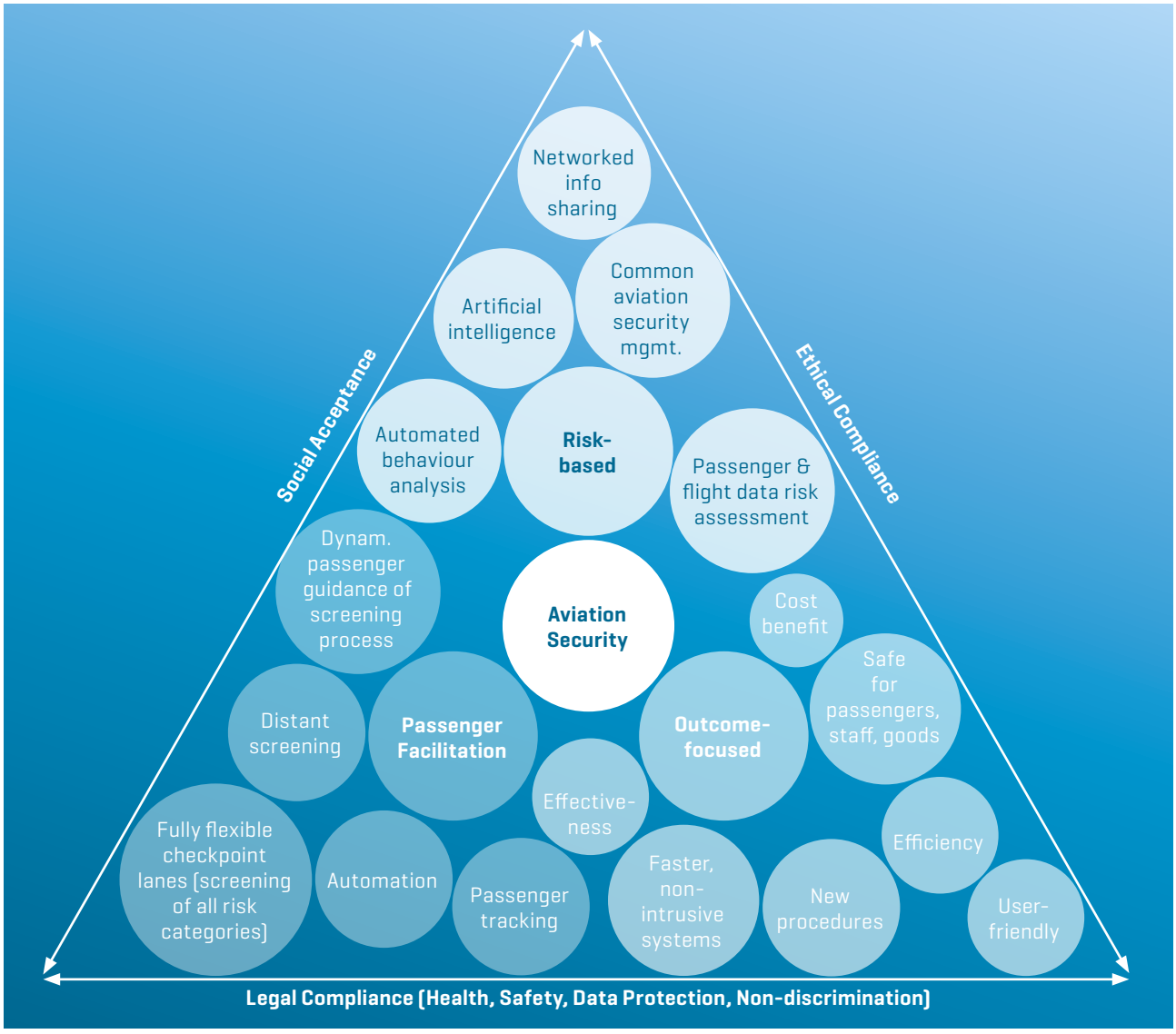
FLYSEC is an ambitious research and innovation project that aims to develop and demonstrate an innovative, integrated, end-to-end airport security process for passengers, airports and airlines.[80]

FLYSEC's primary goal is to enable a guided and streamlined procedure from landside to airside and into the boarding gates while offering an operationally validated innovative concept for end-to-end aviation security. The project will gather excellence and expertise from industry, SMEs, research and academia, including stakeholders and end-users such as major airport operators.

FLYSEC's ambition is based on a well-structured work plan that includes:

- Innovative processes facilitating risk-based screening
- Deployment and integration of new technologies and repurposing of existing solutions towards a risk-based

[25] **FLYSEC Overall Security Concept (Provided by FLYSEC Consortium)**[81]



security paradigm shift

- Improvement of passenger facilitation and customer service, bringing security as a real service in the airport of tomorrow

- Achieving measurable throughput improvement and a whole new level of quality of service.

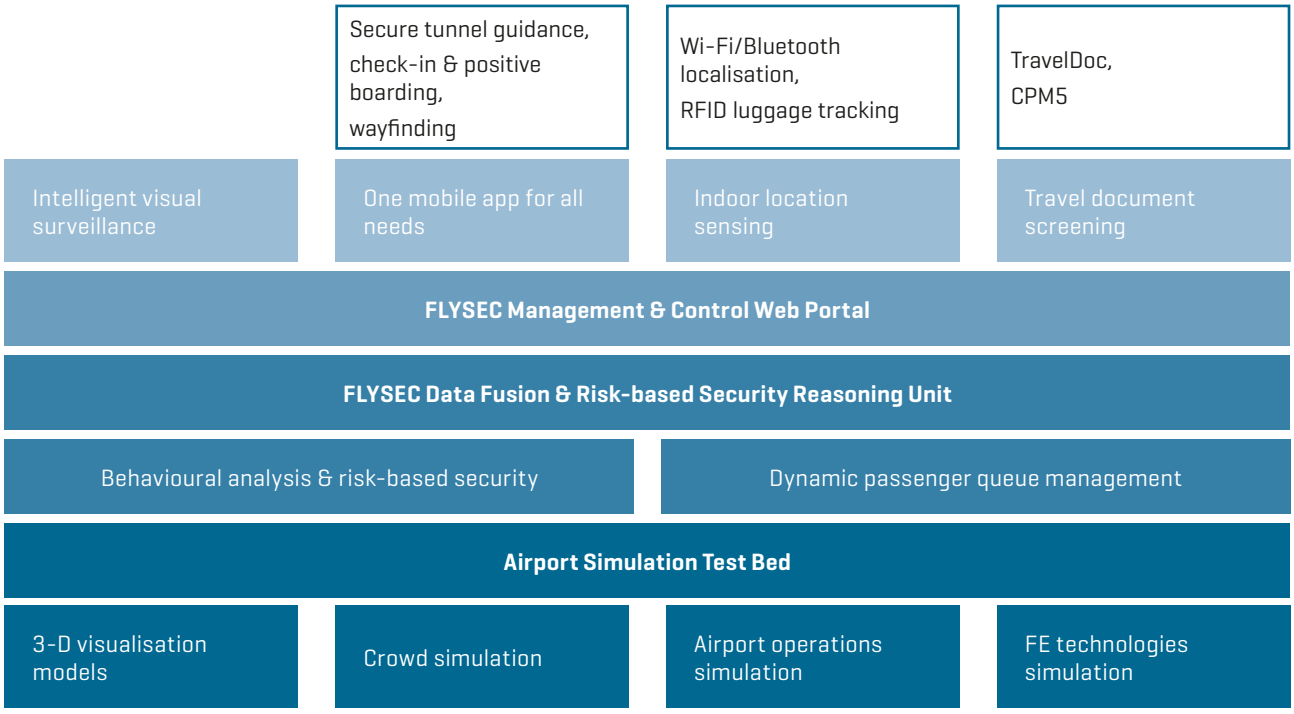
On the technical side, FLYSEC achieves its ambitious goals by integrating new technologies on video surveillance, intelligent remote image processing and biometrics combined with big data analysis, open-source intelligence and crowdsourcing. Repurposing existing technologies is also one of FLYSEC's objectives, such as mobile application technologies for improved passenger experience and positive boarding applications (i.e. services to facilitate boarding and landside/airside wayfinding) as well as RFID for carry-on luggage tracking and quick unattended luggage handling.

FLYSEC aims to implement a seamless risk-based security process combining the aforementioned technologies with behavioural analysis and innovative cognitive algorithms. A key aspect in the design of FLYSEC risk-based security is applying ethical-by-design patterns, maximising the efficiency of security controls through passenger differentiation ranging from »unknown« to »trusted«, while remaining ethical and fair in the process. Policy, regulatory and standardisation aspects will also be examined in the context of the FLYSEC innovative security concept.

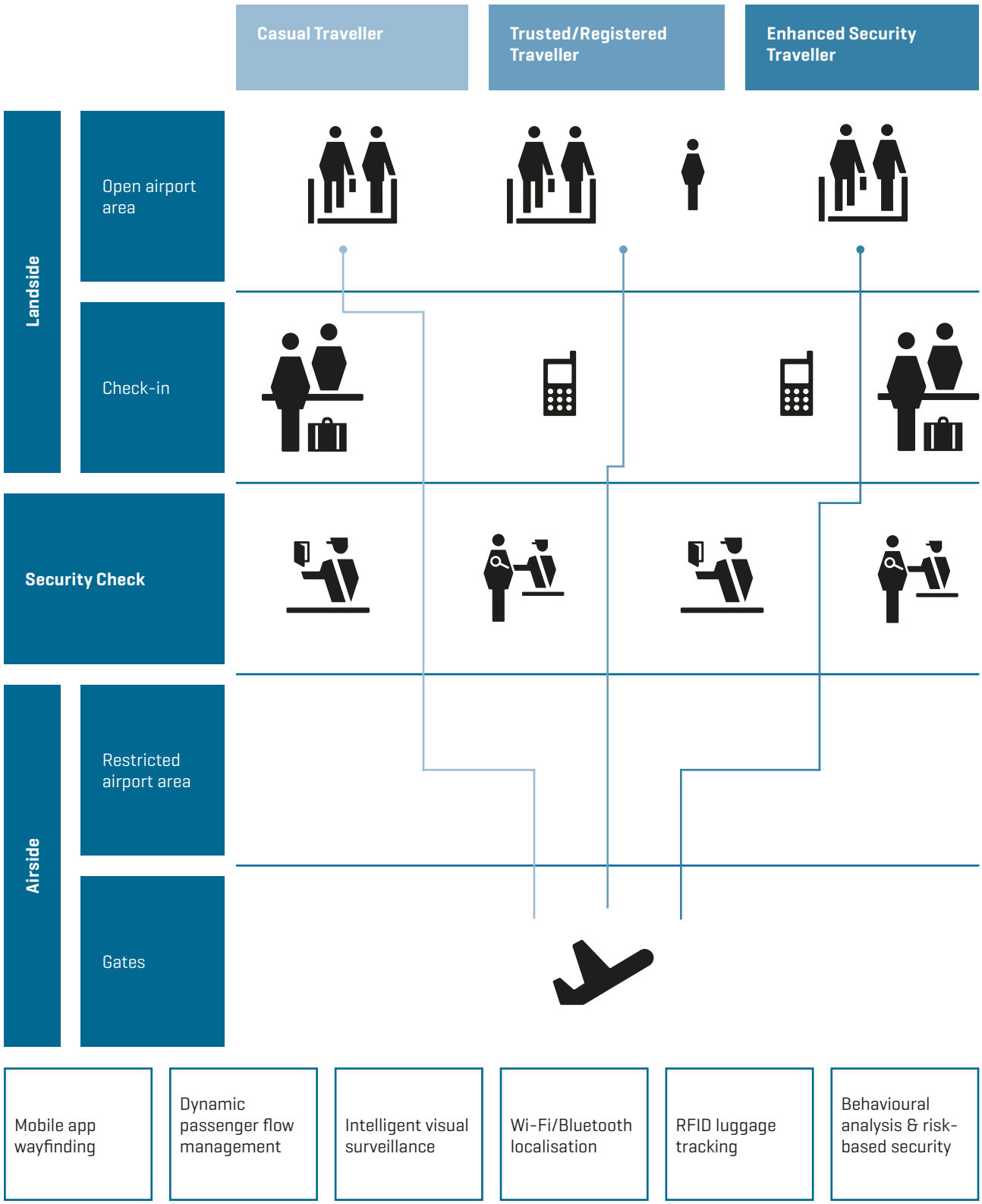
FLYSEC involves technologies from different technology readiness levels (TRL), including in-project prototype development, as well as the adaptation and extension of more mature solutions or the repurposing of commercial products. FLYSEC will validate the operational value of the solution provided through pilot testing in real operational environment.

In February 2017, all technical components, subsystems and software modules of the FLYSEC partners were set up and integrated for Proof-of-Concept (PoC) testing south of Berlin at Schönhagen Airport. The tests were monitored by the European Commission, DG Migration and Home Affairs, the German Federal Police and invited stakeholders from the aviation and security sector. All tests were performed in close coordination with the responsible Officer for Data Protection and Privacy and an Ethics Committee. Subsequent to an ongoing analysis of the PoC results, further testing at Luxembourg Airport has been scheduled for the coming months.

(26) **FLYSEC System Architecture (Provided by FLYSEC Consortium)**[82]



[27] **FLYSEC Scheme (Provided by FLYSEC Consortium)**[83]



Performance Testing of Security Screening Equipment

Dan Chirondojan, Director Space, Security and Migration, European Commission Joint Research Centre

The European Commission's in-house science service, the Joint Research Centre (JRC), draws on over 50 years of scientific experience, but is a relative newcomer to the world of aviation security. One of JRC's tasks is to research and develop test kits and quality control materials which help authorities verify that screening equipment continues to perform satisfactorily during its operational lifetime. Dan Chirondojan, Director »Space, Security and Migration« explains to M-SEC what JRC is working on and why, and shares his plans for future developments in this area.

Security screening equipment plays a crucial frontline role in providing security for air passengers and also represents a significant investment for airports. For this reason, screening equipment is subject to rigorous laboratory testing before being approved by EU member states for operational use.

Once installed in airports, however, it can be challenging to verify that equipment continues to deliver its peak performance over the duration of its operational lifetime. One reason is the impracticality of testing detection equipment with real explosives. However, there are other challenges (i.e. technical, modelling), not to mention time restrictions and the need to minimise disruption to operations.

Nevertheless, as screening becomes more technologically advanced and investments in security evolve, there is growing interest in enhancing the capability to verify the performance of screening equipment insitu.

From the airports' point of view, there is a natural interest in checking the performance of equipment upon delivery (site acceptance testing), but also in implementing smart »routine testing« which can help to protect investments, optimise maintenance schedules, prevent downtime and minimise costs.

From the regulators' point of view, there is a natural interest in confirming that equipment continues to operate in compliance with regulatory performance standards, and in ensuring that passengers continue to benefit from the security measures in place.

In terms of legislation, the European Commission established common rules in the field of civil aviation security aimed at protecting persons and goods from unlawful interference with civil aircraft (Regulation EC No 300/2008)[84]. The Commission's policy services have steered this legislation over the years in consultation with member states, airports, equipment manufacturers and international partners.

The Commission also has the legal mandate to carry out inspections in the field of aviation security, under Regulation (EU) No 72/2010[85]. A team of inspectors from specific services of the Commission verify the effectiveness of national quality control programmes.

The introduction of explosive trace detection (ETD) equipment in European airports as of September 2015 meant that this new category of equipment was included in the scope of inspections. JRC had started activities in security screening equipment and was a natural partner to develop tests for ETD equipment. A key requirement was that the test kit was small, rugged and suitable for field use.

JRC provided a test kit, testing protocol and training to the Commission inspectors in a timely manner, so that they were able to include ETD equipment during their first inspections following the September 2015 deadline. The test kit enables the inspectors to identify, with the necessary confidence and scientific robustness, when a piece of ETD equipment is not performing satisfactorily. Several national authorities have expressed an interest in receiving the test kit.

For trace detection, the amounts involved are very low, however for equipment designed to detect large or bulk quantities of explosives (i.e. X-ray baggage screening), the use of »the real thing« is not feasible. In this case, explosive simulants are required. JRC is currently working on a project to develop bulk explosive simulants for X-ray equipment with the necessary quality assurance to be used for field testing of explosive detection systems (EDS) in EU airports.

Not all of JRC's efforts are focused on field testing, however. Behind the scenes, JRC is also providing materials to the test centres of the European Civil Aviation Conference (ECAC), which are performing laboratory-based type testing of aviation security equipment before it is approved for use.

Always looking to minimise potential sources of variability in testing, JRC has provided a common set of benign substances to ECAC for use in determining the false alarm

JRC's test kit for explosive trace detection (ETD) equipment enables security practitioners to verify, with the necessary confidence, that the equipment continues to perform satisfactorily during its operational lifetime.

rate of ETD equipment. This test kit will be followed by a set of standardised surface materials for swabbing, to further harmonise testing of ETD equipment in Europe.

The JRC is also supporting the Commission's proposal (and future implementation) for a regulation establishing a Union certification system for aviation security equipment (COM-2016-491)[86]. This proposal aims at harmonising at European level the certification of aviation security equipment to contribute to the proper functioning of the EU internal market and at increasing the global competitiveness of the EU industry.

Looking to the future, we foresee an opportunity and a need to take some of the knowledge and experience gained in aviation security and apply it, where appropriate, to other applications, e.g. other transport modes and soft targets. This is particularly relevant for detection technology, since there are almost no common performance standards, test methods or test materials outside aviation.

For example, there are numerous handheld devices on the market that detect explosives and other chemicals of interest. This equipment is intended for multiple user communities, including police, first responders and customs officers. JRC produced a test kit for evaluating the performance of handheld detection equipment used by customs officers.

Aviation security is likely to remain a heightened priority for the foreseeable future, and Europe has to strive to maintain vigilance and the appropriate balance between security and facilitation. A more competitive EU security industry will be able to offer technological solutions which will actively increase the security of European citizens and will contribute to the capacity of the European society to prevent and respond to security threats.

JRC, which is independent from national and commercial interests, is looking forward to making its contribution to this important, collaborative and long-term effort.

/A Hovering Threat from Above? Risks and Advantages of UAVs

Norbert Barthle
Parliamentary State Secretary, Federal Ministry of Transport and Digital Infrastructure, Federal Republic of Germany

Federal Ministry of Transport and Digital Infrastructure

Unmanned flight is fascinating. Today, it is already possible to fly aircraft largely independently of typical air transport infrastructure. Drones can be a useful advance beyond basic transport operations, with a large number of applications, for instance in emergency management or infrastructure protection. This is a great opportunity for national and international aviation. At the same time, however, the operation of drones also raises serious questions as to their operational safety and security.

If we want to exploit the opportunities presented by unmanned aviation, we have to make the basic rules for the lower airspace fit for purpose and – where necessary – add new approaches.

Acting on recent developments in the sphere of drones, we in Germany have established a major regulatory framework for the field of safety by issuing the »Regulations Governing the Operation of Unmanned Aircraft«[89].

These include rules designed to prevent collisions with other airspace users and to protect innocent third parties on the ground. Other assets protected by the new regulations are privacy, nature conservation and, of course, security, i.e. averting threats to public safety and order. In the future, the operation of unmanned aircraft in airspace over gatherings of people, technical installations, airports and land used by security authorities, the armed forces or embassies will be subject to dedicated rules and, ultimately, also prohibitions. For us, there is no doubt that drones will, in the future, play an important role for authorities and organisations with security and safety tasks. Here, too, we have established initial rules. These are all major steps towards integrating unmanned aerial systems into the airspace.

»Even though we are already approaching regulation of this new form of airspace use, there are still some outstanding issues, and we are currently working to resolve them.«

For example, drones represent a not insignificant security problem. In the field of manned aviation, everything has to be done to prevent aircraft from being misused for criminal or terrorist purposes, and the same is true of unmanned aviation. Here, too, there is a diverse risk landscape. From a cybersecurity perspective, risks are literally already »programmed« into these systems. Jamming can interfere with drones and cause them to crash. Or they are used as vehicles to move jamming devices or spoofing technology, for instance for espionage purposes, to places that are otherwise difficult to access. For white-collar criminals, drones certainly have interesting – although from a social perspective negative – potential. And with the low-threshold access to this technology plus increasingly high payloads, the use of drones in conjunction with explosive devices and the like is becoming a scenario that definitely has to be taken seriously.

Drones thus present both an opportunity and a challenge – although the opportunities predominate. It is imperative that use of the lower airspace be future-proofed. We must make it mandatory for safety and security procedures to be integrated into the development and manufacturing processes of drones. Training, skills development, licensing, electronic registration procedures and authorisation

»Drones have huge potential – in private as well as in commercial use. More and more people are using them. However, the more drones in the air, the greater the threat of collision, crash or accident. Clear rules must therefore be established for the use of drones.«

Alexander Dobrindt, Federal Minister of Transport and Digital Infrastructure, Federal Republic of Germany[87]

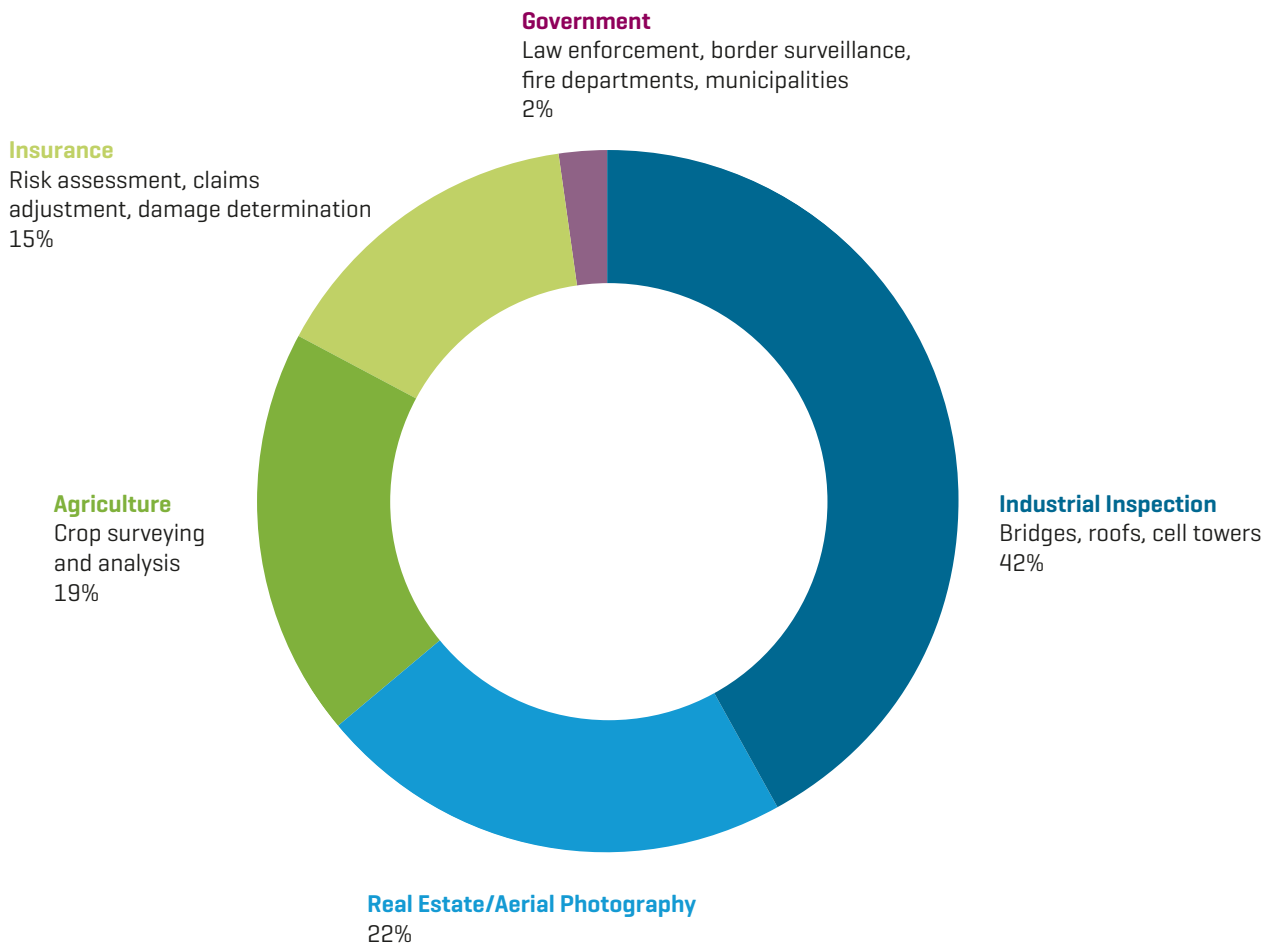
»Unmanned Aerial Vehicles, commonly called drones, represent a considerable threat to humans and to infrastructure.«

Prof Dr Pascale Ehrenfreund, Chairwoman of the Board of Management, German Aerospace Center (DLR)[88]

systems, clear European and international rules and performance requirements for visual line of sight (VLOS) and beyond visual line of sight (BVLOS) operations will help make the flying of drones safer and more secure.

Technological access barriers and preventive safety measures can reduce the risks associated with misuse, but they cannot rule them out. Here, risk-based analyses are needed, such as those that are already established in manned aviation, in order to identify possible attack vectors and develop appropriate countermeasures.

(28) **UAV Usage, 2016 (Provided by Allianz)**[90]



/UAVs: Innovative Potential, but at Risk of Illegal Misuse

Jan Syré, Chairman, German Federal Association for Unmanned Systems

The aviation sector is becoming a forerunner when it comes to utilising unmanned systems. According to BUVUS, the Federal Association for Unmanned Systems, this growing market therefore needs to develop innovatively and liberally.

More than 6,000 companies covering the whole range of drones are currently active on the German market. They do not only develop and produce systems and vehicles for air, water and land, but also cover their professional application. And this is where the sector is just starting to discover its manifold opportunities. It has already become common practice to use footage shot from drones for movies. Other fields are currently catching up, using and processing data from drone flyovers. For example, real estate agents are making use of the advantages of drones by using aerial photos of buildings or surveying building plots. Moreover, inspections can be carried out quickly and thoroughly, be it of high buildings like church towers or industrial chimneys, or agricultural land and forests. And the number of new application areas is expected to rise in the near future.

However, the commercial use of drones is dependent on the necessary permits being issued by the relevant authority. The accompanying complexity becomes obvious upon examining the necessary training requirements: topics include air traffic law, airspace, meteorology, technology, as well as practical elements covering flying itself. Drone pilots need to prove their drone handling capabilities flying an obstacle course. Quick changes in directions and flying in a three-dimensional space are tested. This is what separates the wheat from the chaff. Commercial users hold the relevant permits and are fully insured. An increasing number of recreational drone pilots, however, are operating easily available, ready-to-fly drones without complying with legal requirements. It is this setting that bears the highest risk potential and where most breaches of law occur. What's more, the majority of recreational drone pilots are underinsured, which leads to further complications after an accident when the insurer is asked to pay for damages which are not listed in the insurance policy. In addition, there are issues regarding violations of privacy policy regulations when flying over private properties while taking pictures or making videos without authorisation.

It follows, from BUVUS' and all other industry associations'point of view, that there is a considerable need for the enforcement of laws and regulations.

Presently, commercial drone use is both regulated and monitored. Regulation of recreational use, on the other hand, has some catching up to do. An amended law which entered into force in April deals with this issue.

The distinction between a recreational and a commercial user is difficult to make. Not every commercial use is recognisable or definable as such. Is the uploading of videos to YouTube considered a private or commercial activity? Unfortunately, there is no straightforward answer to this. The more users watch the video, the higher the chance of earning money with it. The underlying motive would be hard or impossible to establish. Worth discussing is also the use of drones for research purposes. Some consider the flight for research purposes neither recreational nor commercial, even though research flights are considered »other purpose of use« in accordance with the German Air Traffic Act [§1 LuftVG [»sonstiger Nutzenzweck«] and would accordingly be treated as commercial flights as the provision stipulates.

Considering the amount of »critical infrastructures« the risk potential is high and potential hazards varied. It should be clear, even to the layman, that the operation of aircraft must be strictly regulated and limited to trained professionals at airports, train stations, power plants and industrial facilities, but also federal motorways, railway lines and waterways. Uncontrolled drones can cause serious accidents in airspace, such as collisions with aeroplanes and helicopters. Most aviation systems designed for human or cargo transport are equipped with »Automatic Dependant Surveillance-Broadcast [ADS-B] systems« in order to ensure a safe and controlled airspace. However, a recreational drone is normally not equipped with technology that transmits its position, nor is it reliant on clearance by an air traffic controller. This is neither stipulated in the current regulations nor are there any indications that this will become a requirement for recreational drone users in the future. Consequently, recreational drones are not identifiable in regular air traffic and cannot be detected by pilots in time to change course. Nevertheless, every day, recreational pilots operate drones without being aware of the risks or being grossly negligent and ignoring them. Thus, crossing the line into illegality is quickly done but can only be sanctioned if the relevant drone pilot and owner can be apprehended. Obviously, UAVs can also be used to deliberately commit criminal offences. To name but a few: the scouting of properties in order to prepare for break-ins, the dropping of weapons or drugs over the walls of

correctional facilities, and terrorist activities. Their relevance results from the current security situation in Germany and Europe. Terrorist organisations are using increasingly diverse means in order to harm the civilian population. Recent events in Germany have shown that terroristic attacks cannot be narrowed down to time or place and that the security situation has worsened as a whole. Being connected worldwide, people are able to get past classic security structures and move freely and undetected across borders. Recreational drones, with their weight-carrying capability improving continuously, can thus be a means for terrorists to prepare for and carry out attacks. Therefore, today's innovative development of the international market and the constant increase in sales of unregistered UAVs should be monitored closely. The newly amended law does prohibit all forms of interference or endangerment, the operation of drones in and above sensitive areas like police and rescue operational sites, crowds, main roads, take-off and landing zones at airports, as well as the operation of drones weighing more than 0.25 kg above residential estates. However, a labelling requirement applies only to UAVs weighing more than 0.25 kg. Unfortunately, since UAVs are becoming lighter and at the same time more professional, this opens up loopholes for criminals – above and beyond non-compliance with the law. In order to establish sensible and expedient defensive and countermeasures, an academic and political discourse is urgently needed.

/Four Major UAV Market Trends [91]

Large corporations will continuously take over successful specialist manufacturers or drone software providers to add to their own product range. For example, Autodesk has invested in Skycatch and 3-D Robotics; two rising drone specialists addressing the construction industry.

More and more **venture capital** is flowing into the industry, especially in the USA and China: in 2015, it amounted to half a billion dollars, according to analysts. No reliable numbers are available for 2016 yet, however they are expected to be higher. The largest manufacturer, DJI from China's high-tech region Shenzhen, was valued at $8 bn in the last round of financing.

Developments that could be observed in the IT industry are resurfacing: **hardware is getting better and cheaper** constantly. DJI used to be looked down upon as a toy manufacturer, but with each drone generation, they are continuously making their way towards the professional segment. Today's recreational 500-1,000-dollar drones often fly with greater stability and provide better image quality than a three-year-old professional model that cost $25,000.

At the same time, **operating systems are being standardised**, in part on an open source base. Building on this, software companies are being established that are developing data and specialty applications. Meanwhile, the first data collectors are entering the market. Similar to Google, they want to filter the valuable information out of the data stream that is being transmitted from the numerous networked drones to their servers. The data collected is to be used to make a close-up photograph of the world – in a much higher resolution than a satellite could ever deliver.

/Risks Associated with UAV Usage [92]

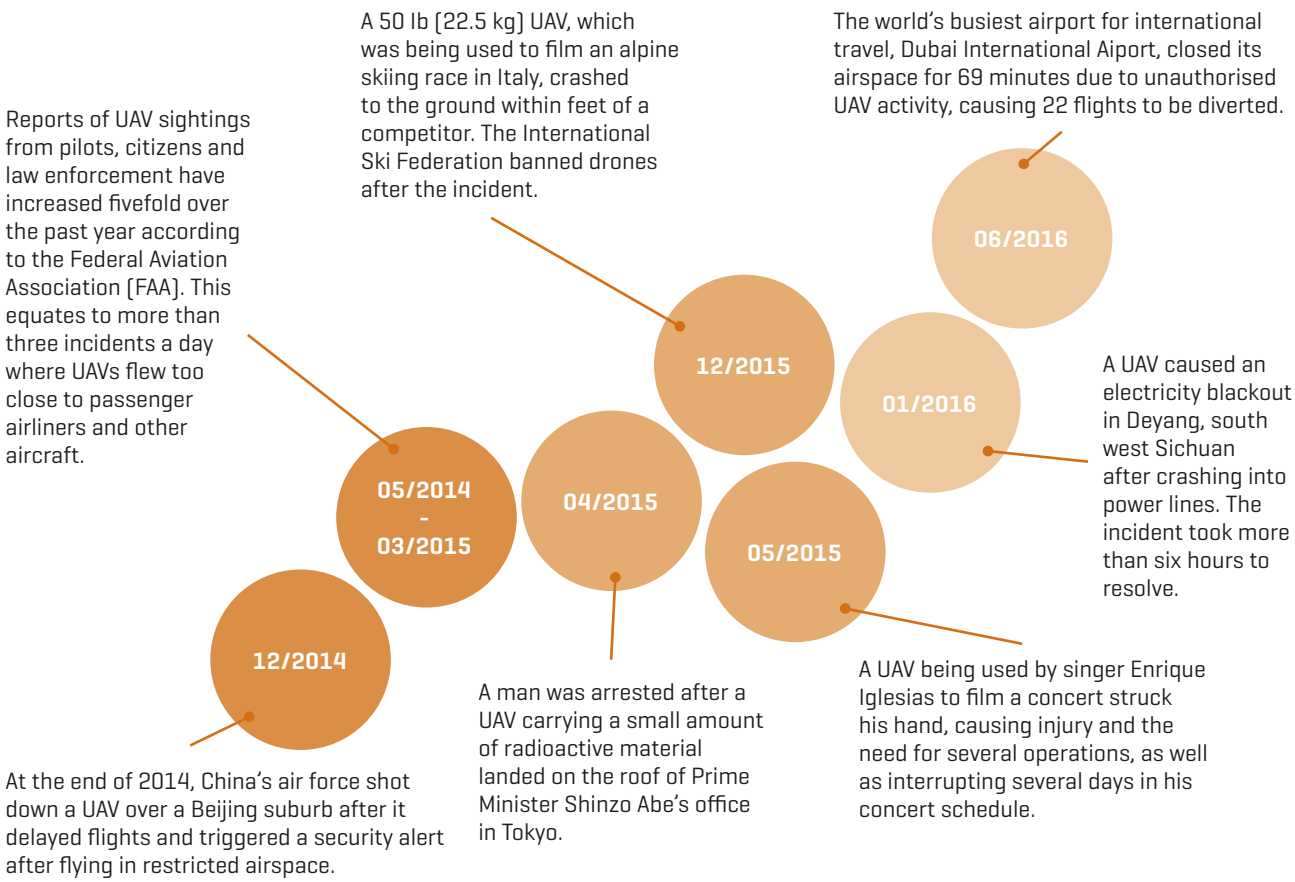
Liability risks
The liability risks associated with UAVs are completely different to those posed by manned aircraft, as there are no occupants on board, and the size and weight of the aircraft are usually significantly smaller. The worst case liability claim envisioned for UAVs is a collision with a manned aircraft.

War/terrorism perils
Such perils pose a high risk to UAV operations. Similarly to manned aircraft, they may be used for malicious acts. There are concerns that UAVs could be used to attack events where large crowds gather. One emerging peril is the potential terrorist threat of UAVs targeting power and nuclear stations. After more than a dozen overflights of reactors, French authorities announced the expenditure of $1.1 m to »detect, identify and neutralise small aerial drones« in 2014.

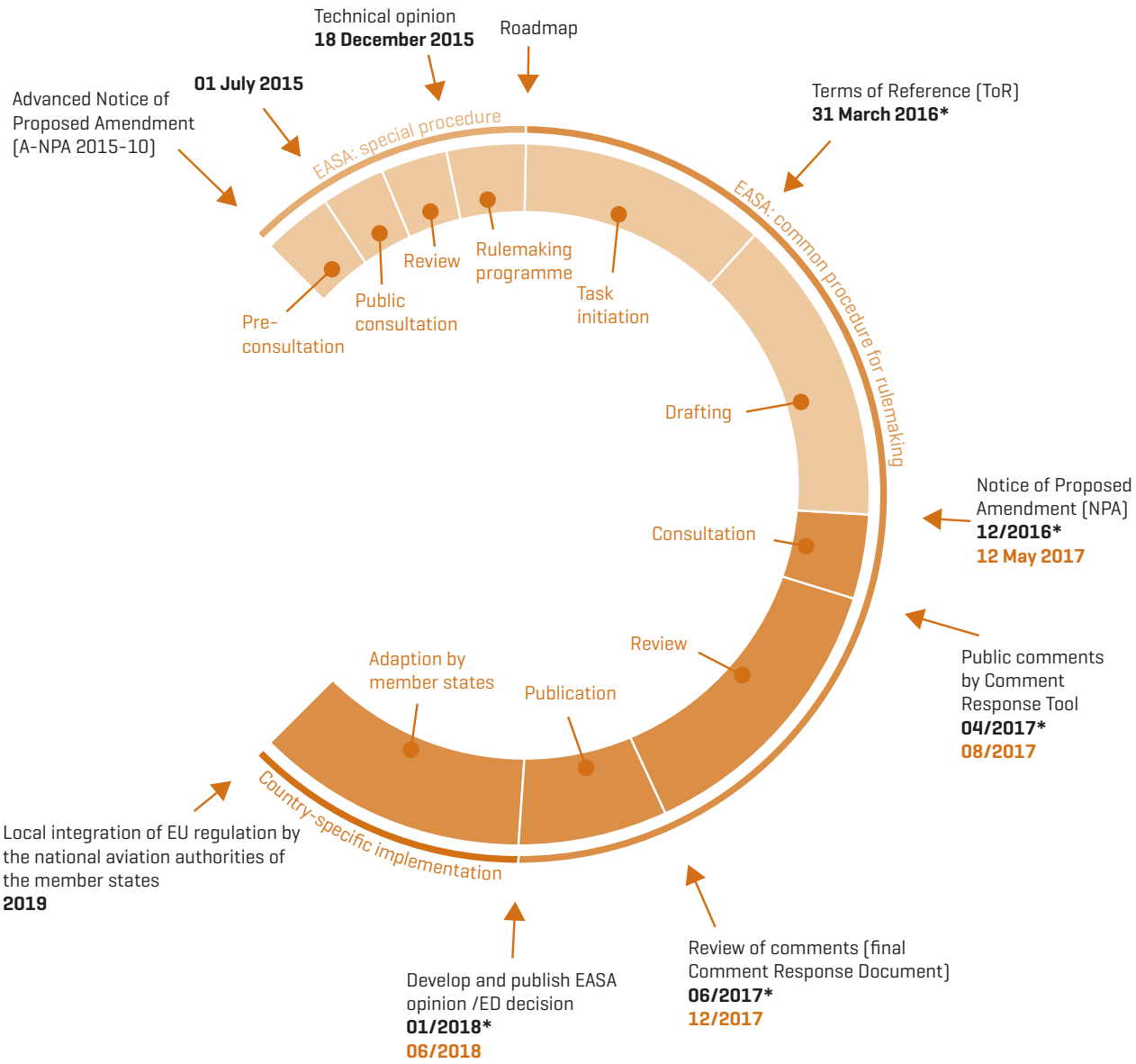
»Spoofing« or cyber attacks
Other scenarios include the prospect of hackers taking control during flight, causing a crash in the air or on the ground, resulting in material damage and loss of life. The term »spoofing« refers to attempts to take control of a UAV by hacking the radio signal and sending commands to the aircraft from another control station. This is a very real risk for UAVs since they are controlled by radio or Wi-Fi signals. Then there is the potential threat of loss or theft of data security. Valuable recorded data can be lost during the flight when the device is transmitting information to the control station.

Privacy issues
There are many public concerns over UAVs regarding issues such as privacy, trespassing and nuisance. In a recent case in Germany, a private UAV operator was served with a cease and desist order including a fine of $278,000 (€250,000) if he flew over his neighbour's estate again.

(29) **Selected Drone Incidents (Source: Allianz Global Corporate & Speciality)[93]**

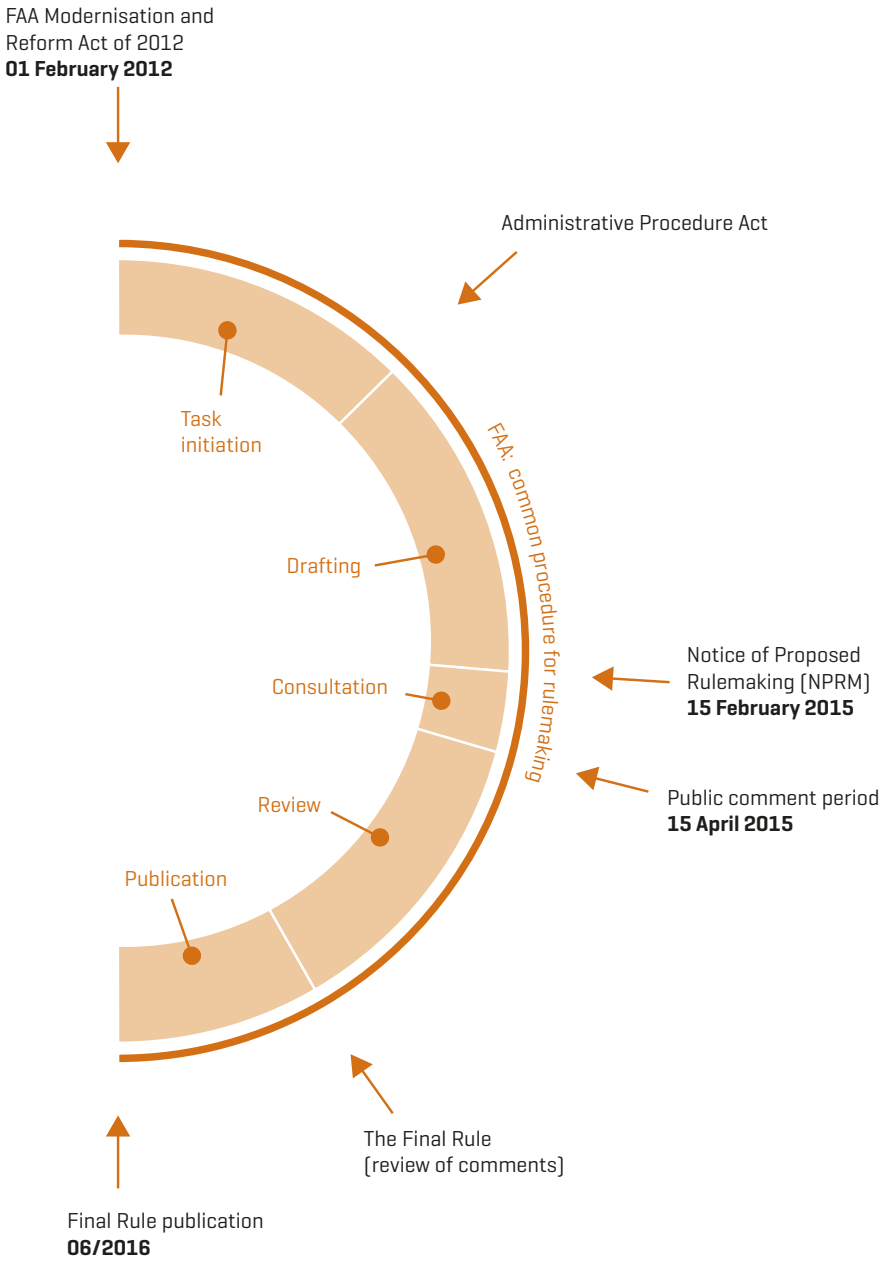


[30] **UAV Rulemaking Process in the EU (Provided by Drone Industry Insights)**[94]



*Initially planned date

[31] **UAV Rulemaking Process in the USA (Provided by Drone Industry Insights)**[94]



/Drones as a Means of Terrorism: Incalculable, Unpredictable Risks

Prof Dr Elmar Giemulla, Honorary Professor of Aviation Law, Berlin University of Technology

Are drones a blessing or a curse? Do they offer opportunities or do they pose risks and even threats to us all? The answer is simple: all technologies are both a blessing and a curse. We live in a technological world: we drive, we fly, we use nuclear power, we allow and even support technological developments – and certainly not because we like risks and threats. We make use of the undisputed advantages of technology. It makes our lives easier, or even more: it makes our lives possible.

It goes without saying that drones can effectively be used for security purposes, too, to monitor company grounds, including airports, to accompany the transport of sensitive goods, and to watch crowds - to name but a few.

On the other hand: useful and peaceful as technology may be, any technology can fail or potentially kill. Even worse, any technology can be misused: and we know that drones will be misused, too. So, the big challenge for the global regulators is: Will it be possible to accommodate this new technology at a »level of safety and security« acceptable to society?

As far as safety is concerned, it is fair to say that it is possible. Although rules and regulations are made for everyone, they are most effective on the willing part of the population, who want to know how to behave when using such technology. Rules and regulations also have an effect on the light-hearted, who must be taught how to behave by imposing fines and penalties. However, rules and regulations alone cannot prevent all criminals and terrorists from deliberately misusing drones. The ability to drop bombs and chemical, biological or nuclear substances is far too appealing. ISIS is already practicing single operations and even swarm attacks.

In order to establish an effective defence strategy, it is necessary to evaluate the characteristics of that »new dimension of threat«. What do traditional and unmanned aviation have in common and how do they differ when it comes to identifying potential criminal or terrorist misuse?

The most important common feature of both manned and unmanned aviation is the lack of physical borders in the skies, not just state borders but any kind of borders that serve to protect: critical infrastructure, sports arenas, inhabited areas etc. A plane cannot be searched before crossing such a critical border. What is more, a traditional plane does not need to carry and drop any bombs due to the fact that it is already carrying tons of kerosene on board, which can turn it into a flying bomb itself by being steered into the World Trade Center.

Consequently, the countermeasures taken since 9/11 are implemented at the airports where all planes start and they aim at preventing terrorists from entering a plane and taking dangerous goods on board. Society is protected by protecting aviation against misuse. However, as logical as such measures may be, they are completely inappropriate for preventing anybody from misusing a drone. Drones cannot be boarded, and their take-off sites are not airports but any verandah, backyard or other unsuspicious site which is not secured and which definitely cannot be secured.

Does this mean that we are utterly at the mercy of terrorists? Certainly not, but the parameters have changed. We must see that the strategy of protecting society by protecting aviation is ineffective when it comes to unmanned aviation. Since drones in the hands of terrorists form an immediate threat, »aviation protection« must be replaced by »aviation defence« (at least against this kind of aviation).

Generally speaking, »defence« means to fight a threat by eliminating it either at the origin or at the target. Technically, it is possible to fight a drone attack at a certain target - but only partly. Specialised developers offer the possibility of erecting a kind of »cheese domes« (drone shields or geofencing) around critical infrastructure or mass events, which prevents drones from flying into defined areas. However, the skies are high and such »cheese domes« do not prevent dangerous freight from being dropped from high above. Drone guns jam the data link between drone and operator. But what about autonomous operations? Technical solutions are urgently required, if they are to be made at all possible.

Perhaps it would be more effective to defend ourselves against the criminal use of drones at their origin: the criminal or at least suspicious purchaser or operator. A partial solution would certainly be to make drone registration obligatory and thus establish a formal connection between drone and operator. The obligation to disclose a criminal record when purchasing a drone should be considered, as well as other measures such as the obligation to declare an imported drone. A network

of measures must be discussed and analysed to make sure that only reliable persons are in the possession of a drone.

Experience has shown that terrorists generally don't buy the cars or lorries they drive into pedestrian zones – they steal them. A system must be established whereby each drone can be tracked from the moment of purchase, during operation and up until its disposal, and whereby each drone operator is obliged to notify the authorities of any loss.

While defending a target is important, it only protects those who are actually at the target. Recent tactics employed by terrorists have involved unsettling and confusing society by carrying out random attacks where least expected. Those caught up in such attacks need and deserve protection, making defence a necessity here, too. We therefore need to discuss how to prevent (potential) evildoers from purchasing and operating drones or at least how they can be prosecuted if they do so. We need transnational intelligence. The obvious objection that all these measures are useless because they can be circumvented cannot be accepted as it would equal the surrender to terrorism.

/Drone Detection and Countermeasures – The DLR Initiative

Prof Dr Pascale Ehrenfreund, Chairwoman of the Board of Management, German Aerospace Center (DLR)

Unmanned aerial systems (UAS), commonly called drones or UAVs, represent a considerable threat to humans and to infrastructure. Often civil drones are simply used for leisure activities and fun, but the potential usage within criminal acts and even possible terrorist attacks is increasingly being picked up on by the public and media. In particular multicopters like quadcopters are technically mature platforms that can be purchased and flown by virtually anyone. They have the capability to carry small payloads, with the most popular payload at the moment being an optical camera. This payload carrying ability has led to many valid applications for UAS. But what happens if it is not a camera mounted on a flying platform but a bomb, a gun or hazardous liquids in a sprayer? Less dramatic reasons for an undesirable UAS usage could be the transport of, for example narcotics across borders or into prisons, the illegal recording of sports or musical events and in general the violation of privacy.

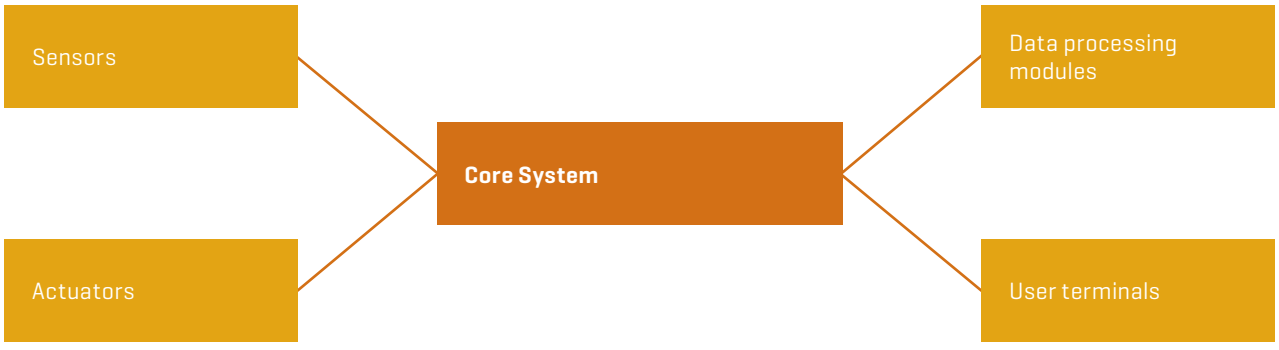
Also the threat drones poses to air traffic is a real and growing danger. The Federal Aviation Administration of the United States receives more than 100 reports of drone sightings in the vicinity of airports and aeroplanes each month. The resulting delays necessary to protect passengers can affect thousands of travellers and cost airlines millions of dollars.

An air surveillance system with the capability to detect unwanted UAS would not only come in handy in many scenarios. There is also an urgent need for such a system to support the work of the police, military and other security task forces.

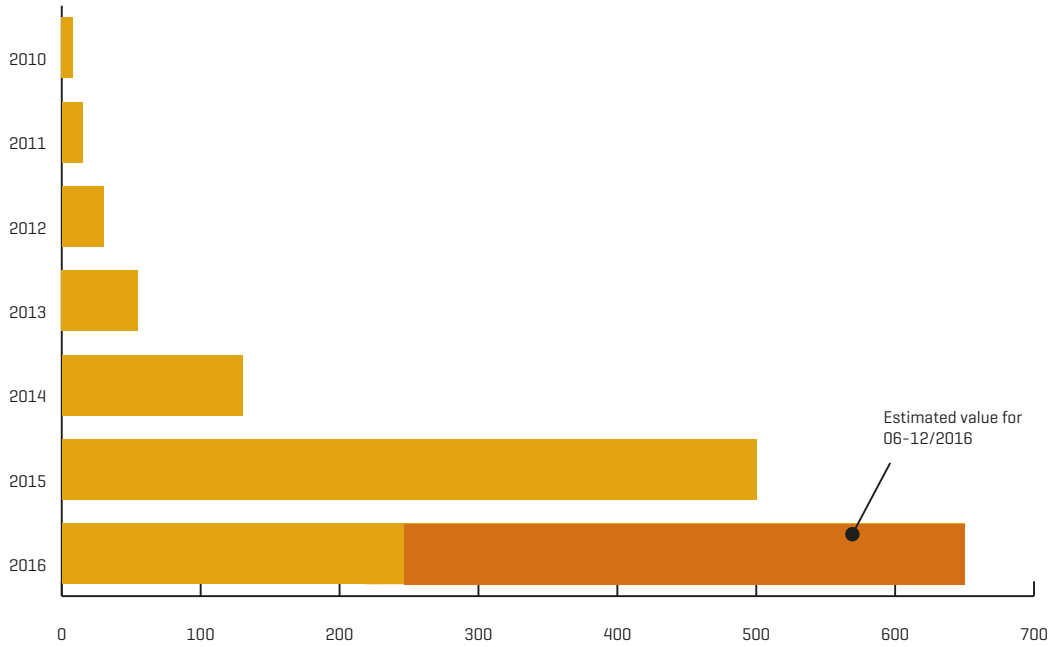
The German Aerospace Center (Deutsches Zentrum für Luft- und Raumfahrt e.V., DLR) is currently designing and developing such an air surveillance system. Specialists from three DLR institutes are collaborating on presenting a hardware demonstrator in the very near future. The required general characteristics of the surveillance system are real-time capability and high configurability in terms of sensors, actuators, data handling and user interface. As the system has to operate from different locations day by day, it has to fulfil certain mobility requirements. Although radar and laser specialists are contributing to the project, a flexible approach to the air surveillance system was chosen, focusing on solving problems instead of being solely technology-driven. The most suitable sensors are to be used and different sensors are to be fused to enable complementary information to be gathered.

Possible scenarios, e.g. for the police, could be to safeguard politicians and other VIPs in public or to protect crowds like visitors at events. In terms of critical objects and infrastructure, the task for an air surveillance system could be to supervise the airspace around an airport or a nuclear power plant. Different kinds of scenarios – in open fields or in urban areas – might require a different choice

[32] **Architecture of DLR's Flexible Air Surveillance System (Provided by DLR)**



[33] **UAV Occurences per Year (Source: EASA)[95]**



of sensors and actuators, and surely require a different set-up and configuration of an air surveillance system.

The DLR's surveillance system consists of a core system with the capability to attach different kinds of sensors, actuators and data processing modules; its general architecture is shown in Figure 32. The sensors, be it optical cameras, infrared cameras, radar or acoustic sensors, will be connected to the system and configured to observe a defined airspace. Their data is handed to the core system, in which data servers and archives are embedded. Data processing modules handle the signal processing of a single sensor's data or fuse the output from different sensors with complementary information to enhance the knowledge of an airspace intruder. The output of the data processing modules will again be handed over to the core system. This can be used to trigger connected actuators to intervene and to act on an intruder. The sensor data, derived products from data processing modules and in general all the gathered information is made available at the user terminals. Here, any kind of graphical display is imaginable. It will also be possible to connect mobile devices such as user terminals, e.g. to provide permanently updated information to every single police officer in the area.

The technology developed at DLR will lead to a hardware and software demonstrator, able to be exhibited in the field. The core system as well as different sensors and actuators with their respective data processing modules will be set up, leading to situation awareness and control capabilities on a user terminal. Shooting or net-throwing devices will not be presented to catch a drone. Instead, highly sophisticated systems to take control over a UAV will be part of the demonstrator.

In summary, DLR is heading towards making a significant contribution to the elimination of potential and already existing threats to humans and infrastructure through UAS. Its system concept to detect, trace and classify as well as to interact against drones is flexible and universally applicable for handling different kinds of air surveillance tasks in various scenarios. The demonstrator under development will show the general purpose of the system and will present its mode of operation. Once set up, it will even be possible to connect guest sensors, and consistently improve and specialise software modules. This technology is DLR's contribution to a safe future regarding the detection and handling of airspace intruders.

/About M-Sec

Hosted by Munich Airport, M-Sec - the Munich Aviation Security Conference - provides a high-level platform for exchange on key aspects and challenges of aviation security. Taking place on 10-11 July 2017, M-Sec will be held under the patronage of Dr Markus Söder, Bavarian State Minister of Finance, Regional Development and Regional Identity and Chairman of the Supervisory Board of Munich Airport, and Ambassador Wolfgang Ischinger, Chairman of the Munich Security Conference.

Background

Not since the end of the Cold War has the world been as dangerous as it is today. Especially aviation security is right in the center of crucial global challenges: terrorist attacks on airports, geopolitical instabilities resulting in substantial threats for civil aviation as well as aviation as target of cyber attacks, to name but a few. On the other hand, technological developments and innovations offer an enormous potential as well as regulatory and political challenges.

Format

For that reason, Munich Airport hosts M-Sec 2017. Preceded by an exclusive dinner reception, this one-day event offers high-ranking German and international decision-makers from politics, the private sector, military, civil society and academia the best-possible platform to discuss key aspects of international aviation security. The high-profile conference format provides room for interdisciplinary exchange and creates opportunities to develop takeaways for the private sector as well as for politics.

About Munich Airport

Munich Airport, which opened at its present site on 17 May 1992, ranks under the top ten busiest passenger airports in Europe. It handled 42 million passengers in 2016.

The FMG corporate group, with its 15 subsidiaries, employs more than 9,000 people. With a total workforce numbering more than 35,000 employees with 550 companies, Munich Airport is one of Bavaria's most important workplaces. Within just a few years of opening, Munich Airport developed into a major air transportation hub. Munich Airport now offers connections to more than 250 destinations all over the world. Moreover, it offers more than 200 shops and service facilities for a supreme experience of shopping and culinary delight and a variety of locations for hosting events, such as one of Europe's largest covered outdoor venues. Munich Airport is the only airport in the world to run its own brewery on site. Thus, in March 2015, Bavaria's gateway to the world has become Europe's first five-star airport.

The pinpoint landing on 17 May 1992, marked the start of a rapid development that saw Munich Airport make the transition from a regional point-to-point airport into a major European hub. Until May 2017, approximately 700 million passengers arrived, departed or changed planes at the new location. Over the past 25 years, Munich Airport has handled around 8.5 million flights and a total of approximately 4.6 million tons of airfreight.

Munich Airport has expanded its passenger-handling capacity to keep pace with demand. The opening of Terminal 2 in 2003 was followed in 2016 by the commissioning of a state-of-the-art satellite terminal that added capacity for a further 11 million passengers per year. Germany's first midfield terminal is linked to the original Terminal 2 via a driverless subway system that transports passengers between the two buildings comfortably and conveniently in less than a minute. In the next few years Terminal 1, which is starting to show its age, is slated to be expanded and updated with an additional pier and a new central complex. This will increase the capacity of Terminal 1 by 6 million passengers per year. The planners expect the expansion of Terminal 1 to be completed by 2022. The next priority is to expand Munich Airport's runway capacity to handle the projected increases in take-offs and landings.

About Agora Strategy Group

The Agora Strategy Group is a political consultancy providing in-depth political analysis and policy recommendations as well as offering tailor made services for the development of formats and concepts to support companies and public institutions in their strategic positioning activities. In doing so, we place a great deal of importance on dialogue and exchange between decision-makers and relevant stakeholders encouraging them to engage in discussions about the biggest political, economic and social issues of our time.

Complementary to our strategic advisory and political analysis portfolio, our consultancy specialises in organising top-level events around the world, from the programming, design and planning phases to execution and follow-up. Ideally, events are an integral part of strategic corporate positioning and contribute to the development of lasting networks. To ensure this is achieved, our services go well beyond organisation and execution thereby maximising value-added with events that range from exclusive dinners and talks with selected multipliers, to international conferences that serve political positioning purposes.

The Agora is the cradle of our democracy. In Ancient Greece, it served as the meeting place for the Polis. People convened here to do politics and business and to take part in cultural life. This idea of interaction and community shapes the foundation of the Agora Strategy Group's activities.

/Acknowledgements

We would like to personally thank the patrons of the Munich Aviation Security Conference and the M-Sec Report, Bavarian State Minister Dr Markus Söder and Ambassador Wolfgang Ischinger for supporting the first edition of the M-Sec Report. We are also grateful to the Bavarian State Ministry of Finance, Regional Development and Regional Identity, as well as the Munich Security Conference, for their support and advice.

This publication would not have been possible without the expertise and generous contributions by numerous renowned institutions, experts and high-ranking political decision makers. We would like to thank all knowledge partners, as well as their institutions and staff, for providing articles, data or research for the M-Sec Report. We would also like to thank and acknowledge the following individuals for their contributions and significant support:

Dimitris Avramopoulos and his Cabinet, European Commission; Anna M. Barcikowska and Jill O'Donnell, NATO Communications and Information Agency; Norbert Barthle and his office, German Federal Ministry of Transport and Digital Infrastructure; Marc Bachmann and Marc Fliehe, Bitkom e.V. - Digital Association of Germany; Douglas Barrie and Dr Bastian Giegerich, International Institute for Strategic Studies; Alexander Borgschulze and Holger Kraft, Munich Airport; Frank Brenner and his office, EUROCONTROL; Dan Chirondojan and the Department of Space, Security and Migration, Joint Research Center of the European Commission; Prof Dr Pascale Ehrenfreund and her office, German Aerospace Center (DLR); Prof Dr Elmar Giemulla and his staff, Berlin University of Technology; Dr Emily Haber and her office, German Federal Ministry of the Interior; Prof Dr Udo Helmbrecht and his office, European Union Agency for Network and Information Security; Ambassador Wolfgang Ischinger and his team, Munich Security Conference; Sir Julian King and his Cabinet, European Commission; Dr Hans-Georg Maaßen and his office, BfV – The German Domestic Intelligence Service; Prof Dr Peter R. Neumann, International Centre for the Study of Radicalisation and Political Violence at King's College London; Brigadier General Burkhard Pototzky and the National Center for Air Operations, German Air Force; Thomas Ramge, brand eins; Dr Steffen Richter, German Federal Police; Jan Syré, German Federal Association for Unmanned Systems (BUVUS); Alexander Sander and the Digital Society e.V.; Robert Viertel, German Aviation Association (BDL); Rob Wainwright and his office, Europol; Sven O. Weirup and the European Aviation Security Center; further more Dr Ekkehard Münzing and Lundeg Purevsuren.

We would also like to thank the following institutions that gave permission to use their data and research in the M-Sec Report:

Allianz Global Corporate & Speciality, Drone Industry Insights, Eurasia Group, FLYSEC Consortium, IBM, International Crisis Group, James Martin Center for Nonproliferation Studies and the Nuclear Threat Initiative, University of Uppsala

/References

Please take note that all links referred to were last revised on 24 June 2017.

1. Pew Research Center, »Europeans Face the World Divided«, 13 June 2016, http://www.pewglobal.org/2016/06/13/europeans-face-the-world-divided/.

2. Daniel S. Hamilton, Joseph P. Quinlan, »The Transatlantic Economy 2017 - Annual Survey of Jobs, Trade and Investment between the United States and Europe«, American Chamber of Commerce to the European Union, 2017, http://www.amchameu.eu/sites/default/files/170227_full-book.pdf.

3. Ian Bremmer, Cliff Kupchan, »Top Risks 2017: The Geopolitical Recession«, Eurasia Group, 3 January 2017, https://www.eurasiagroup.net/files/upload/Top_Risks_2017_Report.pdf.

4. START, »Global Terrorism Database«, as of 19 June 2017, https://www.start.umd.edu/gtd/.

5. See Endnote 4.

6. BBC News, »Somalia's Beledweyne airport hit by laptop bomb«, 7 March 2016, http://www.bbc.com/news/world-africa-35744737.

7. See Endnote 6.

8. BBC News, »Brussels explosions: What we know about airport and metro attacks«, 9 April 2016, http://www.bbc.com/news/world-europe-35869985.

9. BBC News, »EgyptAir flight MS804: What we know«, 15 December 2016, http://www.bbc.com/news/world-middle-east-36330879.

10. BBC News, »Shanghai Pudong airport explosion wounds four«, 12 June 2016, http://www.bbc.com/news/world-asia-china-36511028.

11. NBC News, »Istanbul Airport Attack Death Toll Rises to 45, Dozens Still Hospitalized«, 2 July 2016, http://www.nbcnews.com/storyline/istanbul-ataturk-airport-attack/istanbul-airport-attack-death-toll-rises-45-dozens-still-hospitalized-n602946.

12. Alissa J. Rubin and Benoît Morenne, »Gunman Is Killed in Orly Airport in France After Attacking a Soldier«, The New York Times, 18 March 2017, https://www.nytimes.com/2017/03/18/world/europe/orly-airport-france-shooting.html.

13. The interview was conducted on 2 June 2017.

14. CNN Politics (Video), »Mattis: North Korea a clear and present danger«, as of 22 June 2017, http://edition.cnn.com/videos/politics/2017/06/03/james-mattis-north-korea-clear-present-danger-sot.cnn.

15. James Martin Center for Nonproliferation Studies; The Nuclear Threat Initiative, »The CNS North Korea Missile Test Database«, 22 May 2017, http://www.nti.org/analysis/articles/cns-north-korea-missile-test-database/.

16. James Martin Center for Nonproliferation Studies for the Nuclear Threat Initiative, »North Korea's Strategic Threat«, May 2017, http://www.nti.org/learn/countries/north-korea/.

17. International Crisis Group, »CrisisWatch - Tracking Conflict Worldwide«, May 2017, https://www.crisisgroup.org/crisiswatch.

18. Uppsala University - Department of Peace and Conflict Research, »Uppsala Conflict Data Program«, as of 19 June 2017, http://ucdp.uu.se/.

19. David Rogers, »The Future of Air Transport«, Chartered Institute of Building - Global Construction Review, 8 October 2014, http://www.globalconstructionreview.com/sectors/futur23e-ai35789r-trans590port/, numbers based on own calculations in select cases.

20. Airports Council International, »Total Passenger Traffic 2016«, ACI Media Releases, 19 April 2017, http://www.aci.aero/News/Releases/Most-Recent/2017/04/19/ACI-releases-preliminary-2016-world-airport-traffic-rankingsRobust-gains-in-passenger-traffic-at-hub-airports-serving-transPacific-and-East-Asian-routes.

21. ALPHA SCRAMBLES are Security flights of fighter aircrafts which are conducted for the immediate defence of the Federal Republic of Germany or in order to guarantee the integrity of the airspace of the Federal Republic of Germany and prevent attacks on the safety of air traffic, particularly aircraft hijacking, acts of sabotage and terrorism.

22. Nationales Lage- und Führungszentrum Sicherheit im Luftraum (German), Jährliche von der DFS an das NLFZ SiLuRa gemeldete LOSSCOM-Vorfälle im DEU Luftraum (Oktober 2003 bis Juni 2017), June 2017; directly provided to M-Sec.

23. The International Institute for Strategic Studies (IISS), »Military Balance +« (graphic directly provided to M-Sec by IISS), see databse: http://www.iiss.org/en/publications/military-s-balance/militarybalanceplus.

24. European Aviation Safety Agency (EASA), »Conflict Zones«, as of 19 June 2017, https://www.easa.europa.eu/easa-and-you/international-cooperation/easa-by-country/conflict-zones.

25. Federal Aviation Administration, »Prohibtions, Restrictions and Notices«, as of 19 June 2017, https://www.faa.gov/air_traffic/publications/us_restrictions/.

26. EUROCONTROL, »Network Operations Portlet«, as of 20 June 2017, https://www.public.nm.eurocontrol.int/PUBPORTAL/gateway/spec/index.html, please note: this is the public version, which does not include the Crisis Management Portlet.

27. ICAO, »Conflict Zones Risk Information«, as of 20 June 2017, https://www.icao.int/czir/Pages/posts.aspx?state=default.

28. European Commission - Press Release, »European Agenda on Security: Commission sets out new approach on interoperability of information systems«, 16 May 2017, http://europa.eu/rapid/press-release_IP-17-1303_en.htm.

29. See Endnote 28.

30. IATA, »IATA Industry Fraud Prevention«, as of 19 June 2017, http://www.iata.org/whatwedo/airline-distribution/Pages/industry-fraud-prevention-initiative.aspx.

31. See: https://www.nomoreransom.org/, as of 19 June 2017.

32. Council of the European Union, »Overview of the information exchange environment in the justice and home affairs area«, 15 February 2017, http://data.consilium.europa.eu/doc/document/ST-6253-2017-INIT/en/pdf.

33. eu-LISA, the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, »a newly established EU agency to provide a long-term solution for the operational management of large-scale IT systems, which are essential instruments in the implementation of the asylum, border management and migration policies of the EU«, http://www.eulisa.europa.eu/AboutUs/WhoWeAre/Pages/default.aspx.

34. See Endnote 33.

35. High-level expert group on information systems and interoperability, »Final Report«, May 2017, http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

36. Florian Rötzer, »US-Regierung bewertet das Risikopotenzial aller Ein- und Ausreisenden«, Telepolis (German), 1 December 2006, https://www.heise.de/tp/features/US-Regierung-bewertet-das-Risikopotenzial-aller-Ein-und-Ausreisenden-3409070.html.

37. Court of Justice of the European Communities, Press Release No 46/06, »The Court annuls the Council decision concerning the conclusion of an agreement between the European Community and the United States of America on the processing and transfer of personal data and the Commission decision on the adequate protection of those data«, 30 May 2006, https://curia.europa.eu/jcms/upload/docs/application/pdf/2009-02/cp060046en.pdf.

38. EUR-Lex, Council Decision 2007/551CFSP/JHA, 23 July 2007, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1416845561356&uri=OJ:JOL_2007_204_R_0016_01.

39. European Commission, »Proposal for a Directive of the European Parliament and of the Council on the use of Passanger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime«, 2 February 2011, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011PC0032&from=EN.

40. Official Journal of the European Union, »Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United Stated Department of Homeland Security«, 11 August 2012, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22012A0811(01)&from=EN.

41. Council of the European Union, »Signature of the EU-Canada agreement on Passenger Name Records (PNR)«, 25 June 2014, http://www.consilium.europa.eu/en/press/press-releases/2014/06/pdf/signature-of-the-eu-canada-agreement-on-passenger-name-records-(pnr)/.

42. European Parliament News, »Parliament backs EU directive on use of Passenger Name Records (PNR)«, 14 April 2016, http://www.europarl.europa.eu/news/en/headlines/priorities/20150218TST24901/20160407IPR21775/parliament-backs-eu-directive-on-use-of-passenger-name-records-pnr.

43. Court of Justice of the European Union, Press Release No 89/16, »According to Advocate General Mengozzi, the agreement on the transfer of passenger name record data, planned between the European Union and Canada, cannot be entered into ist current form«, 8 September 2016, https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-09/cp160089en.pdf.

44. Deutscher Bundestag, Dokumente, »Fluggastdaten gegen Kriminelle und Schwerkriminelle nutzen«, 27 April 2017, https://www.bundestag.de/dokumente/textarchiv/2017/kw12-de-fluggastdaten/496772.

45. Official Journal of the European Union, »Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime« , 27 April 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0681&qid=1498336443679&from=en.

46. Landespressedienst (German), Zitat BM de Maizière zur Verabschiedung der EU-PNR im EP (own translation), 14 April 2016, https://www.landespressedienst.de/zitat-bm-de-maiziere-zur-verabschiedung-der-eu-pnr-im-ep/.

47. See the article in this report: »Aviation in Times of Terror - An Interview with Prof Dr Peter Neumann«

48. Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 34, »Gesetz zur Umsetzung der Richtlinie (EU) 2016/681«, 9 June 2017, https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*[@attr_id=%27bgbl117s1484.pdf%27]#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s1484.pdf%27%5D__1497894983950.

49. Sascha Lobo, »Attentäter islamistischer Mordanschläge in der EU (2014-2017)«, SPIEGEL Online, 31 May 2017, http://www.spiegel.de/netzwelt/web/islamistischer-terror-in-europa-unsere-sicherheit-ist-eine-inszenierung-a-1150015.html.

50. Jan Philipp Albrecht Pressemitteilung (German), »PNR-Massenüberwachung schützt nicht vor Terroristen«, (own translation), 14 April 2016, https://www.janalbrecht.eu/presse/pressemitteilungen.html?tx_ttnews%5Btt_news%5D=1750&cHash=9efaaac741033b71033c2554a41f30a0.

51. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (German), Pressemitteilung, »Fluggastdatengesetz erst nach Vorliegen des EuGH-Gutachtens beschließen«, 24 April 2017, https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2017/08_Fluggastdatengesetz.html.

52. Bundesverfassungsgericht, Leitsätze zum Beschluss des Ersten Senats - 1 BvR 518/02, 4 April 2006, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2006/04/rs20060404_1bvr051802.html.

53. Andrew Colley, »Cyber weapons conventions needed, Kaspersky tells CeBIT«, The Australian, 22 May 2012, http://www.theaustralian.com.au/business/technology/cyber-weapons-conventions-needed-kaspersky-tells-cebit/news-story/a530d087af93a58b16a05600c7831a52.

54. Air Traffic Management, »ICAO summit prescribes cyber security approach«, 5 April 2017, http://www.airtrafficmanagement.net/2017/04/icao-summit-prescribes-cyber-security-approach/.

55. Europol, »Serious and Organised Crime Threat Assessment (SOCTA)«, as of 20 June 2017, https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment.

56. National Crime Agency (NCA), »NCA Strategic Cyber Industry - Group Cyber Crime Assessment 2016«, 7 July 2016, http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file.

57. Chloe, Farrand, »The Netherlands will count every vote by hand to stop hackers influencing parliamentary election«, The Independent, 2 February 2017, http://www.independent.co.uk/news/world/europe/netherlands-parliamentary-election-count-vote-by-hand-stop-hackers-cyber-crime-fraud-hacking-a7558701.html.

58. IBM X-Force Research, »Security trends in the transportation industry«, June 2016, https://securityintelligence.com/media/security-trends-transportation-industry/.

59. European Aviation Safety Agency, »Implementation of a European Centre for Cyber Security in Aviation(ECCSA)«, 4 April 2017, https://www.easa.europa.eu/newsroom-and-events/news/implementation-european-centre-cyber-security-aviationeccsa.

60. See Endnote 59.

61. The European Cybercrime Center EC3: »Europol set up the European Cybercrime Centre (EC3) in 2013 to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online crime.«, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

62. The European Union External Action Service, https://eeas.europa.eu/headquarters/headquarters-homepage_en.

63. Dr Bernhard Rohleder, »Digitalisierung in der Luftfahrt«, Bitkom e.V., 1 June 2016, https://www.bitkom.org/Presse/Anhaenge-an-PIs/2016/Juni/Bitkom-Pressekonferenz-Digitalisierung-in-der-Luftfahrt-01-06-2016-Praesentation-final.pdf.

64. The views expressed in this article do not necessarily represent the official position or policy of member governments or NATO.

65. European Union Agency for Network and Information Security, »Securing Smart Airports«, December 2016, https://www.enisa.europa.eu/publications/securing-smart-airports/at_download/fullReport.

66. See Endnote 64.

67. See Endnote 64.

68. ADS-B stands for Automatic Dependent Surveillance – Broadcast, ACARS stands for Aircraft Communications Addressing and Reporting System.

69. Airport Cooperative Research Programe (ACRP), Report 140, »Guidebook on Best Practices for Airport Cybersecurity«, 2015, http://www.trb.org/Publications/Blurbs/172854.aspx.

70. Centre for the Protection of National Infrastructure, »Cyber-security in Civil Aviation«, 2012.

71. Official Journal of the European Union, »Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union«, 6 July 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=DE.

72. For more information on ENISA efforts and to download the report »Securing Smart Airports«, please visit https://enisa.europa.eu/air.

73. See Endnote 64.

74. Official Journal of the European Union, »Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection«, 8 December 2008, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=DE.

75. Bundesministerium des Innern (BMI), »Nationale Strategie zum Schutz kritischer Infrastrukturen (KRITIS-Strategie)«, June 2009, http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.pdf?__blob=publicationFile.

76. Bundesverband der Deutschen Fluggesellschaften, »Überblick über Luftsicherheitsgebühren an deutschen Flughäfen (2017)«, December 2016, http://www.bdf.aero/files/7214/8222/7748/28._Luftsicherheitsgebhren.pdf.

Airliners.de, »Luftsicherheitsgebühren 2014, 2015, 2016 und 2017 pro Passagier«, 14 November 2016, http://www.airliners.de/luftsicherheitsgebuehren-anfang-2017/40044.

Airliners.de (German), »Luftsicherheitsgebühren 2013 und 2014 pro Passagier«, 16 December 2013, http://www.airliners.de/luftsicherheitsgebuehren-steigen-zum-jahresbeginn-teils-kraeftig/30980.

Flughafen München, »Verkehrszahlen«, as of 19 June 2017, https://munich-airport.de/verkehrszahlen-88506.

Fraport AG, »Verkehrszahlen Standort FRA«, as of 19 June 2017, http://www.fraport.de/content/fraport/de/investor-relations/finanz-und-verkehrszahlen/verkehrszahlen.html.

Köln Bonn Airport, »Kennzahlen«, as of 19 June 2017, https://www.koeln-bonn-airport.de/unternehmen/daten-fakten.html.

Düsseldorf Airport DUS, »Daten, Zahlen, Fakten - Verkehrszahlen 2006-2016«, as of 19 June 2017, https://www.dus.com/de-de/konzern/unternehmen/zahlen-und-fakten/verkehrszahlen.

Hamburg Airport, »Zahlen, Daten, Fakten«, as of 22 June 2017, https://www.hamburg-airport.de/de/zahlen_daten_fakten.php.

Flughafen Berlin Brandenburg BER, »Verkehrsstatistik«, as of 22 June 2017, http://www.berlin-airport.de/de/presse/basisinformationen/verkehrsstatistik/index.php.

77. Bundesverband der Deutschen Fluggesellschaften, »Zuständigkeiten und Aufsicht im Bereich Sicherheit im Luftverkehr – Gefahren von außen (Security) und flugbetriebliche Gefahren (Safety)«, as of 19 June 2017, http://www.bdf.aero/download_file/view/144/188/.

78. If this article contains any evaluation or assessment, it is the authors's private opinion and view.

79. Airbus, »Global Market Forecast 2017-2036«, 2017, http://www.aircraft.airbus.com/market/global-market-forecast-2017-2036/.

80. FLYSEC, »About FLYSEC«, as of 22 June 2017, http://www.fly-sec.eu/about.html.

81. FLYSEC, »FLYSEC Overall Security Concept«, as of 22 June 2017, http://www.fly-sec.eu/about.html.

82. FLYSEC, »FLYSEC System Architecture«, as of 22 June 2017, http://www.fly-sec.eu/about.html.

83. See Endnote 79.

84. Official Journal of the European Union, »Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002«, 11 March 2008, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008R0300&from=EN.

85. Official Journal of the European Union, »Commission Regulation (EU) No 72/2010 of 26 January 2010 laying down procedures for conducting Commission inspections in the field of aviation security«, 26 January 2010, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:023:0001:0005:EN:PDF.

86. European Commission, »Proposal for a Regulation of the European Parliament and the Council establishing a Union certification system for aviation security screening equipment (COM 2016/491)«, 7 September 2016, http://eur-lex.europa.eu/resource.html?uri=cellar:094f451e-751d-11e6-b076-01aa75ed71a1.0011.02/DOC_1&format=PDF.

87. Bundesministerium für Verkehr und Digitale Infrastruktur (BMVI), »Klare Regeln für Betrieb von Drohnen«, M-Sec Team translation, as of 20 June 2017, http://www.bmvi.de/SharedDocs/DE/Artikel/LR/151108-drohnen.html.

88. See the article in this report: »Drone Detection and Countermeasures - The DLR-Initiative«, Prof Dr Pascale Ehrenfreund

89. Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 17, »Verordnung zur Regelung des Betriebs von unbemannten Fluggeräten«, 30 March 2017, http://www.bmvi.de/SharedDocs/DE/Anlage/LF/verordnung-zur-regelung-des-betriebs-von-unbemannten-fluggeraeten.pdf?__blob=publicationFile.

90. Allianz Global Corporate & Speciality, »Rise of Drones - Managing the Unique Risks Associated with Unmanned Aircraft Systems«, September 2016, https://www.agcs.allianz.com/assets/PDFs/Reports/AGCS_Rise_of_the_drones_report.pdf.

91. Thomas Ramge, »Drohnen: Startklar«, Brandeins (Ausgabe 02/2017), M-Sec team translation, February 2017, https://www.brandeins.de/archiv/2017/marketing/drohnen-startklar/.

92. See Endnote 89.

93. See Endnote 89.

94. Drone Industry Insights, »UAV rule-making progress in the EU and the USA«, updated version, provided to M-Sec by Drone Industry Insights, as of 20 June 2017, https://www.droneii.com/uav-rule-making-what-is-taking-europe-so-long.

95. European Aviation Safety Agency (EASA), »Drone Collision' Task Force - Final Report«, 4 October 2016, https://www.easa.europa.eu/system/files/dfu/TF%20Drone%20Collision_Report%20for%20Publication%20%28005%29.pdf.

/Disclaimer

The M-Sec Report team:
Tim Gürtler, Tina Hahn, Barbara Mittelhammer, Fabian Vetter, Susanna Weinekötter

The M-Sec Report draws on the research and input provided by M-Sec's various knowledge partners as well as their personal views and contributions. All articles listing an author or an institution combined with the respective logo reflect the opinion and views of the authors/institutions. The M-Sec Report aims to be thought-provoking to the audience of the Munich Aviation Security Conference as well as to the interested public. Therefore, we do not endorse and support every quote, line of analysis or external contribution in this report.

All other information and data presented in the M-Sec Report and further information and data on which the report is based have been obtained from sources which the M-Sec Report team believes to be reliable, accurate and trustworthy. In any case, we cannot guarantee their accuracy or completeness. The M-Sec team has secured all the rights necessary to publish the data presented. The M-Sec team has also secured all the rights necessary to publish any image, photo or graphic used in the M-Sec Report.

The official publisher of the M-Sec Report is Munich Airport in its capacity as host of the Munich Aviation Security Conference 2017. Responsible in terms of concept, content, cooperation with partners, editing, layout and design is the Agora Strategy Group AG, which produced the M-Sec Report in its advisory capacity to Munich Airport.

For further information on this report, please email us at info@agora-strategy.com. We welcome any feedback, criticism, suggestions or ideas for improvement.

Publication details:
Publisher:

Flughafen München GmbH
Corporate Security
Holger Kraft

PO Box 23 17 55
85326 Munich

Responsible for concept, content, cooperation with partners, editing, layout and design:

Agora Strategy Group AG
Tim Gürtler

Residenzstrasse 7
80333 Munich

info@agora-strategy.com
+49 (0)89 2554 4084

Available online at www.m-sec.org/m-sec-report

Printed by: G. Peschke Druckerei GmbH
Co-edited by: Textra Fachübersetzungen GmbH

www.m-sec.org

www.munich-airport.de