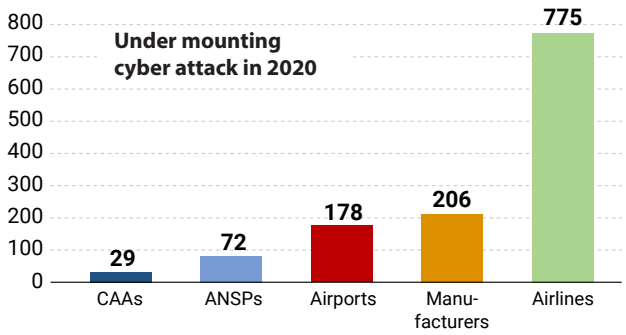
EUROCONTROL

Aviation under attack: Faced with a rising tide of cybercrime, is our industry resilient enough to cope?

The European aviation industry is being increasingly exposed to rising levels of risk, as criminals, hackers and state-sponsored cyber-attackers look to exploit vulnerabilities, cause chaos, and above all, fill their pockets at the expense of the aviation sector, with airlines and the flying public firmly in their sights. Using exclusive EUROCONTROL data from the Agency's EATM-CERT (European Air Traffic Management Computer Emergency Response Team) service, this Think Paper casts light on the urgency of the threat, gives an idea of its magnitude, assesses the threat sources, advises how European aviation actors should enhance their cyber-resilience – and explains what EUROCONTROL can do to help.

This Think Paper finds that the worst financial crisis aviation has ever experienced **has created new opportunities for cybercrime**. Attacks are up in all threat categories, and better reporting alone does not fully account for the **530% year-on-year rise** in reported incidents. In all this, **airlines are most in the line of fire**, targeted by **61% of all 2020 aviation cyber-attacks** in 2020.



We also find that **aviation faces a ransomware attack every week**. Ransomware attacks are a serious threat to business continuity and can **bring a company's operations to a grinding halt**, with potentially **severe financial impacts**, even before factoring in any ransoms paid to buy back data or take back control of internal systems. It's a huge concern – and the price of ransomware mitigation measures alone is expected to cost global companies an eye-watering **$20 billion** a year.

There are also, we find, a growing number of state-sponsored or highly organised crime syndicates capable of conducting large-scale targeted intrusions to disrupt as well as to extort money.

Source: Safety Detectives; projected cost all sectors

However, the fact that the European aviation community has upped its detection capabilities, and improved its reporting culture, are grounds for cautious optimism. Effective cybersecurity advocacy by EUROCONTROL's EATM-CERT service and other partners has played its part in this – and highlights the importance of continuing to raise cyber-awareness.

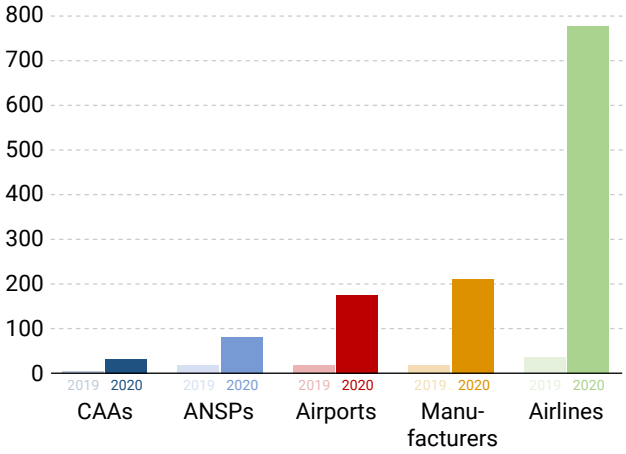
Main Think Paper findings

1. **Airlines continue to be an irresistible target for cybercriminals**, with around **$1 billion a year** lost from fraudulent websites alone. Add to that data theft, card fraud, air miles fraud, phishing, fake invoices and more, and you have **a perfect storm for a part of the industry that continues to reel from the pandemic**.
2. **Every week, an aviation actor suffers a ransomware attack somewhere in the world, with big impacts on productivity and business continuity,** let alone data loss and/or costly extortion demands paid in order to restart operations.
3. **Fortunately no impact on flight safety has yet been reported – but that is no grounds for complacency**, with state-sponsored or highly organised crime syndicates capable of conducting **large-scale targeted intrusions** that aim at **massive disruption** as much as financial gain.
4. **Many aviation actors, including in the supply chain, are exposing themselves to extra risk** by not systematically applying basic IT security controls.
5. **Digital identities need to be better safeguarded, which is why Europe needs the EACP** (European Aviation Common Public Key Infrastructure), a solution currently under development by EUROCONTROL and partners.
6. **EUROCONTROL's EATM-CERT services, and those of its cyber partners, are key to foiling fraudsters, and save stakeholders millions every year.**

The 2020 cyber-attack wave

Cyber-attacks reported to or identified by EUROCONTROL's EATM-CERT (European Air Traffic Management Computer Emergency Response Team) rose by 530% between 2019 and 2020, with startling impacts across market segments, as Figure 1 shows:

FIGURE 1: REPORTED CYBER ATTACKS ON AVIATION 2019 VS 2020



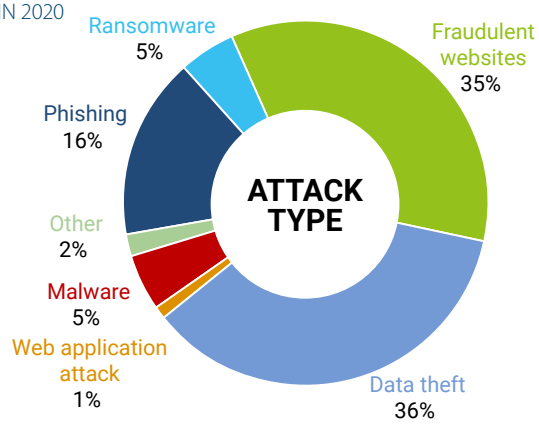
Source: EUROCONTROL EATM-CERT

While growing cyber-maturity in terms of detection and better incident reporting account for part of this rise, it is an inescapable conclusion that cybercrime is significantly increasing.

The cyber-fraud 'Big 3': Fake websites, data theft and phishing

At **36%** of all reported incidents, **data theft** topped the cyber charts in 2020, followed by **website fraud** (**35%**) and **phishing** (**16%**). A notable and growing threat, just **5%** for now but with potentially immense negative impacts when successful, is **ransomware**.

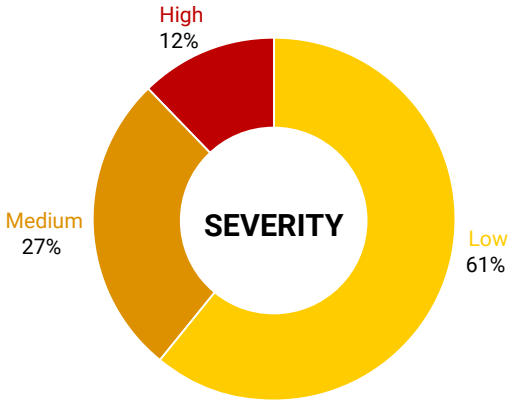
FIGURE 2: BREAKDOWN OF REPORTED CYBER-ATTACKS IN AVIATION IN 2020



Source: EUROCONTROL EATM-CERT

A worrying **39%** of organisations experiencing cyber-attacks in 2020 assessed that **these attacks had had a medium to high impact on their operations**, as Figure 3 shows:

FIGURE 3: SEVERITY OF ATTACKS ON AVIATION IN 2020



Source: EUROCONTROL EATM-CERT

Airlines: In the line of cyber-fire

After losing a colossal €60.6 billion[1] in 2020 owing to COVID, Europe's airlines, airports and air navigation service providers (ANSPs) can ill-afford the additional costs caused by a rising tide of cyber-attacks – but that is exactly what is happening.

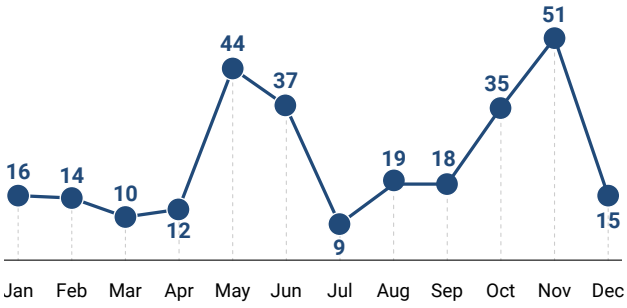
61% of all identified cyber-attacks in 2020 targeted airlines, almost twice as much as the two next largest market segments combined (16% manufacturers, 15% airports).

The vast majority of these attacks – **95%** – were financially motivated: **739** out of **775** incidents. This led to financial loss in **55%** of cases, and the leaking or theft of personal data in an additional **34%** of cases.

Of the **335 fraudulent** and **fake refund websites** uncovered by EUROCONTROL's EATM-CERT in 2020, **280** were **impersonating IATA and A4E airline members**, selling fake tickets and seeking to extract customer credit card data. Fraudsters also took advantage of the uncertainty created by COVID-19 regarding ticket changes and refunds, **with the number of fake websites markedly increasing from the moment States started to impose lockdowns**, as per Figure 4:

"61% of all identified cyber-attacks in 2020 targeted airlines, almost twice as much as the two next largest market segments combined"

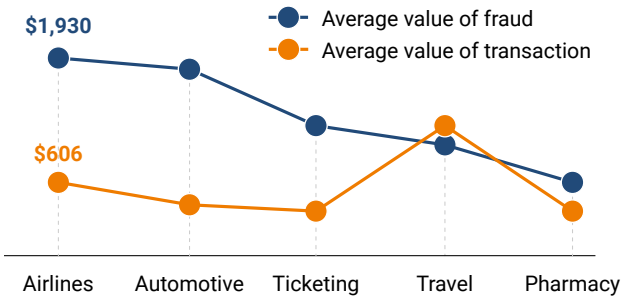
FIGURE 4: MONTHLY VIEW OF FRAUDULENT AIRSPACE USER WEBSITE CREATION, 2020



Source: EUROCONTROL EATM-CERT

The fake airline ticket business is extremely lucrative: the average value of a purchase is significantly higher than that of a legitimate purchase, as Figure 5 highlights. "Big Game Hunting" fraudsters are drawn to the profit margins on airline ticket fraud – where the average cost of a fake ticket, at around **$1,930**, is almost **triple** that of a legitimate purchase (on average **$606**).

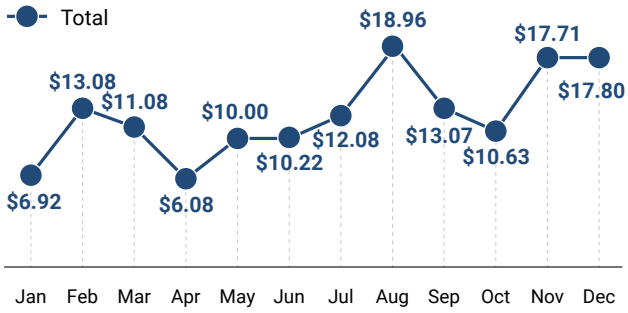
FIGURE 5: AVERAGE VALUE OF FRAUD TRANSACTIONS IN 2020, SELECTED SECTORS



Source: IATA[2]

Airline loyalty programme accounts are a hugely attractive target for fraudsters, and **the pandemic has accelerated criminal interest as airlines began returning money via loyalty accounts to passengers whose flights had been cancelled owing to the pandemic, or extending the validity period of accumulated miles**. In 2020 EATM-CERT issued alerts to **30** airlines, and detected **15,493 accounts** on offer on the dark web, worth over **$400,000**. The total market value of unredeemed miles is enormous – estimated by IATA at **$238 billion**[3]. Figure 6 shows how during the pandemic the average value of a compromised account rose by **48%** between 1Q and 4Q 2020:

FIGURE 6: AVERAGE PRICE OF COMPROMISED ACCOUNTS ACROSS 2020

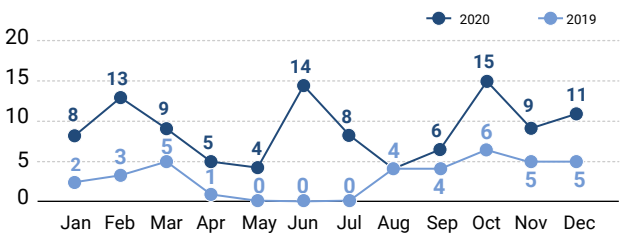


Source: EUROCONTROL EATM-CERT

Data theft continues to be a huge problem, with the customer personal data and credit card details that airlines collect proving an irresistible target for criminals. Since Cathay Pacific suffered the worst breach of personal data ever in the industry back in 2018, with **9.4 million** records stolen, data breaches – with personal data and card info making its way into the hands of criminals over the dark web – have become commonplace, with other high-profile victims including British Airways (around **565,000** exposed details in 2018) and easyJet, which in 2020 suffered an attack leading to **9 million** customers' details being exposed and thousands of credit card details stolen. Most recently, in March 2021 a hack of global aviation industry IT supplier SITA has led to a **massive and not yet fully quantified** breach of passenger data at a company that handles bookings for around 90% of the world's airlines, a breach that could dwarf the Cathay Pacific incident in terms of millions of exposed records.

Route charges (en-route and terminal) collected from airlines and other airspace users by EUROCONTROL's Central Route Charges Office are also a growing target. Figure 7 shows that **attempted airline route charges fraud significantly increased despite the dramatic drop in flights in 2020**. EATM-CERT uncovered **243** false route charges notifications impersonating the Agency, suspended **106** domain names and email addresses, and stopped in one instance a **€1.8 million** route charges fraud.

FIGURE 7: ROUTE CHARGES FRAUD DOMAINS/EMAILS SUSPENDED, 2019 VS. 2020



Source: EUROCONTROL EATM-CERT

"Attempted airline route charges fraud significantly increased in 2020, despite the dramatic drop in flights"

Fraudulent websites, phishing/malware & IPR theft top the threat tables for airports, ANSPs & manufacturers

Airports	ANSPs	Manufacturers
■ **Fraudulent websites** were the biggest numerical threat in 2020 and accounted for **100 of the 178 reported attacks** – with attackers attracted to the large number of public-facing IT-based systems and services, including goods. ■ **93 attacks – again over 50% – aimed at making financial gain**. ■ Airports are highly experienced in cyber-resilience, but **massive budget cuts could put strain on counter-measures**, as a recent ACI study[4] underlines. ■ Fortunately, t**he vast majority of reported attacks (80%) had low impacts**, with few instances of malicious attempts to disrupt operations.	■ **Phishing and malware** were the main threat vectors in 2020, resulting in **39** of **72** reported incidents. ■ **Most threats targeted non-operational systems, and had an overall low impact** (only 12% of attacks classified as medium or high severity). ■ **Only 3 attacks had an operational disruption, with little to no impact on flights in terms of delays or cancellations.** ■ However, **disruptive actors not only motivated by profit are on the rise: there are no grounds for complacency**, and EATM-CERT penetration testing and vulnerability scanning is proving increasingly popular among ANSPs.	■ **Data theft**, as cybercriminals sought to monetise intellectual property, accounted for **122** of **206** reported attacks. As companies move data into cloud-based infrastructure accessible by multiple devices, cyber-protection is becoming increasingly challenging. ■ **Ransomware is worryingly a growing threat**, with **39** reported attacks seeking to blackmail companies into coughing up. ■ **Supply chains and production** were directly affected by **13%** of attacks – **causing significant additional costs**. ■ **75% of reported cyberattacks** were classified by manufacturers as having a medium to high impact.

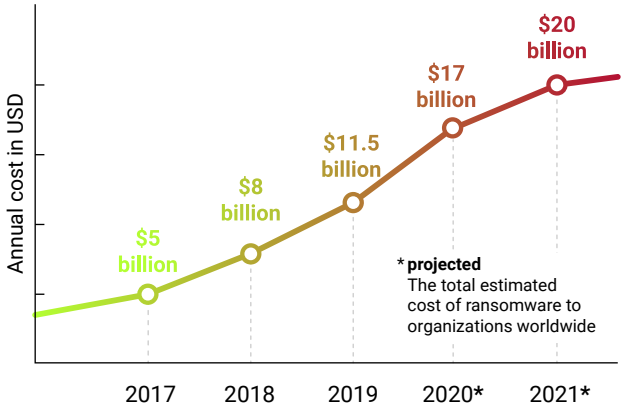
Ransomware: Capable of turning off ops - and hitting one aviation stakeholder every week

Every week, an aviation stakeholder faces a ransomware attack somewhere in the world, with **62** cyber-attacks on global aviation actors detected by or reported to EATM-CERT in 2020.

Ransomware may only comprise **5%** of detected cyber-attacks on aviation in 2020, but it can have huge impacts for the individual actors hit by it – and it is an **increasingly profitable business segment for criminal gangs**. Successful attacks lead to loss of data and/or costly extortion demands to obtain a decrypt key; both successful and unsuccessful ransomware attacks **damage business continuity** while secure file access is regained and may force some or all operations to be temporarily suspended, **hitting profits hard**.

As Figure 8 indicates, the cost of ransomware to global business tripled between 2017 and 2020, and is set to have quadrupled by the end of this year to an eye-watering **$20 billion**. **51%** of IT managers across all industries revealed in a Sophos[5] survey that their businesses had been hit at least once in 2020 by ransomware, with the majority of attacks server-based and highly disruptive.

FIGURE 8: THE GROWING RANSOMWARE TAB, ALL SECTORS, 2017-2021 (PROJECTED)



Source: Safety Detectives[6]

"Every week somewhere in the world, an aviation stakeholder faces a ransomware attack which if successful, generates disproportionately high financial and reputational impacts – and hits productivity hard even if unsuccessful"

Ransomware is clearly on the rise in all sectors including aviation, with 2021 setting **new ransomware records with $50 million demands made**. Three recent high-profile aviation attacks are the June 2020 ransomware attack on US-based VT San Antonio Aerospace, resulting in **1.5 terabytes** of sensitive data stolen; the American ultra-low-cost carrier Spirit Airlines' major data breach in March 2021, with tranches of financial/personal data released on the dark web and a ransom demand issued; and the May 2021 Colonial Pipeline (CP) attack, the largest successful ransomware attack ever mounted on a public infrastructure. CP were forced to pay a **$4.4 million** ransom to recover pipeline operations – resulting in East Coast airports running low on fuel, and forcing airlines to cancel flights and modify flight plans for refuelling purposes. Most recently, the latest aviation actor to report a ransomware attack was Japan Airport Fueling Service, hit on 21 June by an attack that impacted internal systems but did not affect their core refuelling business.

To be better prepared to manage a ransomware attack, EATM-CERT has teamed up with A-ISAC, the Aviation Information Sharing and Analysis Centre, on a joint awareness campaign about ransomware to help aviation stakeholders better understand the threat, and recommend best practices to reduce risks.

Phishing: Cheap, easy, sophisticated and successful

Phishing attempts directed at aviation continued to increase in 2020, as they did in other sectors. **The attractiveness of a phishing campaign remains its low-cost and speculative nature:** phishing emails can be extremely convincing, and some phishing attempts will inevitably slip past organisations' spam and malware filters. **If just one person in an organisation of thousands takes the bait, that can be enough to make the entire attack worthwhile**. This highlights the importance of raising awareness within organisations about how good cybersecurity practice involves every staff member, and that attacks cannot be prevented by technology alone.

To this end, EUROCONTROL's EATM-CERT has created a phishing awareness campaign service to help European aviation stakeholders better manage phishing risk. This will be rolled out in 2021, giving guidance on how to run internal campaigns, how to raise awareness of the need for caution, and how to change behaviours in order to train all staff to be more cyber-resilient.

DDoS: Still a threat – are we well protected enough?

DDoS (distributed denial of service) claims major scalps every year, with 2020 setting a new record as Amazon Web Services faced a **2.3 terabit-per-second DDoS attack**. To counter DDoS, EATM-CERT is trialling an anti-DDoS solution to help aviation stakeholders test the actual performance of their anti-DDoS solutions.

EACP: A secure digital identity

With stakeholders increasingly dependent on information systems, an effective, robust means of securing electronic communications and transactions has become increasingly important. The European Aviation Common Public Key Infrastructure, or EACP for short, aims at addressing European aviation's specific needs for identification and authentication, and will support stakeholders in complying with Common Pilot Project (CP1) Implementing Rule (EC N° 2021/116). It is aimed at all European airlines, ANSPs, airports, civil aviation authorities, military organisations, manufacturers or businesses providing aviation services in any of EUROCONTROL's 41 Member States and 2 Comprehensive Agreement States.

Built on a PKI (Public Key Infrastructure), the EACP will secure electronic communications and transactions, allowing European aviation actors to carry out secure communications. PKI is based on digital IDs which act like electronic passports. Implementation is set for 2022, with full operations planned for 2023.

CONCLUSIONS

While European aviation has become more cyber-secure, **cybercrime and cyber warfare are a new battleground**, and the aviation industry **cannot afford to lower its defences** as it struggles to recover from the worst financial crisis in its history.

Main Think Paper findings

1. **Airlines continue to be an irresistible target for cybercriminals**, with around **$1 billion a year** lost from fraudulent websites alone. Add to that data theft, card fraud, air miles fraud, phishing, fake invoices and more, and you have **a perfect storm for a part of the industry that continues to reel from the pandemic**.

2. **Every week, an aviation actor suffers a ransomware attack somewhere in the world, with big impacts on productivity and business continuity,** let alone data loss and/or costly extortion demands paid in order to restart operations.

3. **Fortunately no impact on flight safety has yet been reported – but that is no grounds for complacency**, with state-sponsored or highly organised crime syndicates capable of conducting large-scale targeted intrusions that **aim at massive disruption as much as financial gain** on the rise.

4. **Many aviation actors, including in the aviation supply chain, are exposing themselves to unnecessary additional risk** by not systematically applying basic IT security controls.

5. **Digital identities need to be better safeguarded, which is why Europe needs the EACP** (European Aviation Common Public Key Infrastructure), a solution currently under development by EUROCONTROL and partners.

6. **EUROCONTROL's EATM-CERT services, and those of its cyber partners, are key to foiling fraudsters, and save stakeholders millions every year.**

---

1 **EUROCONTROL, "Think Paper #8:** What COVID-10 Did to European Aviation in 2020, and Outlook 2021", January 2021 Think Paper, available at: https://www.eurocontrol.int/sites/default/files/2021-02/eurocontrol-think-paper-8-impact-of-covid-19-on-european-aviation-in-2020-and-outlook-2021.pdf

2 **IATA, "Fraud in the Airline Industry:** Why Carriers Need to Think of Themselves as Crimefighters", July 2020 White Paper, available at: https://www.iata.org/contentassets/8a1d401955164c868258e7875edd5d5a/iata_whitepaper_fraud_july2020_digital_en.pdf

3 **IATA, "Fraud prevention:** Strengthening the Defences", 6 March 2019, available at: https://www.airlines.iata.org/analysis/fraud-prevention-strengthening-the-defences

4 **ACI, "Airport Cybersecurity in a COVID-19 World**, 6 January 2021, available at: https://blog.aci.aero/airport-cybersecurity-in-a-covid-19-world/

5 **Sophos, "The State of Ransomware 2020"**, May 2020 White Paper, available at: https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

6 **Safety Detectives, "Ransomware Facts, Trends & Statistics for 2021"**, 3 February 2021 blog, available at: https://www.safetydetectives.com/blog/ransomware-statistics/

EUROCONTROL Think Paper series

EUROCONTROL produces regular Think Papers aimed at decision-makers which are designed to inform, stimulate debate and present alternative approaches.

EUROCONTROL Think Paper #11 – Plane and train: Getting the balance right https://www.eurocontrol.int/sites/default/files/2021-06/eurocontrol-think-paper-11-plane-and-train-right-balance.pdf

EUROCONTROL Think Paper #10 – Flying the 'perfect green flight' https://www.eurocontrol.int/sites/default/files/2021-04/eurocontrol-think-paper-10-perfect-green-flight.pdf

EUROCONTROL Think Paper #9 – Does Radio Frequency Interference to satellite navigation pose an increasing threat to network efficiency, cost-effectiveness and ultimately safety? https://www.eurocontrol.int/sites/default/files/2021-03/eurocontrol-think-paper-9-radio-frequency-intereference-satellite-navigation.pdf

EUROCONTROL Think Paper #8 - Impact of COVID-19 on European Aviation in 2020 and Outlook 2021 https://www.eurocontrol.int/sites/default/files/2021-02/eurocontrol-think-paper-8-impact-of-covid-19-on-european-aviation-in-2020-and-outlook-2021.pdf

EUROCONTROL Think Paper #7 - Does taxing aviation really reduce emissions? https://www.eurocontrol.int/sites/default/files/2020-10/eurocontrol-think-paper-taxing-aviation-oct-2020.pdf

EUROCONTROL Think Paper #6 - Arriving on time: the passenger priority https://www.eurocontrol.int/sites/default/files/2020-01/eurocontrol-think-paper-6-arriving-on-time-passenger-priority.pdf

EUROCONTROL Think Paper #5 - Effects on the network of extra standby aircraft and Boeing 737 MAX grounding https://www.eurocontrol.int/sites/default/files/2020-01/eurocontrol-think-paper-5-737.pdf

EUROCONTROL Think Paper #4 - The aviation network - Decarbonisation issues https://www.eurocontrol.int/sites/default/files/2020-01/eurocontrol-think-paper-4-decarbonisation-en.pdf

EUROCONTROL Think Paper #3 - Cybersecurity in aviation https://www.eurocontrol.int/sites/default/files/2020-01/eurocontrol-think-paper-3-cybersecurity-aviation.pdf

EUROCONTROL Think Paper #2 - Air traffic flow management (ATFM) regulations: a power for good https://www.eurocontrol.int/sites/default/files/2020-01/eurocontrol-think-paper-2-atfm-regulation.pdf

EUROCONTROL Think Paper #1 - Fuel tankering in European skies: economic benefits and environmental impact https://www.eurocontrol.int/sites/default/files/2020-01/eurocontrol-think-paper-1-fuel-tankering.pdf

EUROCONTROL

SUPPORTING EUROPEAN AVIATION

www.eurocontrol.int