2018 10th International Conference on Cyber Conflict
CyCon X: Maximising Effects
T. Minárik, R. Jakschis, L. Lindström (Eds.)
2018 © NATO CCD COE Publications, Tallinn

Utilizing Air Traffic Communications for OSINT on State and Government Aircraft

Martin Strohmeier
Department of Computer Science
University of Oxford
Oxford, United Kingdom
martin.strohmeier@cs.ox.ac.uk

Matthew Smith
Department of Computer Science
University of Oxford
Oxford, United Kingdom
matthew.smith@cs.ox.ac.uk

Daniel Moser
Department of Computer Science
ETH Zurich
Zurich, Switzerland
daniel.moser@inf.ethz.ch

Matthias Schäfer
Department of Computer Science
University of Kaiserslautern
Kaiserslautern, Germany
schaefer@cs.uni-kl.de

Vincent Lenders
Science and Technology
armasuisse
Thun, Switzerland
vincent.lenders@armasuisse.ch

Ivan Martinovic
Department of Computer Science
University of Oxford
Oxford, United Kingdom
ivan.martinovic@cs.ox.ac.uk

Abstract: In recent times, we have witnessed a trend in which communications data is increasingly collected and made open source by the public. A prominent example is the tracking of aircraft movements using unencrypted air traffic control (ATC) communication. This paper studies the implications of such new open source aircraft datasets on the operational privacy of military and government actors. We use publicly available aircraft metadata in conjunction with unfiltered ATC communication gathered from the collaborative sensor network OpenSky. We show that using these datasets, it is possible to collect, process and analyze large numbers of movements in an automated fashion, providing insights into potentially sensitive operations.

We use movement data collected from more than 580 identified aircraft used by 100 different governments and over 6,000 military aircraft to identify operations and relationships in the real world. We also provide case studies which show that potentially sensitive information appears in these open datasets in the clear from both military and government-operated aircraft, despite attempts at encrypting some of this information.

Considering these privacy violations, we establish which countries' militaries and governments take active steps in blocking the movements of their sensitive aircraft from online tracking websites. We find that overall more than 80% of all military aircraft and 60% of all government aircraft are filtered for reasons of privacy, with significant variation between different countries.

Finally, we study the main mitigation methods available to state aircraft operators and find that all currently existing options have significant downsides, which inhibit either their usability or their effectiveness.

Keywords: *OSINT, wireless security, air traffic communication, sensor networks, privacy*

1. INTRODUCTION

Nation states and military organizations have a long tradition of intelligence gathering for purposes such as national security, counter-terrorism or counter-proliferation. The public has often held these intelligence activities in contempt, as the associated data collection methods tend to be intrusive to personal privacy. In recent times, however, we have witnessed the opposite trend in which people themselves are increasingly collecting and analyzing intelligence data concerning state and military activities.

One of the most prominent examples is the tracking of military and government aircraft movements. As active communities surrounding affordable software-defined radios have brought previously hard-to-access communications into the reach of low-skilled observers, effective privacy no longer exists on unencrypted radio channels. Many avionics communications use such channels, transmitting messages for private, military, and governmental aircraft [1], [2]. Thus far, privacy, whilst used for civil air traffic communication, is ensured solely by means of policy.

This paper studies the implications of new open source aircraft data collection initiatives on the privacy of military and government actors. We used publicly available aircraft metadata in conjunction with unfiltered air traffic communication data gathered from the collaborative sensor network, OpenSky [3]. We collected and examined messages sent via the ACARS and ADS-B protocols by military and government-operated planes over the period of one year. We show that it is possible to collect and process large amounts of data in an automated fashion, providing insights into potentially sensitive operations conducted by military and government aircraft. The novelty of this work is that such analysis is possible using open source data and is not restricted to professional intelligence services, but rather can be conducted by a wide range of actors.

In our work, we applied both large dataset analysis and case studies to illustrate the potential impact of air traffic data for intelligence purposes in several different areas. Our contributions in this paper are:

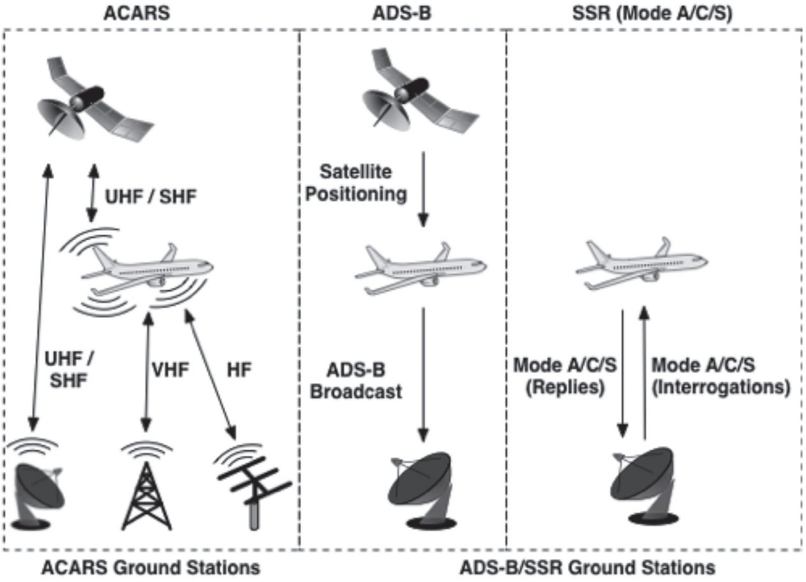
- We use movement data collected from more than 500 identified aircraft used by 100 different governments as well as over 6,000 military aircraft to identify operations and relationships in the real world.
- We provide evidence that potentially sensitive information is communicated in the clear by both military and government-operated aircraft using ACARS, despite attempts at encrypting some of this information.
- We establish which countries' militaries and governments are aware of the existence of large commercial air traffic sensor networks and take active steps to block the tracking of their sensitive aircraft on these websites.
- Finally, we examine the technical mitigation options open to state aircraft operators. Based on our analysis, we argue that all existing methods have severe drawbacks, which either inhibit their usability or their effectiveness.

In the remainder of this work, we first briefly describe the ATC technologies which we exploited in Section 2. Section 3 describes the crowdsourced system and the available public datasets which were used. Section 4 introduces our threat model, Section 5 presents the approach and the obtained results, and Section 6 analyzes the potential mitigations. Finally, Section 7 discusses the implication of our results and Section 8 concludes this paper.

2. BACKGROUND

Figure 1 provides an abstract overview and comparison of the wireless communication links of the three considered technologies, which are explained in the following sections.

FIGURE 1: REPRESENTATION OF ADS-B, SSR, AND ACARS SYSTEMS.



A. ACARS

The Aircraft Communications Addressing and Reporting System (ACARS) has been in use for over 20 years, providing a digital data link between the ground and the air [4]. It serves two main purposes: to administer ATC in order to decongest voice frequencies, and to improve efficiency for aircraft operations. As such, it can be used for safety critical procedures such as negotiating ATC clearance, as well as operational purposes including maintenance reports, engine data and weather information.

It is served over three bands: High Frequency (HF), Very High Frequency (VHF), and Satellite Communications (SATCOM). Most aircraft are equipped for all three, but may choose to not use one or more. VHF is further split into Plain Old ACARS (POA) and VHF Data Link mode 2 (VDLm2); the former is older and slower than the latter, though currently has wider coverage. SATCOM is offered by both Inmarsat and Iridium, which offer a range of packages depending on the use. ACARS messages are ASCII-based and are handled by a network provider, which maintains the network infrastructure and access to it. Two main providers exist – SITA and Rockwell Collins.

B. SSR and ADS-B

Secondary Surveillance Radar (SSR) is a cooperative ATC technology currently based on the so-called transponder Modes A, C, and S, which provide digital target information unlike traditional analog primary radar (PSR) [5]. Aircraft transponders are interrogated on the 1030 MHz frequency and reply with the desired information on the 1090 MHz channel, as shown in Figure 1. With the newer Automatic Dependent Surveillance-Broadcast (ADS-B) protocol (see Figure 1), aircraft regularly broadcast their own identity, position, velocity, and additional information such as intent, status, or emergency codes. These broadcasts do not require interrogation; position and velocity are automatically transmitted twice a second [6].

C. Relationship to other ATC Technologies

Both ADS-B/SSR and ACARS are digital technologies, which send aircraft identification data (either the ICAO address, a registration, or both) with every message, enabling surveillance and data collection on a large scale. As security was not part of the design of these systems, neither includes any cryptography which could provide confidentiality for their users.

A large part of civil ATC is conducted with analog technologies such as traditional voice communication on the VHF band. It should be noted that the features used in this work could also be obtained through analyzing such analog communication (e.g., using automatic speech recognition [7]). However, focusing on unencrypted digital technologies has the key advantage of worldwide scalability, with easy manipulation and reliable extraction of relevant information using existing crowdsourced infrastructure.

D. Aircraft Identifiers in ATC Communication

A 24-bit address assigned by the International Civil Aviation Organization (ICAO) to every aircraft is transmitted via both ADS-B/SSR and partly on ACARS (on the SATCOM/VDLm2 data links). This identifier is different to an aircraft squawk or callsign. Squawks, of which there are only 4096, are allocated locally by ATC and are not useful for continuous tracking. The callsign can be set separately through the flight deck for every flight, and can include both letters and numbers. Callsigns of private aircraft typically consist of the aircraft registration number, commercial airliners use the flight number, and military and government operators often use special call signs depending on their mission.

In contrast, the ICAO identifier is unique providing address space for 16 million assignments, and enables the continuous tracking of the movements of particular aircraft; while the transponder can be re-programmed by engineers, the identifier is not easily (or legally) changed by the pilot. These characteristics make the ICAO identifier ideal for continuous tracking over a prolonged period of time.

E. Related Work

Open source information has been enjoying increased popularity, including by private and public intelligence services, which use it for OSINT purposes [8]. Much of the related OSINT literature concentrates on social media and the wider Internet as a source for information [9], [10]. To the best of our knowledge, no academic work has examined the true effect of wireless ATC communication for this purpose. However, the authors in [11] recently analyzed the current state of the transponder equipment of a sample of military and state aircraft, which is a pre-requisite for the present work. Similarly, several works have examined the state of privacy in aviation communication and highlighted the fundamental lack of confidentiality within the ADS-B and ACARS protocols [2], [12]–[15].

This is not limited to aviation; ships of various size and purpose use Automatic Identification System (AIS) to report their position in a similar way to ADS-B. AIS also suffers from basic security problems, much like ADS-B [16]. In recent years, its clear-text broadcast nature has been used to track illegal fishing [17] or monitor oil movements around the world [18].

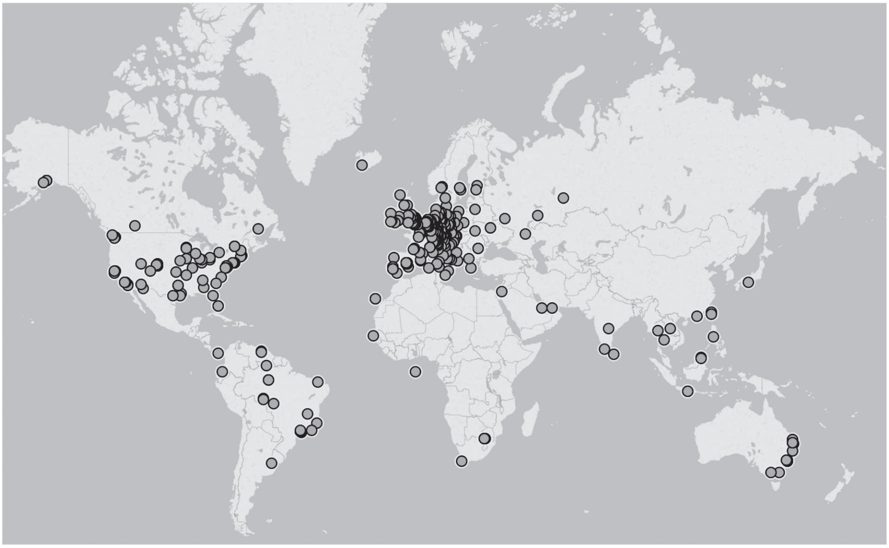
3. OVERVIEW OF PUBLICLY AVAILABLE AVIATION DATA

In this section, we present the data collection process. We first discuss the OpenSky Network as a representative example of a global sensor network available to passive threat actors. Following this, we analyze the potential sources from which to obtain metadata information about the observed aircraft. Finally, we illustrate the dataset that we use for our analysis in this paper.

A. The OpenSky Network

OpenSky is a crowdsourced network which is used as proof-of-concept for our OSINT collection. As of January 2018, the OpenSky Network consisted of 590 registered and about 450 anonymous sensors streaming data to its servers. Registered sensors are those operated by active members of the OpenSky Network community, and the operators of anonymous sensors are unknown. The network has currently received and stored over 4 trillion ATC messages, adding over 15 billion messages by more than 50,000 different aircraft every day.

FIGURE 2: A MAP OF SENSORS REGISTERED TO THE OPENSKY NETWORK (JANUARY 2018).



B. Public Metadata Sources

Besides the pure movement data, we require metadata about the aircraft to contextualize their behavior for OSINT purposes. We discuss the available sources of aircraft and airport metadata below.

1) Aircraft Metadata

Several public data sources exist which provide aircraft meta-information based on different identifiers. These identifiers include aircraft registration or the unique 24-bit ICAO Mode S transponder address. The data usually includes type and the owner or operator, which can then be used for further in-depth analysis and stakeholder identification. We used several of these third-party databases in our analysis of aircraft metadata:

- The plane spotting and aviation community actively maintains and shares database files with spotted aircraft using the BaseStation format for this [19].
- Junzi Sun maintains a database of aircraft seen on Flightradar24. The version used in this work is of 24 months and amounting to 136,637 rows [20].
- Aircraft registered in the US are logged on a daily-updated FAA database containing owner records. This is online and available for download, but excludes any sensitive owner information. Even so, the data set used for this work contained 312,162 records in December 2017 [21].

Besides these offline databases, which amounted to data of more than 2 million aircraft, we used several online sources to identify and verify aircraft as being operated by the government and military. These sources include the two major private flight tracking websites FlightAware [22] and Flightradar24 [23] and the popular database website airframes.org. Further leads and insights on more obscure aircraft identifications can also be gained on social media (Twitter, Flickr), a Wikipedia article on the topic [24], specialized aviation forums and aircraft photo websites such as JetPhotos [25].

2) Airport Metadata

To relate the actual destinations (countries and cities) of the tracked aircraft, we obtained the open airport database from Openflights.org [26]. As of December 2017, it contained 12,057 different airports around the globe, including name, ICAO and IATA (International Air Transport Association) short codes and precise location.

C. Overview of the Analyzed Datasets

For our work, we created two ADS-B datasets for further analysis, one for government aircraft and one for military aircraft. For government movements, we looked at a period of one year from 1 July 2016 to 30 June 2017, while for the significantly larger military dataset, we considered the period of one month in April 2017 for a more straightforward analysis. Regarding the ACARS data, we were able to obtain separate datasets for the three data links spanning 9 months in total, which we combined to analyze both government and military aircraft together.

1) Government Aircraft Movements

Using the public data sources described above, we created a list of 590 verified government aircraft from 113 different states. Table 1 shows the distributions of these aircraft and their operating governments per world region and whether OpenSky has tracked their position using ADS-B in the observed time frame of one year.

TABLE 1: OVERVIEW OF KNOWN AND TRACKED GOVERNMENTS IN THE DATASET.

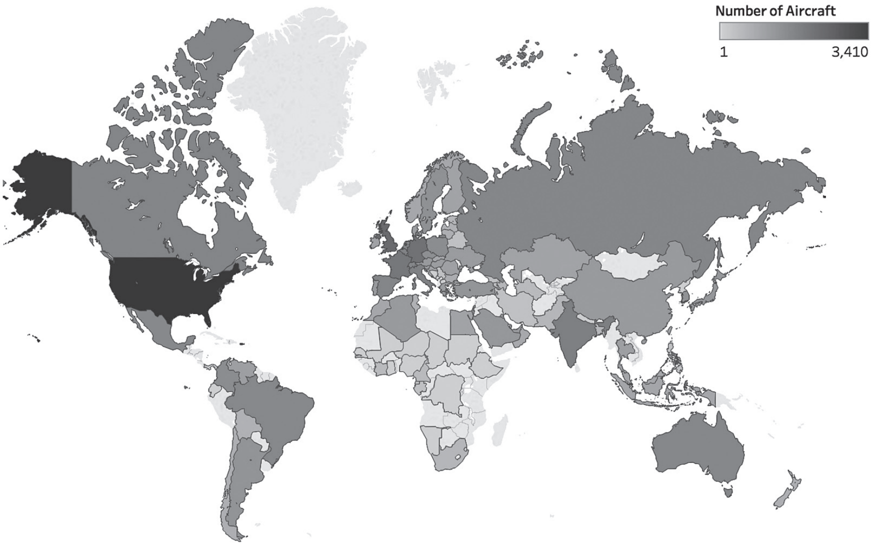
	Europe	Americas	Africa	Asia	Oceania	Mid. East
A/C	172	78	119	79	8	134
Tracked A/C	157	73	76	66	7	113
Gov’s	33	14	33	18	3	12
Tracked Gov’s	33	13	30	16	3	11
Flights	8,915	1,775	399	706	248	2,115

2) Military Aircraft Movements

Unlike government aircraft, military aircraft are not limited to those contained in the public data sources. Air forces typically reserve a block in their country's ICAO ID range for military transponders; for example, identifiers used by the US Air Force tend to begin with 'AE'. Any aircraft with an ICAO ID matching this pattern can be identified as being used for military purposes. Exploiting this information, we can identify aircraft not in our public metadata sources – including the country and operator – though in these instances we lack additional meta information such as aircraft type. Overall, this approach resulted in a list of about 520,000 potential military aircraft transponder IDs.

In order to analyze the movements of military aircraft, we combined this list with all 1090 MHz downlink transponder transmissions recorded by OpenSky in April 2017. In this set of about 290 billion transmissions, we detected 6,024 unique military aircraft that broadcast unencrypted Mode S or ADS-B messages within range. Figure 3 shows the distribution of countries these aircraft were registered to.

FIGURE 3: DISTRIBUTION OF MILITARY AIRCRAFT SEEN IN OPENSKY BY ORIGIN COUNTRIES (APRIL 2017).



3) ACARS Collection

We further used the data from an ACARS receiver set up for the OpenSky Network in Central Europe, which collected 2,760,141 messages from 9,924 different aircraft on three data links (SATCOM, POA and VDLm2) over a period of 2 months for SATCOM and 7 months for VHF and VDLm2. While this ACARS data is not currently open source, there are existing platforms such as AVDelphi [27] which make such ACARS data publicly available.

In this dataset, we received 6,149 ACARS messages sent by 200 unique government aircraft and 24,923 messages sent by 438 aircraft operated by the military. The majority of messages from these groups were received via SATCOM (60% for the government and 97% for the military), indicating a strong preference for this data link.

4. THREAT MODEL

We consider a purely passive attacker as described in [14]. In our model, these are interested observers who exploit the open nature of air traffic communication protocols to obtain open source intelligence. This threat actor does not actively interfere with any of the observed technologies. Instead, they use public tracking services such as FlightRadar24 or ADS-B Exchange [28] in conjunction with public metadata sources to gather intelligence about government or military aviation movements. A more powerful version of this threat actor uses their own network of cheap SDR receivers to gather an unfiltered air traffic picture in real time which can be stored for historic analysis. This enables them to listen to a wider range of technologies such as ACARS and is within the capabilities of practically any determined attacker today [2].

5. EXPLOITING OPEN SOURCE ATC DATA FOR INTELLIGENCE PURPOSES

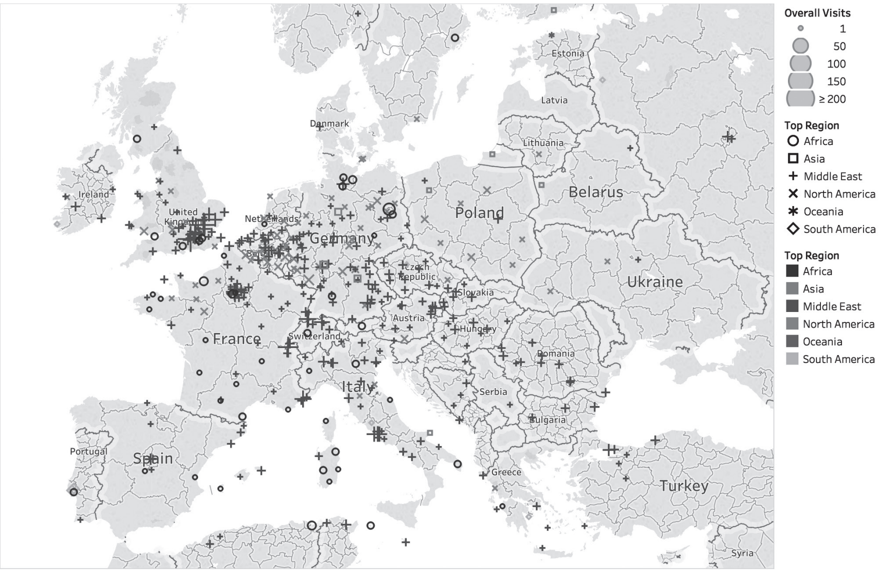
In this section, we provide examples of the type and scope of intelligence that can be gleaned from ATC data. We first discuss the government dataset, followed by the military dataset and an exemplary case study of a government jet operated by the military.

A. Government

We assume that governments are less secretive by nature than the military. At least in democratic countries, the electorate should be able to hold the government accountable, which requires an element of transparency. Whilst there are instances in which government transport might need to be kept private momentarily, most day-to-day government operations may not be secret in order to provide said accountability. However, this is evidently not true for all government missions from all countries. Thus, in the following, we analyze the quantitative possibilities a passive observer has with regards to the tracking of government aircraft.[1] Figure 4 illustrates the scope of our observations by showing the number and distributions of non-European government aircraft in Europe during the observation period.

[1] Analyzing the reasons and motivations for specific relationships and government movements is out of the scope of this paper.

FIGURE 4: AIRCRAFT USED BY NON-EUROPEAN GOVERNMENTS VISITING EUROPE DURING JULY 2016 – JUNE 2017.



1) Meetings

During the one-year observation period, we observed 164 meetings of groups of at least three aircraft from different governments at the same destination.[2] As would be expected, the majority of these meet-ups happened at the major European capitals: Paris (44 times), Brussels (23), Rome (10), London (9), and Berlin (8).

The largest meetings with the most participants are naturally large global summits, such as the World Economic Forum (21 tracked governments), the Nuclear Security Summit (20), or the Munich Security Council (13). While these gatherings are not secret, their list of participants is not always published, and if it is, it may not be complete. Indeed, we found several government aircraft which landed in the vicinity of the World Economic Forum that were absent from the official list of participants [29].

While large multinational meetings such as the EU or NATO summits are well known, most smaller gatherings of three or four countries are not easily attributable. We acknowledge that every such occurrence may be due to simple chance, however, they can provide a heuristic starting point for further investigations.

2) Relationships

While there is a possibility of coincidence for every time that government aircraft are in the same location, this becomes much less likely for the consistently high

[2] We define a potential multilateral meeting as three or more aircraft, which have landed within 50 km range within the same 48h period and not left again.

numbers of meetings we have seen over a prolonged time frame for many government pairs. Table 2 shows the top relationships between all tracked government aircraft in OpenSky's sensor range. The top three relationships have seen two governments at the same airport for 133 times (France/Saudi Arabia), 127 times (France/Morocco), and 102 times (Dubai/Qatar), respectively. Overall, we detected 7,106 pairwise meetings over 994 different relationships with a median of 3 meetings/relationship.

TABLE 2: RELATIONSHIPS BETWEEN MOST SEEN GOVERNMENTS BASED ON ADS-B DATA.
Note: We counted the Emirates of Dubai and Abu Dhabi as separate entities due to their prevalence.

	Qatar	Saudi Arabia	US	UK	Nether-lands	Morocco	Total
France	65	133	4	4	13	127	346
Germany	35	19	91	20	76	10	251
Dubai	102	23	17	71	9	2	224
Belgium	9	6	38	32	72	-	157
Bahrain	49	16	11	46	5	8	135
Abu Dhabi	28	40	33	13	2	13	129
Total	288	237	194	186	177	160	

Besides looking at the spatio-temporal correlation of two or more government aircraft, we can also investigate the most popular destinations of any single aircraft over time to infer public or private relationships of the operator. Table 3 lists the most visited destinations by the top eight observed governments. Considering OpenSky's core coverage area in Europe and the US, it is unsurprising that the most observed government aircraft are those from European countries and the US. Their preferred foreign destinations reflect the close diplomatic ties between these countries, or special commitments as in the case of Slovakia's EU presidency (Jul-Dec 2016), which necessitated a large amount of flights to the EU's headquarters in Brussels.

TABLE 3: MOST POPULAR NON-DOMESTIC DESTINATION COUNTRIES
AND AIRPORTS OF THE EIGHT MOST SEEN GOVERNMENTS.
Note: Numbers in brackets indicate the number of times an aircraft was observed visiting the destination. Note, that country and airport are measured separately and can be unrelated.

Government (seen)	Top Destination Country	Top Destination Airport
Germany (2,345)	United States (57)	Washington (44)
United States (1,221)	Germany (48)	Brussels (9)
Russia (972)	Germany (54)	Rome (16)
Italy (740)	Belgium (17)	Brussels (15)
France (717)	Germany (19)	Basel (9)
Qatar (554)	United Kingdom (148)	London (75)
Czech Republic (536)	Germany (28)	Brussels (8)
Slovakia (472)	Belgium (39)	Brussels (32)

3) ACARS Analysis

Of the government aircraft considered in this section, 29.9% were observed sending ACARS messages. This in turn means that they often leak both their existence (their identification) and their intent (where they are going).

In Table 4 we see the position leakage for government aircraft as a result of using ACARS across the different subnetworks. Explicit position is simply a set of coordinates, whereas indicated position is when the aircraft is sending messages which reveal the area it is in. These could be airport information requests, for example. Note that we see at least 20% of government aircraft leak indicated position leakage on each link. Some of these aircraft were observed transmitting clear text e-mail messages via the ACARS satellite link. The nature of these messages was mainly flight status related, but some included names and e-mail addresses of fleet operators or government employees.

TABLE 4: POSITION-RELATED MESSAGES SENT OVER ACARS BY GOVERNMENT AIRCRAFT (AC). PERCENTAGES ARE OF ALL GOVERNMENT AIRCRAFT SEEN ON THAT SUB-NETWORK.

Sub-network	Number of Messages	Number of Aircraft	Explicit Position	Number of Aircraft	Indicated Position	Number of Aircraft
POA	1,491	66	169	26 (39.4%)	47	15 (22.7%)
VDLm2	275	54	31	13 (24.1%)	11	11 (20.4%)
SATCOM	3,654	117	218	13 (11.1%)	480	41 (35.0%)

B. Military

Compared to the identified government aircraft, military aircraft are much less likely to be equipped with ADS-B. Nonetheless, of the 6,024 unique military aircraft observed in April 2017, 42.9% were equipped with ADS-B and broadcast their positions at least some of the time. This varies greatly between different aircraft categories and also between countries as previous research has shown [5], [11]. Compared to the government aircraft, clusters of military aircraft on the ground are not as obviously insightful to an observer, as most operational missions are normally airborne and do not require landing. Yet, visits to foreign countries are interesting nonetheless and can support analyzes of military strategy and troop movements.

To prove that valuable OSINT can be collected on military aircraft, we offer some additional approaches: we analyze the ACARS messages sent by these aircraft and also look at the prevalence of military UAV movements in the dataset.

1) ACARS Analysis

Of all military aircraft we investigated, we observed 462 or 7.7% sending ACARS messages. Table 5 shows the distribution of these messages by subnetwork. It illustrates that satellite communication is by far the most popular data link, making up about 98% of all traffic received by aircraft of this category. One might speculate that this preference indicates concern about the operational security of the ground-based links; however, the difficulty of eavesdropping on SATCOM with software-defined radios is broadly similar in practice.

As can be seen, 118 of the observed 462 military aircraft explicitly sent their position in the clear using ACARS at least once. Furthermore, 269 aircraft broadcast data that would give away their position by, for example, requesting weather reports for their destination airport.

TABLE 5: POSITION-RELATED MESSAGES SENT OVER ACARS BY MILITARY AIRCRAFT (AC). PERCENTAGES ARE OF ALL MILITARY AIRCRAFT SEEN ON THAT SUB-NETWORK.

Sub-network	Number of Messages	Number of Aircraft	Explicit Position	Number of Aircraft	Indicated Position	Number of Aircraft
POA	305	19	19	6 (31.6%)	26	7 (36.8%)
VDLm2	165	25	25	3 (12.0%)	9	4 (16.0%)
SATCOM	24,124	418	1,183	109 (26.1%)	2,011	258 (61.7%)

2) UAV Detection

Unmanned Aerial Vehicles (UAV) are fast becoming a major presence in civil airspace, and many UAVs are operated by governments or the military. Some of these drones carry ADS-B or Mode S transponders to cooperate with ATC and detect and avoid other aircraft. Hence, their presence and movements are visible to flight trackers and ATC receivers in general.

Using the metadata described in Section 3, we obtained the identifiers of 74 military-operated UAVs. We analyzed the complete historical data of OpenSky to find evidence of these Mode S and ADS-B-equipped UAVs, which returned sightings for 31 or 41.9% of the complete set.

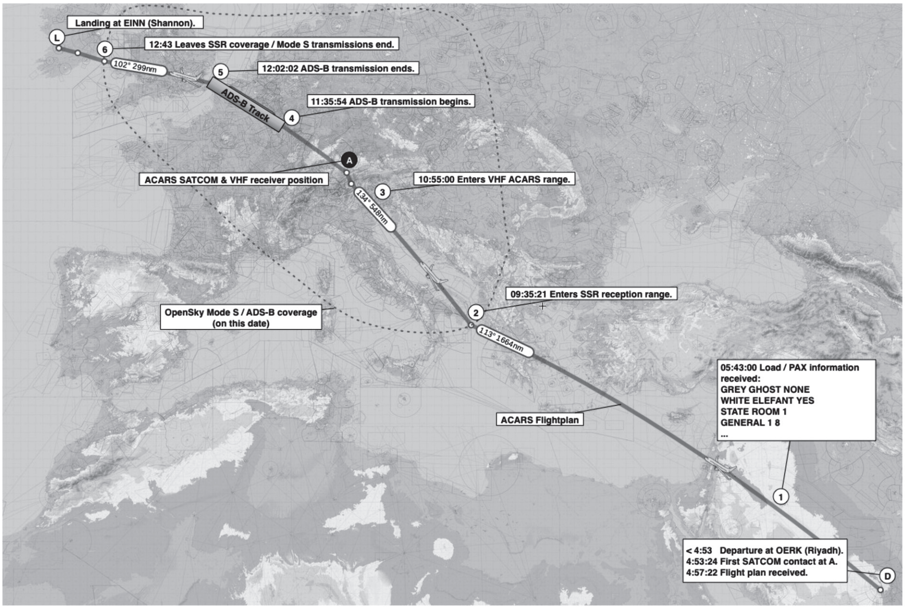
“ADS 95 Ranger Drones” operated by the Swiss Air Force to patrol borders and for general surveillance purposes provided the most striking evidence of such UAVs. Overall, we encountered messages from 14 of these drones, which use Mode S to communicate their identification and altitude.

Additionally, we received ATC messages from four General Atomics MQ-9 Reaper UAV and 10 Northrop Grumman RQ-4 Global Hawks. Some of these sightings have also been reported in aviation and military blogs on the Internet, showing that gathering OSINT by eavesdropping on air traffic communication is becoming more and more widespread [30].

C. Case Study

Figure 5 provides a case study on typical OSINT that can be gleaned from a government flight operated by a country's air force. It illustrates that, even with limited sensor coverage, the pieces put together via different technologies can provide a detailed picture of the whole flight.

FIGURE 5: A CASE STUDY OF OPEN SOURCE FLIGHT INFORMATION OBTAINABLE ABOUT A GOVERNMENT FLIGHT.


Landing at EINN (Shannon).
L
6
12:43 Leaves SSR coverage / Mode S transmissions end.
102° 299nm
5
12:02:02 ADS-B transmission ends.
ADS-B Track
11:35:54 ADS-B transmission begins.
4
A
ACARS SATCOM & VHF receiver position
3
10:55:00 Enters VHF ACARS range.
134° 548nm
2
09:35:21 Enters SSR reception range.
OpenSky Mode S / ADS-B coverage (on this date)
113° 1664nm
05:43:00 Load / PAX information received:
GREY GHOST NONE
WHITE ELEFANT YES
STATE ROOM 1
GENERAL 1 8
...
ACARS Flightplan
1
< 4:53 Departure at OERK (Riyadh).
4:53:24 First SATCOM contact at A.
4:57:22 Flight plan received.
D

At the time of flight in December 2016, the OpenSky Network had comprehensive ADS-B and SSR coverage in the area within the dotted red line. A satellite ACARS receiver was placed centrally within this area, which was able to pick up the uplink part of the satellite communication; i.e., the one sent out by aircraft and addressed to the ground network.

Figure 5 shows the complete flight from the departure (D) in Riyadh to the landing (L) in Shannon. Around departure, the flight plan was sent out via ACARS by the aircraft and picked up by the receiver in Europe, detailing the precise route and waypoints the aircraft was planning to take. Several other ACARS messages containing potentially sensitive information about load and passengers were also picked up within an hour of departure (1). At (2), the aircraft reached the ground sensor coverage of OpenSky, which received 18,348 messages, providing the altitude of the aircraft and positional information within the range of the receivers. At (3) it entered the range of the ground ACARS receiver, which captured all information provided via this channel only. While still at cruising altitude between (4) and (5), the aircraft activated its ADS-B transponder, broadcasting its exact position, call sign and velocity. It switched off the positional broadcasts again before leaving OpenSky's SSR range at (6) during the approach to Shannon (as verified by the Mode S altitude messages).

This behavior shows that ADS-B can and is turned on and off by military-operated aircraft. Turning it on at least sometimes indicates a general willingness to use ADS-B and, by doing so, facilitate tracking with civil surveillance technologies. However, turning it on only at cruising altitude and turning it off again before descending most likely aims at concealing the airport of departure and/or arrival.

6. EXISTING MITIGATION OPTIONS

There are several potential mitigation options for both government and military aircraft to prevent the information leakages discussed in the previous section. Here, we analyze the effectiveness of blocking information from web trackers, the use of pseudonyms, encryption, and attempts at forgoing civil ATC communication completely.

A. Web Tracker Blocking

One approach to limiting the privacy leaks of aircraft tracking is through block lists, which instruct the companies operating aircraft tracking websites to hide the aircraft on the list from public view. The most popular example of such a list is the Blocked Aircraft Registration Request (BARR) program, originally run by the National Business Aviation Association (NBAA) but now maintained by the FAA [31]. A BARR block places a restriction on the feed of aircraft send out by the FAA, which is used as a source by flight trackers. Table 6 shows that in our sample 85.0% of all military aircraft and 61.6% of all government aircraft were being filtered on the most popular flight tracking website (FlightRadar24). This indicates a clear awareness of a privacy impact through flight tracking by a majority of these state actors.

TABLE 6: PERCENTAGE OF IDENTIFIABLE MILITARY AND GOVERNMENT AIRCRAFT BLOCKED FROM POPULAR WEB TRACKERS. PERCENTAGES ARE OF THE NUMBER OF AIRCRAFT TRACKED.

		Europe	Americas	Africa	Asia	Oceania	Mid. East
Gov.	Tracked	157	73	76	66	7	113
	Blocked	93 (59.2%)	61 (83.6%)	38 (50.0%)	31 (47.0%)	6 (85.7%)	74 (65.5%)
Mil.	Tracked	1,851	3,646	45	268	73	78
	Blocked	1,359 (73.4%)	3,418 (93.7%)	36 (80.0%)	157 (58.6%)	38 (52.1%)	56 (71.8%)

Despite the popularity of the blocking approach, it is wholly ineffective against our threat model. As illustrated in the previous section, any passive actor with control over the raw data obtained from ATC sensors has full access to an unfiltered view of the airspace, including any government and military aircraft. Yet, for unknown reasons, 18 of all 106 tracked governments (17%) do not ask any of their aircraft to be blocked, forgoing even these basic mitigations.

B. Pseudonyms

A more comprehensive solution to the described tracking problem consists of pseudonymous identifiers that thwart an attacker's ability to correlate flight tracks with each other and with a specific aircraft.

For aircraft call signs, this is generally feasible for all considered technologies; changing a call sign before or during a flight is technically straightforward and often legally possible. For example, there are online services such as FltPlan.com [32], which offer randomized call signs to private operators, and both commercial and military operators are known to change their call signs regularly depending on an aircraft's mission. For the ICAO 24-bit identifier, the case is very different, as the pilot or operator cannot easily change it. The ICAO allows for a manual change in case of sensitive missions [33], yet we do not see this option in wide operation by government or military aircraft as our results in the previous section show.

ADS-B can alternatively be served over a newly developed data link, the Universal Access Transceiver (UAT), which offers a built-in privacy mechanism that generates a non-conflicting, random, temporary ICAO 24-bit identifier to avoid third-party tracking. However, it has been shown that this implementation is flawed and does not successfully disable aircraft tracking over time [34]. Furthermore, it is only in use by general aviation aircraft within the US airspace and as such not a quick fix for any other operator.

Finally, regardless of identifier, it has been shown that it is possible to fingerprint ADS-B transponders on the physical and link layer levels, which, in sufficient granularity, would circumvent even properly implemented pseudonyms [35].

C. Encryption

As mentioned previously, the use of encrypted communication would be the most effective countermeasure to the described data leakages. Unauthorized access to both movement data and other information can be stopped through the use of symmetric or asymmetric encryption as it is in current use in many wireless communication technologies.

As with any distributed security solution, implementing a public-key infrastructure is costly and requires thoughtful, security-conscious design. Especially in the case of aircraft, which must be able to communicate with unexpected ground stations, keeping credentials up-to-date for all communications partners is a challenge. Secure ACARS, available since 2001 [36], provides such an option, and not only to military and government operators. However, we have not seen Secure ACARS in use in the wild; in our data set of 1,749,142 messages from all three data links, we never recorded a single message of this type.[3] We speculate that the fact that it comes at a surcharge to the ACARS service impedes its adoption.

This assumption is supported by the fact that there are several proprietary encryption solutions in use for ACARS, which are not standardized, but potentially come at a cheaper running cost. Unfortunately, many such solutions are insecure, quickly broken and provide no more security than clear-text messages against any interested adversary. One such example is discussed by Smith et al. [12], who show that it is in wide use even in government and military aircraft. In our dataset, we found that 1.78% of the observed military and 11.36% of the observed government aircraft used this obfuscation method, a serious lapse of operational security. In principle, however, there is no fundamental obstacle to developing a secure proprietary ACARS solution for exclusive use by a state's sensitive aircraft as long as compatibility with the existing system is ensured.

While ACARS messages can be encrypted by the user's choice, this is not possible for both ADS-B and SSR. As has been analyzed previously, the current technological lock-in does not allow for a quick encryption solution for these protocols [15]. While there are military equivalents to civil SSR and ADS-B in use and under development (NATO STANAG 4193, SSR Modes 4 and 5), due to obvious secrecy requirements, very few details are publicly available. As Mode 5 is believed to provide full confidentiality using strong encryption, its use would indeed fully mitigate the information leakage of ATC movement data. However, due to the lack of independent scrutiny, it is not possible to make any reliable statements on the security of the system.

Unfortunately, even for those military operators with access to encrypted protocols, the preference of civil ATC authorities for open systems and maximum compatibility precludes any proprietary solutions as long as they are flying in civil airspace [14]. In short, all operators must be aware that using any current civil ATC technology will leak information immediately and widely.

D. Switch off civil ATC communication

The final mitigation option for military and government aircraft operators is to not use civil ATC communications. For ACARS, this is fairly simple, as it is not a required

[3] A distinct set of message labels is reserved in the ACARS standard for Secure ACARS messages, enabling us to detect their presence even where it is not possible to decrypt them.

technology in controlled airspace and some operators choose to forgo ACARS for cost reasons, including entire airlines. Yet, as shown above, many sensitive aircraft use unencrypted ACARS, presumably for operational reasons.

When considering ADS-B and SSR, the picture is much more complex. Aircraft are still not required to broadcast their precise position using ADS-B. As long as the technology is not mandated for state aircraft in (mostly Western) civil airspaces, there are many operators who choose to delay the upgrade in the first place for reasons of cost, convenience, or indeed privacy. Overall, only around 6.7% of all government aircraft but 57.1% of the military aircraft in our sample did not yet use ADS-B, which is in line with previous research [11]. Naturally, this is only a solution in the very short term and the consequences of upgrading will have to be addressed in the very near future.

7. DISCUSSION

We have demonstrated that tracking aircraft using civil ATC systems allows us to glean significant intelligence that the aircraft operators or users might not be interested in sharing. Indeed, with a relatively low level of skill and equipment used by a purely passive attacker, this combination of public data sources can reveal much more than where an aircraft is. Even though options exist to mitigate the problem, they are largely ineffective against a reasonably persistent attacker. Naturally, this generates some recommendations for how to improve the state of privacy in aviation. In the short term, regulation provides a possible key to allowing relevant actors to protect their privacy. Governments would have to legally restrict and regulate those entities (private and commercial) that are sharing data about aircraft movements for which a reasonable effort at privacy has been made. This would need to be a more concerted effort than the BARR scheme, which is, to some extent, opt-in.

In the longer term, technical solutions should be developed to provide guarantees of privacy. For example, a robust pseudonym system would go a long way to limiting the ability to track aircraft over time, similar to the concept of Temporary Mobile Subscriber Identity (TMSI) in cellular networks. There is no critical technical or procedural need to have a consistent, publicly known identifier for aircraft — there is in fact evidence of aircraft being prescribed alternative ICAO identifiers by the authorities in situations such as sensitive military flights [33]. Doing away with the inflexible current system in favor of a more transient one would in turn de-correlate consecutive flights by a given aircraft. This measure alone would greatly reduce the impact of ATC-based flight tracking.

Hence, in our opinion, the only way to effectively create the opportunity for privacy in ATC systems is through the combination of technical and regulatory measures. Regulatory measures can cover the case of data generated by state entities, but technical measures are needed to stop passive observers from easily collecting significant amounts of data.

As discussed in [14], there is currently a preference for open systems in aviation, but this is not necessarily wise if a good level of security and privacy is required. Parallels can be drawn to the creation of the Internet in that, initially, open systems allowed easy integration and global interaction between different networks. However, in the longer term, malicious parties have resulted in both a desire and need for securing all communications. Aviation networks carry bigger safety risk, so should aim for similar, if not greater, levels of security than the Internet currently uses.

8. CONCLUSION

The findings we have presented in this work conclusively prove that it is possible to collect, process, and ultimately exploit, a trove of open source air traffic communication data for intelligence purposes. While examining all potential use cases for such data is out of the scope of a single paper, we believe that our proof of concept is sufficient to raise awareness of the issue among all concerned stakeholders.

It has also become clear that traditional ways of protecting the privacy of aircraft owners are all but obsolete in the era of cheap software-defined radio receivers, and relying on them should be done with extreme caution. Military and nation state actors have superior means and resources to protect their operational privacy and security in some cases, as evidenced by the existence of encrypted communications solutions. However, the requirement to be able to communicate with civil ATC negates at least some of this advantage as illustrated in this work. Consequently, only a change to those civil communication technologies will lead to comprehensive privacy improvements for those who seek it. In the meantime, many actors will be able to exploit the openly available information gained in this domain for their purposes.

REFERENCES

[1] M. Strohmeier, M. Smith, V. Lenders, and I. Martinovic, “The Real First Class? Inferring Confidential Corporate Mergers and Government Relations from Air Traffic Communication,” in *IEEE European Symposium on Security and Privacy (EuroS&P)*, 2018.

[2] M. Smith, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic, “Analyzing Privacy Breaches in the Aircraft Communications Addressing and Reporting System (ACARS),” no. arXiv:1705.07065v1 [cs.CR], 2017.

[3] M. Schäfer, M. Strohmeier, V. Lenders, I. Martinovic, and M. Wilhelm, "Bringing up OpenSky: A large-scale ADS-B sensor network for research," in *Proceedings of the 13th International Symposium on Information Processing in Sensor Networks (IPSN)*, 2014, pp. 83–94.

[4] R. T. Oishi and A. Heinke, "Air-Ground Communication," in *Digital Avionics Handbook*, Third., C. R. Spitzer, U. Ferrell, and T. Ferrell, Eds. Taylor & Francis Group, 2015, p. 2.1-2.3.

[5] C. R. Spitzer, U. Ferrell, and T. Ferrell, *Digital Avionics Handbook*, 3rd ed. CRC Press, 2014.

[6] RTCA Inc., "DO-262 - Minimum Operational Performance Standards (MOPS) for 1090 MHz Automatic Dependent Surveillance - Broadcast (ADS-B)." 2000.

[7] D. Hoffman and S. Rezchikov, "Busting the BARR: Tracking 'Untrackable' Private Aircraft for Fun & Profit," in DEF CON 20, 2012.

[8] R. Steele, "Open Source Intelligence," in *Handbook of Intelligence Studies*, Routledge, 2007, pp. 129–147.

[9] D. Gritzalis and V. Stavrou, "Exploiting Open Source Intelligence capabilities for the benefit of the Hellenic Air Force," in *4th Air Power Conference*, 2016.

[10] C. Weinbaum, S. Berner, and B. McClintock, "SIGINT for Anyone - The Growing Availability of Signals Intelligence in the Public Domain." 2017.

[11] M. Schäfer, M. Strohmeier, M. Smith, M. Fuchs, V. Lenders, M. Liechti, and I. Martinovic, "OpenSky Report 2017 : Mode S and ADS-B Usage of Military and other State Aircraft," in *Digitial Avionics Systems Conference (DASC), 2017 IEEE/AIAA 36th*, 2017.

[12] M. Smith, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic, "Economy Class Crypto: Exploring Weak Cipher Usage in Avionic Communications via ACARS," in *21st International Conference on Financial Cryptography and Data Security*, 2017.

[13] K. Sampigethaya and R. Poovendran, "Security and privacy of future aircraft wireless communications with offboard systems," in *Third International Conference on Communication Systems and Networks (COMSNETS 2011)*, 2011, pp. 1–6.

[14] M. Strohmeier, M. Smith, M. Schäfer, V. Lenders, and I. Martinovic, "Assessing the Impact of Aviation Security on Cyber Power," in *8th International Conference on Cyber Conflict (CyCon)*, 2016, pp. 223–241.

[15] M. Strohmeier, V. Lenders, and I. Martinovic, "On the Security of the Automatic Dependent Surveillance-Broadcast Protocol," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 2, pp. 1066–1087, 2015.

[16] M. Balduzzi, K. Wilhoit, and A. Pasta, "A Security Evaluation of AIS," 2014.

[17] Image Sat International (iSi), "Optimizing fish production with space intelligence," 2017. [Online]. Available: https://www.imagesatintl.com/optimizing-fish-production-space-intelligence/. [Accessed: 18-Dec-2017].

[18] S. Madani and L. Ward, "TankerTrackers.com," 2017. [Online]. Available: http://tankertrackers.com. [Accessed: 18-Dec-2017].

[19] D. Taylor, "Databases," *Planeplotter*, 2016. .

[20] J. Sun, "World Aircraft Database," 2017. [Online]. Available: http://junzisun.com/adb/. [Accessed: 11-Dec-2017].

[21] Federal Aviation Administration, "Aircraft Registry - Releasable Aircraft Database Download," 2017. [Online]. Available: https://www.faa.gov/licenses_certificates/aircraft_certification/aircraft_registry/releasable_aircraft_download/. [Accessed: 11-Dec-2017].

[22] FlightAware, "FlightAware," 2017. [Online]. Available: https://www.flightaware.com/. [Accessed: 06-Mar-2017].

[23] Flightradar24 AB, "Flightradar24," 2017. [Online]. Available: https://www.flightradar24.com. [Accessed: 06-Mar-2017].

[24] "Air Transports of Heads of State and Government," *Wikipedia*, 2017. [Online]. Available: https://en.wikipedia.org/wiki/Air_transports_of_heads_of_state_and_government. [Accessed: 11-Dec-2017].

[25] O. A. Saffe and S. De Rudder, "JetPhotos," 2017. [Online]. Available: 2017-12-11.

[26] J. Patokallio, "OpenFlights.org," 2017. [Online]. Available: https://openflights.org. [Accessed: 11-Dec-2017].

[27] D. R. Crocker, "AvDelphi," 2018. [Online]. Available: https://www.avdelphi.com/. [Accessed: 06-Jan-2018].

[28] D. Streufert, "ADS-B Exchange," 2017. [Online]. Available: https://www.adsbexchange.com/. [Accessed: 11-Dec-2017].

[29] World Economic Forum, "World Economic Forum Annual Meeting - List of Public Figures," Davos-Klosters, 2017.

[30] D. Cenciotti, "U.S. Air Force RQ-4 Global Hawk drone flew over Ukraine with transponder turned on for everyone to see," *The Aviationist*, 2016. [Online]. Available: https://theaviationist.com/2016/10/18/u-s-air-force-rq-4-global-hawk-drone-flew-over-ukraine-with-transponder-turned-on-for-everyone-to-see/. [Accessed: 18-Dec-2017].

[31] National Business Aviation Association, “Block Aircraft Registration Request (BARR) Program,” 2011. [Online]. Available: https://www.nbaa.org/ops/security/barr/background/. [Accessed: 24-Oct-2017].

[32] FltPlan.com, “Flying in Private,” 2017. [Online]. Available: https://flttrack.fltplan.com/FltPlanInfo/DCMCallSigns.htm. [Accessed: 13-Dec-2017].

[33] Directorate of Air Traffic Management, “Automatic Dependent Surveillance-Broadcast (ADS-B),” New Delhi, 2014.

[34] K. Sampigethaya, S. Taylor, and R. Poovendran, “Flight Privacy in the NextGen: Challenges and Opportunities.” 2013.

[35] M. Leonardi, L. Di Gregorio, and D. Di Fausto, “Air Traffic Security: Aircraft Classification Using ADS-B Message’s Phase-Pattern,” *Aerospace*, vol. 4, no. 4, p. 51, 2017.

[36] A. Roy, “Secure aircraft communications addressing and reporting system (ACARS),” *20th Digital Avionics Systems Conference*, vol. 2, p. 7A2/1--7A2/11 vol.2, 2001.