IAI
Istituto Affari Internazionali

ISSN 2280-6164

DOCUMENTI IAI 15 | 23E - DECEMBER 2015

The Defence of Civilian Air Traffic Systems from Cyber Threats

by Tommaso De Zan,

Fabrizio d'Amore and Federica Di Camillo

ABSTRACT

The use of ICT in civil aviation has increased exponentially in the last years. Digitalisation and the technological tools and systems often connected to the internet constitute serious risks for aviation cyber security. The Government Accountability Office (GAO) has recently stated that air traffic management and control (ATM/ATC) vulnerabilities could be used to undermine national security. Against this backdrop, several related questions arise: what technologies do air traffic management and control systems rely on? Are these systems vulnerable? Which actors could pose a threat to these systems? Do they have the technological skills to conduct attacks that could compromise them? The low technical skills of the non-state actors analysed in this research, the cyber security countermeasures adopted by ENAV and the preventive activities conducted by Italian authorities make the risk for Italian ATM/ATC systems low. However, it is necessary to keep a high level of attention and awareness on possible future developments of the cyber threat.

keywords

Aviation security | *Cyber security* | *Italy*

The Defence of Civilian Air Traffic Systems from Cyber Threats

by Tommaso De Zan, Fabrizio d'Amore and Federica Di Camillo*

* Tommaso De Zan is Junior Researcher in the Security and Defence programme at the Istituto Affari Internazionali (IAI). Fabrizio d'Amore is Associate Professor in the Department of Computer, Control, and Management Engineering (DIAG) "Antonio Ruberti" at the Sapienza University of Rome and member of the Research Center of Cyber Intelligence and Information Security (CIS). Federica Di Camillo is Senior Fellow in the IAI Security and Defence programme.

· Final report of the research project "The defence of civilian air traffic systems from cyber threats", conducted by the Istituto Affari Internazionali (IAI) with the support of Vitrociset. This report was translated from Italian to English with the support of ENAV.

ISSN 2280-6164

List of Acronyms

ACC	Area Control Center
ACARS	Aircraft Communications Addressing and Reporting System
ACI	Airports Council International
ADS-B	Automatic Dependent Surveillance-Broadcast
AFTN	Aeronautical Fixed Telecommunication Network
ALS	ALerting Service
AMHS	ATS Message Handling Service
ANSP	Air Navigation Service Provider
AOIS	Aeronautical Operational Information System
ARO	Air Traffic Services Reporting Office
ARTAS	Atm Surveillance Tracker and Server
ASM	Air Space Management
ASMGCS	Advanced Surface Movement Guidance and Control System
ATC	Air Traffic Control
ATFM	Air Traffic Flow Management
ATIS	Automatic Terminal Information Service
ATM	Air Traffic Management
ATM	Asynchronous Transfer Mode
ATN	Aeronautical Telecommunication Network
ATS	Air Traffic Services
AVSEC	Aviation Security
BYOD	Bring-Your-Own-Device
CANSO	Civil Air Navigation Services Organisation
CENTCOM	Central Command
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CIDIN	Common ICAO Data Interchange Network
CIS	Centre for Internet Security
CIS	Cyber Intelligence and Information Security Center
CNAIPIC	National Anti-crime Computer Centre for the Protection of Critical Infrastructures (Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche)
CNMCA	National Center of Aeronautical Meteorology and Climatology (Centro nazionale di meteorologia e climatologia aeronautica)
CNS	Communications, Navigation, Surveillance
COPASIR	Parliamentary Committee for the Security of the Republic (Comitato parlamentare per la sicurezza della Repubblica)
CPDLC	Controller Pilot Data-Link Communication
CPNI	Centre for the Protection of National Infrastructure
CRCO	Central Route Charges Office
CWP	Control Working Position
DDoS	Distributed denial of service
DIS	Security Intelligence Department (Dipartimento delle Informazioni per la sicurezza)

ISSN 2280-6164

DoS	Denial of Service
EASA	European Aviation Safety Agency
EATMP	European Air Traffic Management Programme
EGNOS	European Geostationary Navigation Overlay Service
ENAC	Italian Civil Aviation Authority (Ente nazionale per l'aviazione civile)
ENAV	Italian Air Navigation Service Provider (Ente nazionale per l'assistenza al volo)
ESARR	Eurocontrol Safety Regulatory Requirements
ESSP	European Satellite Services Provider
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FDP	Flight Data Processing
FDPM	Flight Plan Data Management
FIR	Flight Information Region
FIS	Flight Information Service
GAO	Government Accountability Office
IATA	International Air Transport Association
ICAO	International Civil Aviation Organisation
ICC	International Communications Centre
ICCAIA	International Coordinating Council of Aerospace Industries Associations
ICS	Industrial Control Systems
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ICT	Information Communication Technology
IDS	Intrusion Detection System
IED	Improvised Explosive Device
IETF	Internet Engineering Task Force
IFALPA	International Federation of Air Line Pilots' Associations
IFR	Instrument Flight Rules
IP	Internet Protocol
IRE	Interconnessione reti esterne
ISHD	Islamic State Hacking Division
ISIS	Islamic State of Iraq and Syria
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
IT	Information Technology
ITU	International Telecommunication Union
LAN	Local Area Network
MET	Aviation meteorology
MPLS	Multi Protocol Label Switching
NIPRNET	Nonclassified Internet Protocol Router Network
NMOC	Network Manager Operations Centre
NOTAM	Notices To Air Men
NSA	National Security Agency
OLDI	On-Line Data Interchange
OSI	Open Systems Interconnection

ISSN 2280-6164

OSSTM	Open Source Security Testing Methodology
OWASP	Open Web Application Security Project
PENS	Pan European Network Services
PoP	Point of Presence
RFC	Request for Comments
RWY	Runway
SADIS	Satellite Distribution System
SARPS	Standards and Recommended Practices
SCADA	Supervisory Control and Data Acquisition
SES	Single European Sky
SESAR	Single European Sky ATM Research
SIEM	Security Information and Event Management
SIPRNET	Secret Internet Protocol Router Network
SOC	Security Operation Centre
SOP	Same Origin Policy
SQL	Structured Query Language
SQLI	SQL-Injection
SRC	Safety Regulation Commission
SVFR	Special Visual Flight Rules
SWIM	System-Wide Information Management
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TMA	Terminal Control Area
TOR	The Onion Router
TPP	Trans Pacific Partnership
TTIP	Transatlantic Trade and Investment Partnership
UHF	Ultra High Frequency
UIR	Upper Information Region
VFR	Visual Flight Rules
VHF	Very High Frequency
VOR	Vhf Omnidirectional Radio Range
VPN	Virtual Private Network
WAN	Wide Area Network
XSS	Cross-Site Scripting

ISSN 2280-6164

Introduction

The US Government Accountability Office (GAO), which reports to the Congress, published a report in January 2015[1] in which it underscored several vulnerabilities found in the Federal Aviation Administration (FAA) air traffic control system.[2] According to the GAO, these weaknesses threaten "the agency's ability to ensure the safe and uninterrupted operation of the national airspace system (NAS)." The report concludes with the assertion that, despite the FAA's attempts to address these weaknesses, it has not yet found a solution to some that could expose their ICT systems to cyber attacks.[3] In a 2010 report "On the possible national security implications and threats deriving from the use of cyber space," COPASIR[4] cited a series of examples – a good portion of which were taken from the American experience – of possible attacks on air traffic management and control (ATM/ATC)[5] systems owing to the increasingly pervasive use of information technology. In particular, COPASIR urged legislators and national security bodies to lend the requisite attention to defending air traffic control systems, considered as a critical infrastructure whose defence helps guaranteeing values ensured by the Constitution, such as the life and safety of persons in-flight and on the ground and the freedom of circulation.[6] Along the same lines, in a statement announcing major government investments in cyber security, Chancellor of the Exchequer of the United Kingdom George Osborne underscored the highly sensitive nature of air traffic control systems.[7]

The COPASIR and GAO reports pinpoint a central national security problem: how the growing dependence of air traffic management and control systems on digital technologies inevitably introduces new forms of vulnerability. Against this backdrop, several related questions arise: What technologies do air traffic management and control systems rely on? Are these systems vulnerable? Which actors could pose a threat to these systems? Do they have the technological skills to conduct attacks that could compromise them?

[1] US Government Accountability Office (GAO), *FAA Needs to Address Weaknesses in Air Traffic Control Systems*, January 2015, http://www.gao.gov/assets/670/668169.pdf.

[2] The FAA is the agency of US Department of Transportation that regulates civil aviation in the United States.

[3] Aaron Cooper, "Report: Air traffic control system vulnerable to cyber-attack", in *CNN Politics*, 2 March 2015, http://cnn.it/1FOFlBU.

[4] Italy's Parliamentary Committee for the Security of the Republic.

[5] Air Traffic Management (ATM) and Air Traffic Control (ATC).

[6] COPASIR, *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico*, 7 July 2010, http://www.senato.it/leg/16/BGT/Schede/docnonleg/19825.htm. COPASIR considerations refer mainly to the consequences in case a threat was to materialise. The report does not express a judgement on the status of ATM/ATC security in Italy.

[7] George Osborne, *Chancellor's speech to GCHQ on cyber security*, 17 November 2015, https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security.

ISSN 2280-6164

This study is part of a broader discussion on the relationship between critical infrastructures and cyber security. Indeed, the majority of developed nations consider air transportation a critical infrastructure. Singapore has recognised civil aviation as crucial to the "Critical Infocomm Infrastructure Protection" programme of its national cyber security plan for 2018.[8] The United States lists transportation systems among 18 examples of critical infrastructure in Presidential Directive 7 on domestic security, within the context of the National Infrastructure Protection Plan.[9] The European Commission included transportation as a critical sector in its 2006 Directive on European Critical Infrastructures. Finally, with a 2008 decree entitled "Identification of Critical ICT Infrastructures of National Interest," the Italian Ministry of Interior included among as critical infrastructure, "Ministries – and the agencies and bodies charged with their oversight – operating in the sectors of international relations, security, justice, defence, finance, communications, transportation, energy, environment and health."[10]

Given the importance to national security and their inter-independence, critical infrastructures require a high level of protection that is not always easy to ensure. The report entitled "2013 Italian Cyber Security Report: Critical Infrastructure and Other Sensitive Sectors Readiness" drafted by the Cyber Intelligence and Information Security Centre (CIS) of the Sapienza University of Rome, states that Italy lags behind other developed countries in implementing a cyber strategy that gives due consideration to the defence of those infrastructures. The report points out that, in the four sectors analysed (public administration, public utilities, major industry and the financial sector), there were computerised components that, if successfully attacked, could lead to serious consequences at national and European levels. The operators within these macro sectors seemed unaware of being potential sensitive targets.[11]

The dangers to these systems are not only potential, but real and on the rise. In 2014 the National Anti-crime Computer Centre for the Protection of Critical Infrastructures (CNAIPIC) reported 1,151 cyber attacks – 161 of which involved web

[8] Singapore Ministry of Transport, *Singapore hosts civil aviation cyber security conference. Press release*, 9 July 2015, http://www.news.gov.sg/public/sgpc/en/media_releases/agencies/mot/press_release/P-20150709-1.html.

[9] Kasthurirangan Gopalakrishnan et al., "Cyber Security for Airports", in *International Journal for Traffic and Transport Engineering*, Vol. 3, No. 4 (December 2013), p. 365-376, http://dx.doi.org/10.7708/ijtte.2013.3(4).02.

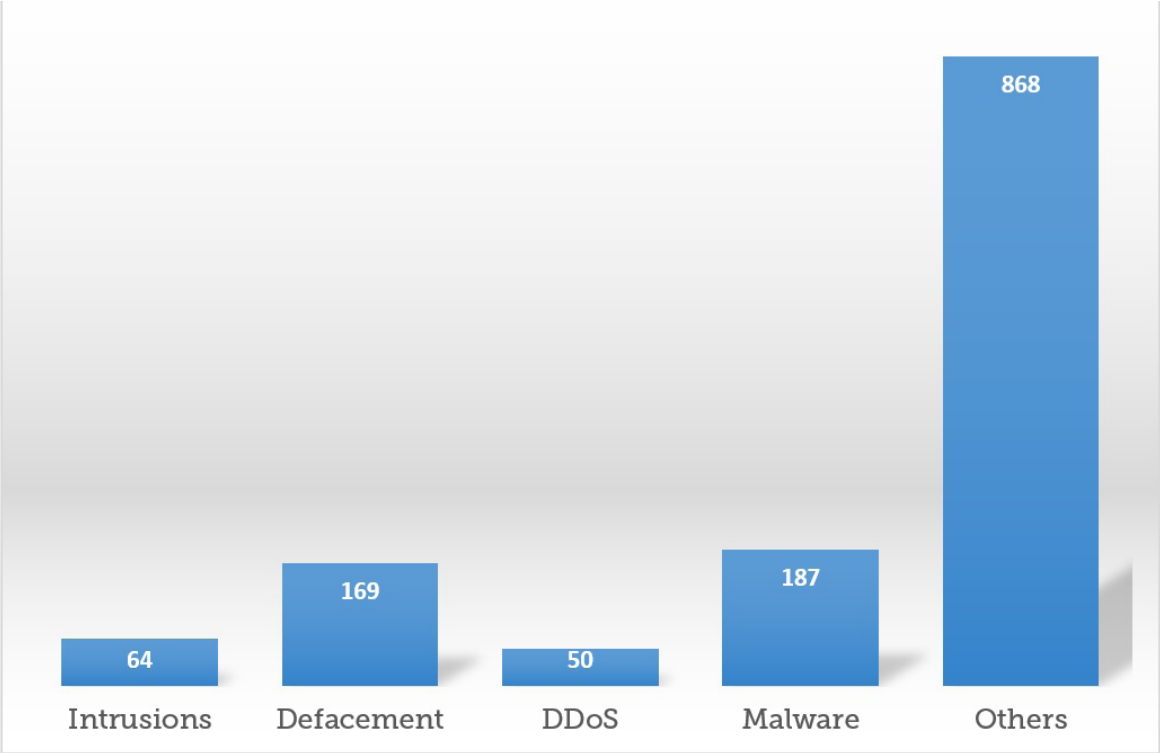
[10] Italian Ministry of Interior, *Decree of 9 January 2008*, Individuazione delle infrastrutture critiche informatiche di interesse nazionale, G.U. No. 101 of 30 April 2008, http://gazzette.comune.jesi.an.it/2008/101/1.htm.

[11] Cyber Intelligence and Information Security Centre (CIS), *2013 Italian Cyber Security Report. Critical Infrastructure and Other Sensitive Sectors Readiness*, Rome, Università "La Sapienza", December 2013, http://www.cis.uniroma1.it/sites/default/files/allegati/2013CIS-Report.pdf.

ISSN 2280-6164

defacement[12] and 50 Distributed Denial of Service (DDoS)[13] – against institutional internet websites and critical Italian infrastructures. Of these attacks, 64 were system intrusions and 187 compromises due to malware,[14] which had infected the websites of institutional entities and private enterprises. During the same period, 154 potential weaknesses and 148 other possible attacks were revealed.[15]

Figure 1 | Attacks addressed by CNAIPIC in 2014



Source: 2015 Clusit Report, p. 84.

The purpose of this study is to assess eventual weaknesses in Italian ATM/ATC systems that could be exploited by malicious actors. Also observed are the organisational, technological and process-related counter measures put in place

[12] "An attack carried out against a website and consisting in modifying the contents of the homepage or of other pages of the website." See Italian Presidency of the Council of Ministers, *National Strategic Framework for Cyberspace Security*, December 2013, p. 43, http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf.

[13] "An attack that prevents or impairs the authorized use of information system resources or services." See "denial of service" in the *Cyber Glossary* of the National Initiative for Cybersecurity Careers and Studies (NICCS): https://niccs.us-cert.gov/glossary#denial_of_service. Other instruments used by Anonymous include malware and phishing.

[14] "A technique to breach the security of a network or information system in violation of security policy." See "exploit" in NICCS *Cyber Glossary*: https://niccs.us-cert.gov/glossary#exploit.

[15] Italian Association for ICT Security, *Rapporto Clusit 2015 sulla sicurezza Ict in Italia*, Milan, Astrea, 2015, https://www.clusit.it/download/Rapporto_Clusit%202013.pdf.

ISSN 2280-6164

by the national Air Navigation Service Provider, ENAV,[16] as well as by government agencies, in compliance with the national cyber strategy and in light of Italy's commitments within the framework of international legal conventions. To that end, the first section introduces the theme of cyber security in civil aviation. A brief analysis of ICT-related incidents that have affected the sector will be followed by identification of the main problems and an outline of the scope of the present study. The second section explains what an ATM/ATC system is and how it works. The third describes the actors that civil aviation authorities consider a threat, including an assessment of the technical skills and objectives of the two main terrorist organisations, ISIS and Al-Qaeda, hacktivists and cyber criminals. The fourth section examines the role of and technologies employed by ENAV, with a discussion of possible cyber threats directed against Italy. Conclusions offer some food for thought on the study's results and on possible developments in the relationship between civil aviation and cyber security.

1. Cyber Security and Civil Aviation

"Aviation relies on computer systems extensively in ground and flight operations and air traffic management, and we know we are a target."[17]
Tony Tyler, Director General of the International Air Transport Association

As it has in many other complex human activities, the use of ICT in civil aviation has increased exponentially over recent years, from the development and construction of aircraft to communications and navigation instruments, along with all the thousands of connections that link the various parts of an airport. As in other fields, the digitalisation and placement online of such complex instrumentation have introduced considerable problems associated with cyber security. It is not surprising then that a 2012 report by the British Centre for the Protection of National Infrastructure (CPNI)[18] found that the interface and interdependence inherent to ICT-use has raised the vulnerability of aircraft and aviation systems, and consequently the impact of eventual compromise.[19] Despite financial and managerial improvements, it remains clear that weaknesses linked with cyber activity pose a noteworthy threat to civil aviation.

[16] National Flight Assistance Agency.

[17] Jonathan Gould and Victoria Bryan, "Cyber attacks, drones increase threats to plane safety: insurer", in *Reuters*, 4 December 2014, http://reut.rs/1tRTAOZ.

[18] British government authority that offers advice and recommendations on the security and defence of national infrastructure industries and organisations.

[19] Centre for the Protection of National Infrastructure (CPNI), *Cyber Security in Civil Aviation*, August 2012, http://www.cpni.gov.uk/highlights/cyber-security-in-civil-aviation.

DOCUMENTI IAI 15 | 23E - DECEMBER 2015
ISSN 2280-6164

Figure 2 | ICT technologies in civil aviation

Source: American Institute of Aeronautics and Astronautics, *A Framework for Aviation Cybersecurity*, August 2013, p. 8, http://www.aiaa.org/aviationcybersecurity.

The goal of this section is to provide an introductory framework for the relationship between cyber security and civil aviation, with the initial presentation of some ICT incidents that have affected the sector. It will go on to examine international efforts to combat cyber threats and the counter measures currently in place. Finally, the main ICT problems that condition in-flight and ground security will be described.

1.1 Significant events

Civil aviation has historically been an especially appetising target. As the sector has evolved, the threats it faces have changed in both dimension and modality, with a shift away from traditional physical attacks on aircraft and airports to new kinds of events that include the many episodes ascribable to the cyber threat. The following are some recent examples of ICT incidents involving the civil aviation sector:[20]

• 2006, July: a cyber attack forces the American FAA to shut down several ATC systems in Alaska.[21]

• 2008, August: at Spain's Madrid-Bajaras airport, a trojan[22] in one of Spanair's main

[20] The events described are only a partial sampling of such incidents. It should be noted that the majority do not involve ATM/ATC systems, with the exception of the 2006 Alaskan incident.

[21] Bernard Lim, "Aviation Security: Emerging Threats from Cyber Security in Aviation – Challenges and Mitigations", in *Journal of Aviation Management*, 2014, p. 84, http://www.saa.com.sg/saaWeb2011/export/sites/saa/en/Publication/downloads/SAA_Journal_2014.pdf.

[22] "A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program." See "trojan horse" in NICCS *Cyber Glossary*: https://niccs.us-cert.gov/glossary#Trojan_horse.

ISSN 2280-6164

computer systems blocks the reception and activation of an alarm message from flight No. 5022. This was cited among the causes of the plane's collision and the loss of 154 passenger lives. It has yet to be determined whether the systems were intentionally compromised through the Trojan.[23]

• 2009, February: an attack on FAA computers allows unknown hackers to access 48,000 personnel files.[24]

• 2011, June: three engineers are accused of "interruption of computer services" that had caused heavy check-in and flight delays.[25]

• 2013, July: the passport control systems of the Istanbul Ataturk and Sabiha Gökçen airports are blocked by a cyber attack, resulting in numerous flight delays.[26]

• 2013: according to a report by the Centre for Internet Security (CIS),[27] approximately 75 American airports were attacked by prolonged spear phishing campaigns.[28]

• 2014, March: Malaysia Airlines flight MH370 disappears from tracking radar, and the Boeing 777-200ER is later given up for lost in an airline press release. In the overall uncertainty surrounding the event, it was also suggested that the plane had been commandeered by means of a mobile phone and/or a USB drive.[29] The theory has never been proven and has been roundly rejected by Boeing.

• 2014, December: the Cylance company accuses Iranian hackers of a coordinated attack against the computer systems of over 16 countries, including attacks on the systems of the airports and airlines of Pakistan, Saudi Arabia, South Korea and the United States.[30]

• 2015, February: the FAA discovers various forms of malware in personnel e-mail accounts. The agency claims there was no damage from the attack.[31]

• 2015, April: Ryanair airline suffers financial damages of nearly 3 million pounds resulting from a cyber attack on its bank accounts.[32]

[23] Roland Heickerö, "Cyber Terrorism: Electronic Jihad", in *Strategic Analysis*, Vol. 38, No. 4 (2014), p. 556, http://dx.doi.org/10.1080/09700161.2014.918435.

[24] Bernard Lim, "Aviation Security: Emerging Threats from Cyber Security in Aviation", cit., p. 84.

[25] ICCAIA, *Cyber Security for Civil Aviation*, presented at the Twelfth Air Navigation Conference, Montréal, 19-30 November 2012, http://www.icao.int/Meetings/anconf12/WorkingPapers/ANConfWP122.1.1.ENonly.pdf.

[26] Ramon Lopez and Ben Vogel, "Authorities face uphill battle against cyber-attacks", in *IHS Jane's Airport Review*, 9 April 2015, http://www.ihsairport360.com/article/6186/authorities-face-uphill-battle-against-cyber-attacks.

[27] US non-governmental and non-profit organisations whose mission is to improve public and private agencies' readiness to address cyber security, with a view to achieving excellent results through collaboration.

[28] Ramon Lopez and Ben Vogel, "Authorities face uphill battle against cyber attacks", cit. Phishing is "A digital form of social engineering to deceive individuals into providing sensitive information." See "phishing" in NICCS *Cyber Glossary*: https://niccs.us-cert.gov/glossary#phishing.

[29] Ellie Zolfagharifard, "Hackers are a serious threat to aircraft safety': Aviation chiefs warn of the devastating consequences of a cyber attack", in *Daily Mail Online*, 11 December 2014, http://dailym.ai/1zalBGR; Pierluigi Paganini, "Cyber Threats against the Aviation Industry", in *InfoSec Resources*, 8 April 2014, http://resources.infosecinstitute.com/?p=25456.

[30] Ramon Lopez and Ben Vogel, "Authorities face uphill battle against cyber attacks", cit.

[31] Bart Jansen, "FAA hit by cyberattack, finds no damage", in *USA Today*, 7 April 2015, http://usat.ly/1yaHNV0.

[32] Jack Elliott-Frey, "The threat in the skies: Have cyber attackers boarded the plane?", in *Insurance*

ISSN 2280-6164

• 2015, June: an attack on the Polish national airline (LOT) network grounds ten flights to Denmark, Germany and Poland, causing delays for another ten. The attack compromised the system that creates flight plans.[33]

This far from exhaustive list shows how computer incidents have contributed significantly to moving cyber security to centre stage in the discussion on civil aviation. Such events have prompted the principal international sector organisations to seek concrete ways to address their systems' possible vulnerabilities.

1.2 International efforts

There is currently no overarching, universal approach to cybersecurity in civil aviation, although many attempts have been made to address the issue.[34]

In October 2012, during the 12th Air Navigation Conference sponsored by the ICAO,[35] the ICCAIA[36] asserted that cybersecurity had been identified as a high level impediment to the implementation of the Global Air Navigation Plan, and that the new technologies about to be adopted, were intrinsically more vulnerable to cyber attacks.[37] The association urged the creation of a working group tasked with implementing, managing and monitoring cyber security-related procedures and practices. In March 2014, the ICAO's AVSEC Panel[38] called for additional efforts at assessing cyber risks to air traffic management systems based on new ICT technologies,[39] since Annex 17 of the 1944 Chicago Convention on Civil Aviation still referred to cyber security as a "recommended practice" and not a "standard."[40]

Business Blog, 27 May 2015, http://www.ibamag.com/news/blog-the-threat-in-the-skies-have-cyber-attackers-boarded-the-plane-22592.aspx.

[33] "Polish LOT aeroplanes grounded by computer hack", in *BBC News*, 21 June 2015, http://www.bbc.com/news/world-europe-33219276.

[34] Bart Elias, "Protecting Civil Aviation from Cyberattacks", in *CRS Insights*, 18 June 2015, http://www.fas.org/sgp/crs/homesec/IN10296.pdf.

[35] The International Civil Aviation Organisation is the UN agency that regulates international civil aviation.

[36] International Coordinating Council of Aerospace Industries Associations.

[37] ICCAIA, *Cyber Security for Civil Aviation*, cit. Also in 2012, the same organisation amended one of the 19 Annexes of the International Civil Aviation Convention on which it was founded to include cyber security.

[38] The Aviation Security (AVSEC) Panel Working Group is a group of ICAO experts tasked with assessing security problems and possible threats to civil aviation.

[39] Bernard Lim, "Aviation Security: Emerging Threats from Cyber Security in Aviation", cit. The problems the group is currently reviewing include a series of possible cyber attacks on cockpits, ICT systems supporting modern ATM systems and airport computer systems such as departure controls and flight information displays. See: Raymond Benjamin, *Opening Remarks to the Conference on Civil Aviation Cyber Security*, 9-10 July 2015, http://www.icao.int/Documents/secretary-general/rbenjamin/20150720_Singapore_Cyber_Security.pdf.

[40] Interview, November 2015. Annex 17 (Safeguarding Against Acts of Unlawful Interference) cites the "Primary objective of each contracting state is safe guarding its passengers, ground personnel, crew as well as the general public against any acts of unlawful interference," including attacks of a technological nature against air navigation infrastructure.

ISSN 2280-6164

In 2013, IFALPA[41] published "Cyber threats: who controls your aircraft?", a report citing the "significant and emergent" threat of cyber attacks on aircraft, ground facilities or other systems important to civil aviation. The report underscored navigation data's lack of security and the noteworthy distress that could result from their alteration.[42]

In 2014, CANSO[43] set up the ATM Security Work Group, which produced, among other things, a "Cyber Security and Risk Assessment Guide" for the purpose of fostering the application of sector best practices between associated Air Navigation Service Providers (ANSPs).[44] Also in 2014, IATA[45] published a cyber security in civil aviation manual that was updated in July 2015.[46]

In December 2014, ICAO, IATA, ACI,[47] CANSO and ICCAIA signed a Civil Aviation Cyber Security Action Plan coordinating their respective efforts to counter the cyber threat and "promote the development of a robust cyber-security culture in all organizations involved in international civil aviation, while additionally identifying and sharing best practices."[48]

The general belief, voiced also in the Industry High-Level Group (Cyber) studies sponsored by ICAO with CANSO, IATA, ACI and ICCAIA, is that the civil aviation sector needs a specific approach to cyber protection. Nevertheless, a more general approach must also be considered since the technologies employed in civil aviation are also used in other sectors and are, therefore, subject to the same cyber threats.

Recent international undertakings indicate the degree of importance that cyber security has gained in the context of civil aviation. Depending on the system considered, the vulnerabilities that could be exploited by various actors with criminal intent are numerous. The next paragraph offers a brief description of those systems that, if compromised, could represent a danger to the safety of persons and to national security in general.

[41] International Federation of Air Line Pilots' Associations represents approximately 100,000 pilots around the world.

[42] IFALPA, "Cyber threats: who controls your aircraft?", in *IFALPA Position Papers*, No. 14POS03 (5 June 2013), http://www.ifalpa.org/store/14POS03%20-%20Cyber%20threats.pdf.

[43] Civil Air Navigation Services Organisation, association of air navigation services providers that includes ENAV.

[44] CANSO, *Cyber Security and Risk Assessment Guide*, 2014, https://www.canso.org/node/753.

[45] International Air Transport Association, sector association with a membership of 260 airlines, which account for 83 percent of global air traffic.

[46] Intended to offer a general overview of the topic, and to provide airlines with a cyber risk assessment tool and a guide to implementing a cyber security management system. IATA, *Aviation Cyber Security Toolkit*, 2nd edition, July 2015, https://www.iata.org/publications/Pages/cyber-security.aspx.

[47] Airports Council International.

[48] Raymond Benjamin, *Opening Remarks to the Conference on Civil Aviation Cyber Security*, cit.

ISSN 2280-6164

1.3 Main arguments and scope of the study

There are three main targets that could be the focus of cyber-related attacks on civil aviation: internal airport computer systems, in-flight aircraft control systems and air traffic management systems.[49]

Airport facilities are especially vulnerable to cyber threats. In addition to the systems of the organisations and entities that routinely use the internet for daily operations, such as data exchanges and messaging, other targets could include the Supervisory Control and Data Acquisition (SCADA) systems that often control ventilation systems, baggage transport, and so forth. In the future, the increased use of web-linked mobile applications will probably further menace operations within airports, making them potentially vulnerable to attack by a vast number of both physical devices (USB drives, computers, digital cameras, etc.) and virtual operations (DoS, phishing, trojans, etc.).[50]

Many information security experts have stressed how the introduction of on-board Wi-Fi has produced noteworthy security faults. In 2013, at a conference of the European Aviation Safety Agency (EASA), Spanish expert Hugo Teso demonstrated how it was possible to commandeer an aircraft control system with a smartphone, using a software application that he had created, and eventually make the plane crash.[51] Both the FAA and EASA subsequently asserted the limited validity of the test since it had been performed with a flight simulator, and that Teso's method would not yield the same results when using a software application installed on certified for flight hardware.[52] In 2014, Ruben Santamarta proved that it was possible to interfere with satellite communications, and therefore with flight navigation systems, using the in-flight entertainment system accessible through Wi-Fi.[53] Similarly, in July

[49] Another concern is computer fraud: the sector's substantial potential profits make it one of cyber criminals' preferred channels, to the extent that, according to some figures, approximately 50 percent of all phishing attempts target airlines and their passengers. See: ICAO, *Aviation Unites on Cyber Threat*, 10 December 2014, http://www.icao.int/Newsroom/Pages/aviation-unites-on-cyber-threat.aspx.

[50] Kasthurirangan Gopalakrishnan et al., "Cyber Security for Airports", cit.

[51] Marcel Rosenbach and Gerald Traufetter, "Cyber-Attack Warning: Could Hackers Bring Down a Plane?", in *Spiegel Online International*, 22 May 2015, http://spon.de/aevsu; Neil McAllister, "FAA: 'No, you CAN'T hijack a plane with an Android app'", in *The Register*, 13 April 2013, http://goo.gl/news/0PmU. EASA has confronted the theme on other occasions as well: Cyrille Rosay, *Aviation Cybersecurity Roadmap Research Needs*, Aerodays2015, London, 20-23 October 2015, http://www.aerodays2015.com/wp-content/uploads/sites/20/6H-3-Emmanuel-Isambert.pdf.

[52] Neil McAllister, "FAA: 'No, you CAN'T hijack a plane with an Android app'", cit. Airbus funded an independent study to show that in-flight Wi-Fi systems are entirely independent of avionics, and that ACARS and ADS-B can clearly be subject to interference in that they are collaborative systems carried over radio frequencies, but that this is something different from a hacker commandeering an aircraft. Interview, November 2015.

[53] Some industry representatives that produce potentially violable systems have confirmed the validity of some of Santamarta's results, although they downplay the actual risk. See: Jim Finkle, "Hacker says to show passenger jets at risk of cyber-attack", in *Reuters*, 4 August 2014, http://reut.rs/1olAeyA.

ISSN 2280-6164

2015 Chris Roberts was able to manipulate the control systems of the aeroplane he was flying on through the in-flight entertainment system. According to Federal Bureau of Investigation (FBI) documentation, after connecting his computer to the electronic box located under his seat, Roberts typed in the command "CLB" (climb) and the plane's engine responded to the prompt.[54]

Finally, ATM/ATC systems have also come under scrutiny given their growing dependence on ICT and interface with other systems and technologies. A 2009 report by the US Department of Transportation Inspector General criticised inefficiencies and weaknesses in the FAA's ATM systems, especially with regard to access control procedures and the ability to identify unlawful intrusions.[55] A more recent report by the GAO (January 2015) underscored that "significant security control weaknesses remain, threatening the agency's ability to ensure the safe and uninterrupted operation of the national airspace system (NAS). These include weaknesses in controls intended to prevent, limit, and detect unauthorized access to computer resources, such as controls for protecting system boundaries, identifying and authenticating users, authorizing users to access systems, encrypting sensitive data, and auditing and monitoring activity on FAA's systems."[56] According to the report, some of the systems weaknesses were owing to the lack of a comprehensive cyber risk management programme, proof of which lay in the absence of a precise definition of roles and responsibilities within the FAA.

As for the relationship between cyber security and civil aviation, this report confronts the lattermost of the foregoing themes, i.e. the cyber threat to ATM/ATC systems.

2. Function and Components of ATM/ATC Systems

An ATM system is a pool of air traffic management services. In an effort to circumscribe its field of investigation, this study will focus on the Air Traffic Services component (ATS) and, in particular, on Air Traffic Control (ATC).

The main purpose of an ATM is to allow operators (e.g. airlines) to comply with their established departure and arrival times and maintain their preferred fight profiles (routes and altitudes indicated in flight plans) without compromising security. The ATM can be understood as the integration of the following components:
ATM = ATS + Air Traffic Flow Management (ATFM) + Air Space Management (ASM).[57]

[54] Marcel Rosenbach and Gerald Traufetter, "Cyber-Attack Warning...", cit.; Kim Zetter, "Feds Say That Banned Researcher Commandeered a Plane", in *Wired*, 15 May 2015, http://www.wired.com/?p=1782748.

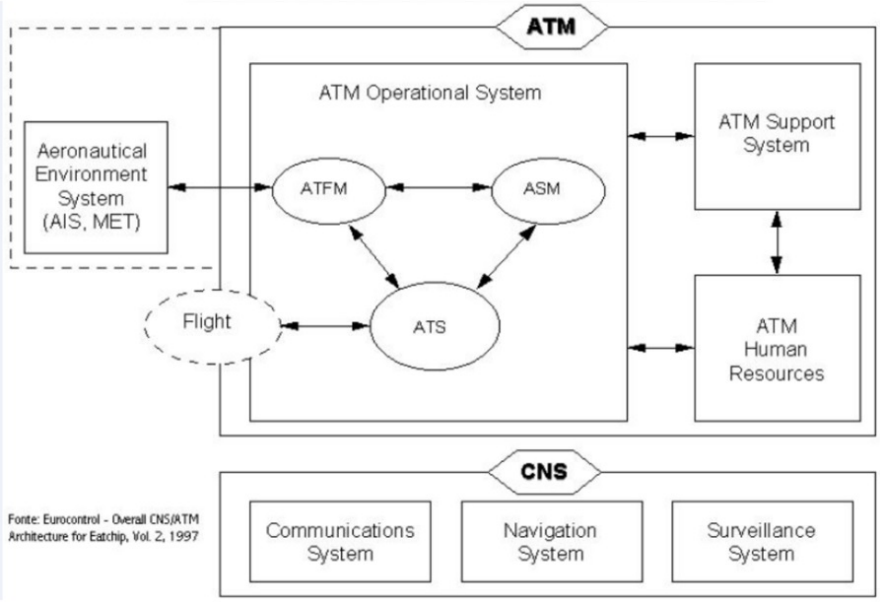
[55] Bart Elias, "Protecting Civil Aviation from Cyberattacks", cit.

[56] GAO, *FAA Needs to Address Weaknesses in Air Traffic Control Systems*, cit.

[57] ENAV, "Gestione del traffico aereo", in *Compendio ATC*, September 2011, p. 92, http://www.enav.it/ec5/enav/it/pdf/compendio_77_155.pdf.

ISSN 2280-6164

Figure 3 | Principal CNS/ATM system elements



ATS services are generally provided by ANSPs that use the instruments and personnel of airports and Area Control Centres (ACC), where control rooms equipped with various systems (radar, radio, weather sensors, etc.) ensure operations management. The most important of ANSP personnel are the air traffic controllers,[58] who are specialised in providing ATS. Air space is divided into what are called Flight Information Regions (FIR), and each FIR is assigned to a designated ACC in compliance with the international accords stipulated by ICAO.[59]

The ATC is a complex system based on national and international legislation, procedures, organisations and technological instruments for the purpose of preventing collisions between aircraft or with various other obstacles, organising and optimising air traffic flow, providing information and recommendations to pilots to improve the quality and efficiency of flights and assisting third parties in search and rescue operations. In many countries, ATCs provide services to all private, military, commercial and government carriers operating in their assigned air space. Depending on the type of flight and class of air space, ATC makes recommendations that pilots may choose to follow or not, or instructions that pilots are obliged to follow, save in cases of clearly perceived emergency.[60]

[58] Commonly known as flight controllers.

[59] FIR size and format can differ considerably; in some cases, FIRs can be subdivided horizontally and, in that case, the term FIR refers to the air space below and the term Upper Information Region (UIR) to the air space above.

[60] The pilot is responsible for the safety of the aircraft. See: ICAO, *Rules of the Air*. Annex 2 to the Convention on International Civil Aviation, 10th edition, July 2005, http://www.icao.int/Meetings/anconf12/Document%20Archive/an02_cons%5B1%5D.pdf.

ISSN 2280-6164

ATC procedures are based on ICAO's assignment of air space volumes to seven classes[61] (although some countries are allowed to make adaptations in accordance with specific local needs), and are subject to Visual Flight Rules (VFR), Instrument Flight Rules (IFR) and, in some cases, Special Visual Flight Rules (SVFR). Operational modes vary from the strict Class A to the more relaxed Class G. Each class is defined in consideration of specific required features: whether air space control is required, whether operations must be under IFR/VFR/SVFR; maintenance of separation, which ATS services are provided, minimum visibility conditions and distance from clouds, obligation of radio contact, the need for entry authorisation, on-board transponder modality[62] and so forth. Classes A to E correspond to controlled air space, F and G to uncontrolled air space. ATC services are required for IFR flights in Classes A, B, C, D and E, and for VFR flights in Classes B, C and D.[63]

ATC services involve all phases of an aircraft's movement – taxiing, boarding and debarking, airport areas,[64] take-off/landing operations and cruising – and are distinguished as Ground Control, Local Control and Area Control.

Ground Control, coordinated from the airport control tower, regulates and organises the movement of aircraft and other vehicles in the airport area, including entry/exit into/out of the taxiway, inactive runways, stopping and transit areas (in departure, after leaving the gate, upon arrival, coming off the runway). Any aircraft, vehicle or person moving in these controlled areas must receive explicit authorisation from Ground Control via VHF/UHF radio.

Local Control, normally handled by the control tower,[65] is responsible for the use of the runway (RWY), taxiways to the runways, aircraft take-off/landing stages (Approach Control), for which it provides specific authorisations and instructions, ensuring separation between runways and aircraft at all times. In the pre-take-off phase, shortly before starting up the runway, local control provides the pilot with taxiway and runway indications and route instructions upon take-off, with the related authorisations (Clearance Delivery). Flight Data, normally coordinated with Clearance Delivery, is the resource that delivers pilots accurate and updated information on weather variations, interruptions, delays in ground operations, runway closures, and so forth, and are broadcast on a continuous loop over a dedicated frequency known as the Automatic Terminal Information Service (ATIS). The ACC also provides route details for reaching a designated landing strip. In the case of anomalies in an aircraft approaching for landing, Local Control can issue a go-around directive, telling the pilot to interrupt landing operations and stand

[61] Normally denoted by the first 7 letters of the ICAO phonetic alphabet: Alpha, Bravo, Charlie, Delta, Echo, Foxtrot, Golf. See Annex 11 (Air Traffic Services), in ICAO, *The Convention on International Civil Aviation. Annexes 1 to 18*, http://www.icao.int/safety/airnavigation/nationalitymarks/annexes_booklet_en.pdf.

[62] Receiver-transmitter that generates a signal in response to a specific query.

[63] ICAO, *Annex 11* (Air Traffic Services), cit.

[64] Take-off/landing area.

[65] Pilots often refer to Local Control with the term Control Tower.

ISSN 2280-6164

by to receive new instructions. Controllers assisting approaching aircraft normally manage planes at a distance of up to 30-50 nautical miles from the airport, and are sometimes assisted by the airport's radar rooms operators and a control centre (or other airport) nearby.

Area Control is provided by an ACC assigned to the FIR in which a plane is located during cruise stage. Basic ATS services for each FIR consist of a Flight Information Service (FIS) and an Alerting Service (ALS). FIS data cover weather conditions, volcanic activity, the presence of radioactive or toxic substances in the atmosphere, changes in the operational efficacy of navigation aids, unmanned balloons, risk of collision, presence of ships in the area and all other security-related information. The ALS notifies the proper authorities of aircraft in need of search and rescue operations and assists with those as necessary.

3. Cyber Threats to ATM/ATC Systems

In December 2014, ICAO, IATA, ACI, CANSO and ICCAIA signed an action plan for cybersecurity in civil aviation, in an effort to form a common front against "hackers, 'hacktivists', cyber criminals and terrorists now focused on malicious intent ranging from the theft of information and general disruption to potential loss of life."[66] Similarly, during the August 2015 cybersecurity conference in Singapore, ICAO secretary general Raymond Benjamin stated that, despite the fact that the organisation had not yet been informed of any cyber-related catastrophic events, it was fully aware that "terrorists, criminals and hacktivists are generally set on exploiting vulnerabilities in civil society."[67] According to these institutions, the most direct cyber threat to civil aviation is posed by non-state actors, i.e. terrorists, hacktivists and cyber crime groups. Based on this assessment, the present study excludes analysis of the threat of possible attack by state or para-state entities. It also does not deal with electronic warfare operations. Nevertheless, it is worth pointing out that, in light of their combined resources and technological skills, states pose the greatest danger to the critical infrastructures of third countries.[68] Similarly, the study will not make direct reference to the possible risks associated with the acts of disloyal employees or of actors traceable to suppliers or sub-suppliers who could potentially be manipulated.

The following section will seek to unravel the logic employed by non-state actors operating in cyber space. A subsequent detailed analysis of their modus operandi will attempt to reveal any regularities that may exist in both their techniques and

[66] ICAO, *Aviation Unites on Cyber Threat*, cit.

[67] Raymond Benjamin, *Opening Remarks to the Conference on Civil Aviation Cyber Security*, cit.

[68] According to some estimates, for the next 5-10 years only national governments will have the technological and financial means for developing the capabilities needed to attack a country's critical infrastructure. See: ICS-CERT, *Cyber Threat Source Descriptions*, https://ics-cert.us-cert.gov/node/18.

ISSN 2280-6164

targets. The last part will summarise what the analysis brings to light and offer an initial assessment of the status of the cyber threat to critical infrastructures such as ATM/ATC systems.

3.1 Attack or not? Two views compared

What could spur terrorists or other malicious actors to launch a cyber attack on a country's critical infrastructures?[69] The study brings two main approaches to confronting the question. According to a cost/benefit analysis, a terrorist cannot afford to plan and conduct a complex operation in cyber space because it is expensive and its potential results would not have the media impact of a simple bomb detonated in the heart of a city. From a more technological point of view, however, a terrorist could target the critical infrastructure of a country simply because it can be done; in other words, because the systems that maintain those facilities are not, and will never be, entirely secure, as is true of all IT systems.

Departing from the work of Giampiero Giacomello,[70] Maura Conway maintains that at least four factors motivate a terrorist organisation to use other than cyber tactics and tools: cost, complexity, destruction factor and media impact.[71] The author uses the examples of Stuxnet and an improvised explosive device (IED) to explain her theory. Stuxnet is a "worm"[72] (probably) created by one or more government authorities with the intention of slowing and/or halting the Iranian nuclear programme. The worm was discovered in 2010 when Iranian engineers realised that one-fifth of a nuclear plant's centrifuges had been damaged. Based on the available sources, this has been the only cyber attack to date to produce a physical effect. Although the damage was limited to the centrifuges, the act's outcome required noteworthy technical expertise and massive financial resources. According to some analyses, Stuxnet was the product of 10,000 hours of development by one or more teams of computer science experts and engineers, for an overall cost of from a few million to tens of millions of dollars.[73] By contrast, building an IED is especially simple based on the low cost and ease of finding the materials needed and their relatively easy assembly. Despite that, an IED attack is capable of causing

[69] This section does not intend to describe the specific vulnerabilities of infrastructure such as ATMs, considering that there are no SCADA systems in the realm of ATC, and in the case of Italy in particular. This section aims to foreground how terrorist, hacktivist or cyber crime groups' choices are cost/benefit driven. The section refers mainly to the logic behind terrorist organisations' acts.

[70] Giampiero Giacomello, "Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism", in *Studies in Conflict and Terrorism*, Vol. 27, No. 5 (2004), p. 387-408.

[71] Maura Conway, "Reality Check: Assessing the (Un)likelihood of Cyberterrorism", in Thomas M. Chen, Lee Jarvis, Stuart Macdonald (eds.), *Cyberterrorism. Understanding, Assessment, and Response*, New York, Springer, 2014, p. 103-122.

[72] "A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself." See "worm" in NICCS *Cyber Glossary*: https://niccs.us-cert.gov/glossary#worm.

[73] For an in-depth analysis, see: US Senate Committee on the Judiciary, *Virtual Threat, Real Terror: Cyberterrorism in the 21st Century*, Hearing before the Subcommittee on Terrorism, Technology, and Homeland Security, 24 February 2004, http://www.gpo.gov/fdsys/pkg/CHRG-108shrg94639.

ISSN 2280-6164

dramatic physical harm, certainly greater than that caused by Stuxnet. The degree of destruction therefore becomes a determining factor, and not least in light of the final element to be considered: media impact. According to Conway, cyber attacks such as those that various terrorist organisations could launch lack the media resonance of a bomb that leaves dozens of civilian victims. The combination of these four factors makes cyber terrorism possible but, fortunately, improbable.[74]

Alternatively, Clay Wilson argues from a technological standpoint that digitised networks feature vulnerabilities that are easily exploitable by terrorists. In the first place, the security updates of software that regulate and make critical infrastructures function properly are not fast or frequent enough.[75] In cases in which such system software is patented, non-standard or dated, one may decide to stop patching security vulnerabilities even in the presence of newly discovered ones. This is extremely risky since software that is not updated is easily visible by public search engines such as Shodan. Updating a security patch can be costly and difficult to manage, even in the case of non-obsolete software. Installing updates on critical infrastructure components could lead to the suspension of service and thus make continuous updating difficult, if not impossible. Similarly, many critical infrastructures today are remotely linked and managed from SCADA and Industrial Control Systems (ICS) headquarters in order to generate reports on the management of the infrastructures systems themselves.[76] Being linked to the public network could make these infrastructures vulnerable to attack and, if not properly protected, to infection by malware capable of spreading to the entire SCADA or ICS systems. Cyber espionage techniques can be used to identify system weaknesses and then be exploited by specifically designed malware to be injected into the targeted system. Finally, potential terrorists could already be in possession of powerful malware that can be "reverse-engineered" to conduct cyber attacks. Flame[77] and Stuxnet are examples of malware that, once discovered, were analysed by various organisations and then altered and reutilised under a variety of circumstances. These two malware made history because they contained multiple zero-day exploits.[78] Counter-measures against these types of malware do not exist precisely because the weaknesses are unknown. Against this backdrop, it seems that whereas these exploits were once the sole prerogative of governments and

[74] Maura Conway, "Reality Check: Assessing the (Un)likelihood of Cyberterrorism", cit. For an opposing view, see: Gabriel Weimann, *Terrorism in Cyberspace. The Next Generation*, Washington, Woodrow Wilson Center Press / New York, Columbia University Press, 2015, p. 152-153.

[75] "A piece of software designed to update a computer program or its supporting data, to fix or improve it". See: Wikipedia, https://en.wikipedia.org/wiki/Patch_(computing).

[76] SCADA and ICS are automated systems used to control industrial processes such as, for example, regulation of the electrical grid. See: Democratic Policy & Communication Center, *Glossary of Cyber Related Terms*, July 2012, http://www.dpc.senate.gov/docs/fs-112-2-183.pdf.

[77] For a description of Flame and its effects, see: Kaspersky Lab, *What is Flame Malware?*, http://www.kaspersky.com/flame.

[78] "Zero-day vulnerability refers to a security hole in software – such as browser software or operating system software – that is yet unknown to the software maker or to antivirus vendors." See, Kim Zetter, "Hacker Lexicon: what is a zero day?", in *Wired*, 11 November 2014, http://www.wired.com/?p=1588707.

ISSN 2280-6164

agencies, today are employed by a variety of actors in the cyber space.[79]

These two discrete perspectives offer some interesting food for thought when considering the possibility that various actors may decide to attack critical systems such as ATM/ATCs. According to Wilson's technological argument, an attempt to compromise the systems and networks of these infrastructures is feasible because they will never be entirely secure. It may be true that a cyber attack capable of blocking centrifuges has less media punch than dozens of fatalities, but that depends on the extent of the cyber attack. If a terrorist organisation will successfully manage to block an ATM system in the future and cause large-scale civilian death, such an attack would certainly not be less media worthy than a bomb going off in a marketplace. In any case, the existence of faults capable of allowing an attack on complex ICT systems does not mean that terrorists, hacktivists and cyber criminals will decide to mount one, or that they are even capable of doing so. As Conway emphasises, carrying out an attack with effects similar to those resulting from the Stuxnet worm is currently an extremely complex undertaking, requiring massive financial and technical resources. As will become evident as this study continues, it is not clear whether non-state actors have yet this economic and technical capability.

3.2 Actors, objectives and modus operandi

This section offers an analysis of the means and objectives of those actors that civil aviation authorities have identified as possible threats – terrorist organisations, hacktivists and cyber criminals – and an overview of their activities in cyber space, with a view to determining their actual capabilities and intentions.

Terrorist organisations (ISIS and Al-Qaeda)[80]

The Islamic State of Iraq and Syria (ISIS), a militant jihadist group that proclaimed itself a Caliphate in June 2014, currently controls vast portions of Syria and Iraq, thanks not least to the support of thousands of fighters and followers from various parts of the world.[81] As the group claims authority over the entire Muslim world and its intention of extending its jurisdiction across the planet, various international

[79] Clay Wilson, "Cyber Threats to Critical Information Infrastructure"; in Thomas M. Chen, Lee Jarvis, Stuart Macdonald (eds.), *Cyberterrorism. Understanding, Assessment, and Response*, New York, Springer, 2014, p. 123-137.

[80] This study examines the use of cyber space by ISIS and Al-Qaeda only, regardless that other organisations make use of it in the pursuit of their goals. The two were chosen since they represent the greatest threat to Italy (see the case study analysed in the following chapter). For an analysis of the use of the cyber dimension by other terror organisations, see: "Terror Goes Cyber: The Cyber Strategies and Capabilities of Al Qaeda, ISIS, Al Shabaab, and BokoHaram", in *Bat Blue Special Reports*, April 2015, http://www.batblue.com/?p=6166.

[81] Tobias Feakin and Benedict Wilkinson, "The Future of Jihad: What Next for ISIL and al-Qaeda?", in *ASPI Strategic Insights*, June 2015, https://www.aspi.org.au/publications/the-future-of-jihad-what-next-for-isil-and-al-qaeda.

ISSN 2280-6164

organisations and nations have declared it a terrorist organisation. In addition to its military successes on the ground and the brutality of its practices, its use of cyber space has drawn the attention of scholars and experts. ISIS operates in the "deep," the "dark," and the "surface" web, where it seeks the highest possible visibility for its acts.[82] It uses cyber space primarily for propaganda, recruiting,[83] financing and the transfer of ICT expertise.[84]

As another emerging dimension of the group activities in cyber space, ISIS is more often recurring to "hacking," the unauthorised access to computer systems,[85] or Dos/DDoS, the interruption of computer services. These activities are perpetrated by ISIS members or, more probably, by directly affiliated hacker groups.

In March 2015, pro-ISIS militants exploited a series of weaknesses in the WordPress platform and compromised approximately 200 web sites. The following April, ISIS-affiliated hackers took over the Twitter account of Egyptian singer Nugoum to release a flood of propaganda. In August, the affiliated Al-Battar Media group posted a 9-minute video containing the demographic data (name, e-mail and home addresses, telephone number, IP address and home country) of American, English, French and Italian military personnel, claiming to have hacked into a "British military site". Also worthy of note are ISIS "Cyber Army" activities between 19 and 29 March 2015, during which time the cyber jihadists defaced one French, one Russian and three Egyptian websites. Twitter images posted in July contained the data of NATO soldiers obtained, according to the perpetrators, after hacking into one of

[82] The "dark web" is distinct from the "deep web". The deep web is an extensive section of the web made up of web sites, networks and digital content that are not indexed by normal search engines such as Google. The dark web is that portion of the deep web made up of sites whose IP addresses are hidden but accessible by Tor browser if the exact URL is known. See: Pierluigi Paganini, "The Dark web – Why the hidden part of the web is even more dangerous?", in *Security Affairs*, 11 October 2015, http://securityaffairs.co/wordpress/40933. The Tor browser was designed to maintain a user's identity invisible online. For details see the project page: https://www.torproject.org.

[83] Propaganda is disseminated by means of social media, videos, forums, publications, online games and merchandising. Twitter and Facebook are exploited as "diaries" that offer nearly real-time coverage of what is happening on the battlefield. The organisation has managed to create an application ("Dawn of Glad Tidings") capable of sending automatic updates and tweets. With regard to recruitment, it is estimated that as of January 2015 approximately 30,000 individuals from more than 80 countries had travelled to Syria and Iraq to sign up with ISIS, 3,000 of whom came from Europe. Online services such as Kik or Skype make it possible for jihadists to communicate and coordinate recruitment and command/control activities in real-time. Ibid. Beatrice Berton and Patryk Pawlak, "Cyber jihadists and their web", in *EUISS Briefs*, No. 2/2015, http://www.iss.europa.eu/publications/detail/article/cyber-jihadists-and-their-web.

[84] ISIS instructs its operatives on how to remain anonymous online: the JustPaste.it website provides manuals the organisation produces on how to use the Virtual Private Network (VPN) or, more in general, how to make online navigation more secure via both browser and mobile phone. As for financing, ISIS is allegedly capable of transferring sums of money to militants operating in the West and vice versa through services such as PayPal and Bitcoin. Many ISIS cyber attacks are aimed at obtaining bank or credit card data. The jihadists also use phishing attacks or buy credit card data stolen online. Ibid.

[85] Democratic Policy & Communication Center, *Glossary of Cyber Related Terms*, cit.

ISSN 2280-6164

the Atlantic Alliance's websites.[86] In May, ISIS-affiliated hackers allegedly managed to hack into the e-mail of several members of the British government that included Home Secretary Theresa May. It remains unclear what information they were able to access, but authorities could not rule out data exfiltration. This prompted various users to change their password and to a revision of security procedures.[87]

While their nature and affiliation with ISIS are not entirely clear, also the Islamic State Hacking Division (ISHD) and the Cyber Caliphate hacker groups have conducted computer operations on behalf of the terrorist organisation. To date, the most reliable assessments lead to the belief that these are autonomous groups ("crews") that ISIS does not control.[88] Their domination of the media was ample inducement to analyse the two groups' activities in 2015.

The photos and addresses of 100 US military personnel were circulated on several jihadist forums in March. ISHD claimed that they had obtained these data after hacking into multiple military servers, databases and protected e-mail services, and that their goal in disseminating them was to make it possible for "our brothers residing in America [to] deal with you."[89] In August, ISHD posted the names, e-mail addresses and other sensitive data of 1,351 US military and government personnel. It is believed that ISHD was led up until then by 21-year-old Junaid Hussain,[90] aka Abu Hussain Al-Britani, who it is supposed was teaching hacking techniques to ISIS recruits before being killed in a US-led raid on 25 August.

Cyber Caliphate first surfaced in an attack on the *Albuquerque Journal* in December 2014. Between 10 and 16 January 2015, following the Charlie Hebdo terrorist attack, Cyber Caliphate launched the #OpFrance operation against thousands of French websites with the support of an informal network of hacker groups and individuals wishing to show their discontent with the Western reaction to the terrorist attack.[91] According to French authorities, approximately 1,300 sites were attacked, but with negligible consequences (mainly web defacement);[92] according to other sources, a

[86] Steven Stalinsky and R. Sosnow, "Hacking in the Name of the Islamic State (ISIS)", in *MEMRI Inquiry & Analysis Series*, No. 1183 (21 August 2015), http://www.memri.org/report/en/0/0/0/0/0/857/8714.htm.

[87] Claire Newell et al., "Cabinet ministers' email hacked by Isil spies", in *The Guardian*, 11 September 2015, http://t.co/8gLdpIHwGa.

[88] Interview, October 2015.

[89] Steven Stalinsky and R. Sosnow, "Hacking in the Name of the Islamic State (ISIS)", cit.

[90] Ibid.

[91] The principal names associated with the campaign include AnonGhost, the Fallaga Team, the Izzah Hackers and Islamic groups such as the Middle East Cyber Army and the United Islamic Cyber Force.

[92] Carola Frediani, "Isis, al Qaeda e la sfida del cyber terrorismo", in *l'Espresso*, 4 February 2015, http://espresso.repubblica.it/plus/articoli/2015/02/02/news/isis-al-qaeda-e-la-sfida-del-terrorismo-informatico-1.197769; Radware, "ISIS Cyber Attacks" in *ERT Threat Alert*, April 2015, http://security.radware.com/uploadedFiles/Resources_and_Content/Threat/ERT%20Threat%20Alert%20-%20ISIS%20Cyber%20Attacks.pdf.

ISSN 2280-6164

portion of these were DDoS attacks.[93] Also in January, Cyber Caliphate succeeded in hacking the Twitter and YouTube accounts of US CENTCOM to post pro-ISIS propaganda and CENTCOM personnel data that the jihadist group claimed to have obtained by penetrating classified networks. That same month, a group known as the "Official Cyber Caliphate" took credit for violating the website of Malaysia Airlines. Beyond web defacement, however, the company maintained there had been no access to its server.[94] In February, the same group accessed the Newsweek Twitter account, which it used to spread ISIS propaganda and "classified material". In April, the Cyber Caliphate hacked into TV5 Monde computers, interrupting its live television broadcast and its website in addition to defacing its Facebook page.[95] In October, the hacker group gained access to approximately 54,000 Twitter accounts that it once again used to post pro-ISIS messages. The majority of the victims who had their data leaked to the web are from Saudi Arabia. Islamic hackers have also publicised the data of the heads of the CIA, FBI and the National Security Agency (NSA).[96]

Al-Qaeda ("The Base"), a terrorist organisation founded in 1988 by Saudi multimillionaire Osama Bin Laden, was responsible for a series of large-scale terrorist attacks such as those of New York in 2001, Bali in 2002 and Madrid in 2004. Successive military operations in Afghanistan, Iraq, Pakistan and Yemen are believed to have significantly weakened the organisation's leadership, although the regional groups that it has spawned continue to pose a serious threat to Western and non-Western security.[97]

Al-Qaeda already displayed an interest in cyber space 20 years ago, when it created its first website, Azzam.com. According to the "39 Principles of Jihad" published in 2003, electronic jihad is a fundamental and sacred duty for all Muslims,[98] and falls within the broader strategic framework of "44 Ways to Support Jihad", which considers the web an important means for disseminating the "holy war" and monitoring its progress. Al-Qaeda's use of internet can be better understood when viewed in function of the "Al-Qaeda 20 years strategy", which demonstrates how jihad online serves to promote propaganda, the radicalisation of the Islamic community and the recruitment of new martyrs.[99]

[93] Steven Stalinsky and R. Sosnow, "Hacking in the Name of the Islamic State (ISIS)", cit.; Radware, "ISIS Cyber Attacks", cit.

[94] Al-Zaquan Amer Hamzah, "Malaysia Airlines website targeted by hacker group 'Cyber Caliphate'", in *Reuters*, 26 January 2015, http://reut.rs/1z0irG4.

[95] Steven Stalinsky and R. Sosnow, "Hacking in the Name of the Islamic State (ISIS)", cit.; Radware, "ISIS cyber attacks", cit.

[96] Swati Khandelwal, "ISIS Supporter Hacks 54,000 Twitter Accounts and Posts Details of Heads of the CIA and FBI", in *The Hacker News*, 8 November 2015, http://thehackernews.com/2015/11/hacking-twitter-account.html.

[97] Mark Hosenball, "U.S. says al Qaeda core weak, but affiliates still threaten", in *Reuters*, 30 April 2014, http://reut.rs/1hTuTjC.

[98] Beatrice Berton and Patryk Pawlak, "Cyber jihadists and their web", cit.

[99] Vito Morisco, "Network jihadisti tra virtuale e reale", in *Il mondo dell'intelligence. Approfondimenti*, May 2015, https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/

ISSN 2280-6164

ISSN 2280-6164

Towards the mid-2000s, six groups could be associated with Al-Qaeda's cyber jihad: Ansar Al-Jihad Lil-Jihad Al-Electroni, Munazamat Fursan Al-Jihad Al-Electroni, Majmu'at Al-Jihad Al-Electroni, Majma' Al-Haker Al-Muslim, Inhiyar Al-Dolar and Hackboy. Over the years, Al-Qaeda has claimed the successful execution of several cyber operations, although the authenticity of those claims is often unverifiable.[100] In March 2013, the Al-Qaeda Electronic Army and the Tunisian Cyber Army claimed they had hacked into Pentagon and US Department of State websites, news that was also reported on the ehackingnews.com website. One month later, a user of the Shumouk Al-Islam jihadist forum discussed Spanish expert Hugo Teso's discovery of the possibility of hijacking airplanes using an Android smartphone.[101] Al-Qaeda Electronic Army's 2015 activities seem to have focused mainly on Western website defacement.[102]

According to some reports, Al-Qaeda and its cyber "legions" frequently chat on online forums on the possibility of conducting cyber attacks.[103] Al-Qaeda targets include SCADA command and control functions, even though it is not known whether the organisation is actually in possession of the technical skills and resources this type of operation requires. On the other hand, one website associated with Al-Qaeda has posted information concerning the execution of DDoS attacks.[104]

Hacktivists

The term "hacktivism", a compound of hacker and activism, refers to the use of cyber space in support of political causes, including freedom of speech and the promotion of human rights.[105] Hacktivist skills have grown exponentially over the years, going from the defacement of sites not particularly defended to complex operations that display techniques very similar to those of cyber criminals and state-supported hackers.[106] To date, these actors have not been reported as having carried out attacks of any particular importance against the critical infrastructures of any country, although a US ICS-CERT report[107] credits them with a series of

network-jihadisti-tra-virtuale-e-reale.html.

100 Steven Stalinsky and R. Sosnow, "From Al-Qaeda to the Islamic State (ISIS), Jihadi Groups Engage in Cyber Jihad", in *MEMRI Inquiry & Analysis*, 5 December 2014, http://cjlab.memri.org/wp-content/uploads/2014/12/cyber-jihad-2.pdf.

101 Ibid.

102 Site Intelligence Group, "Al-Qaeda Electronic", in *Dark Web & Cyber Security*, https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&bind_to_category=content:37&tagId=656&Itemid=1355.

103 Steven Stalinsky and R. Sosnow, "From Al-Qaeda to the Islamic State (ISIS), Jihadi Groups Engage in Cyber Jihad", cit.

104 Ibid.

105 Pierluigi Paganini, "Hacktivism: Means and Motivations ... What Else?", in *InfoSec Resources*, 2 October 2013, http://resources.infosecinstitute.com/?p=21557. ICS-CERT, *Cyber Threat Source Descriptions*, cit.

106 Pierluigi Paganini, "Hacktivism: Means and Motivations ... What Else?", cit.

107 Industrial Control Systems Cyber Emergency Response Team. For the report see: ICS-CERT,

attacks on ICS/SCADA facilities over 2014.[108]

The most famous of hacktivist collectives is Anonymous, a group of hackers formed in the 2000s on behalf of the freedom of online information. After the 2012 arrest of one the group's leaders, Hector Monsegur, and others of the movement, Anonymous appears to have split into a global and a regional components. The global component rarely launches attack campaigns and, for the most part, in reaction to an event or incident. Its regional pro-active versions, on the other hand, conduct frequent computer attacks that are not necessarily in response to any event.[109] The techniques they most frequently use include web defacement, DoS against government sites and/or other major institutions, and SQL-injection.[110] Anonymous' modus operandi usually consists of three phases.[111] In the first phase, a few hacktivists attempt to unite as many persons as possible on social media such as Facebook and Twitter and sites such as YouTube. In the second, the more highly skilled hackers launch a process of reconnaissance using tools such as Nikto and Acunetix to identify weaknesses and then launch an attack against the targeted systems;[112] during the attack, they use special data exfiltration software such as Havij.[113] In the third phase, in case the data exfiltration process has failed, the more highly skilled hackers request assistance from the previously recruited member base in order to launch a DDoS. The attack is carried out using conventional software that can be bought over the web black market or through websites created especially for the attack.[114]

Anonymous did not significantly interrupt or veer from the previous years' activities in 2015, apart from those launched against ISIS supporters and affiliates. They launched a series of attacks in April against Israeli websites to avenge "crimes committed in the Palestinian territories". Although the Israeli Computer Emergency Response Team (CERT) asserted that no Israeli government site had been hacked, Anonymous claimed otherwise, announcing it had stolen 150,000 demographic

ICS-CERT Monitor, September 2014-February 2015, https://ics-cert.us-cert.gov/monitors/ICS-MM201502.

[108] Pierluigi Paganini, "Hacktivism: Means and Motivations ... What Else?", cit. In a message to the Wall Street Journal, Anonymous called the idea of those who attributed the intention to attack the electrical grid to them as ridiculous.

[109] Rob Rachwald, "The Evolving Nature of Hacktivism", in *Imperva Cyber Security Blog*, 8 August 2012, http://blog.imperva.com/2012/08/the-evolving-nature-of-hacktivism.html.

[110] "Results from failure of the application to appropriately validate input. When specially crafted user-controlled input consisting of SQL syntax is used without proper validation as part of SQL queries, it is possible to glean information from the database in ways not envisaged during application design. (MITRE)." See "SQL injection" in *ISACA Glossary*, http://www.isaca.org/Pages/Glossary.aspx?tid=2188&char=S.

[111] Imperva, "The Anatomy of an Anonymous Attack", in *Hacker Intelligence Reports*, February 2012, http://www.imperva.com/download.asp?id=312.

[112] Nikto is a web scanner used to test for web servers' vulnerabilities. It searches for dangerous files, out of date software and other types of problems. Acunetix is a "black box" scanner use to identify website and application weaknesses.

[113] Havij is a tool that reveals a website's SQL-injection vulnerabilities.

[114] Imperva, "The Anatomy of an Anonymous Attack", cit.

ISSN 2280-6164

data (telephone numbers and Facebook, Gmail and Hotmail accounts). Israeli press agencies confirmed that some government sites had been compromised.[115] In June, the masked hackers were responsible for a DDoS attack against the Canadian government's computer system in response to approval of a new counter-terrorism law.[116] In July, the collective succeeded in obtaining US Census Bureau data in reaction to Transatlantic Trade and Investment Partnership (TTIP) and Trans Pacific Partnership (TPP) negotiations that, according to the hackers, threatened to extend intellectual property restrictions to the countries of East Asia.[117] Particularly interesting was Anonymous' reaction to the terrorist attack in which two journalists of the French periodical Charlie Hebdo were killed. Following a week of cyber attacks by ISIS sympathisers and supporters, the hackers collective announced reprisals against anyone who backed violent jihad.[118] According to government sources, between January and July 2015, the hacker group collaborated with the FBI's investigation into the US CENTCOM Twitter account hack, and appears to have hacked into social media accounts used by ISIS to spread propaganda and to have published a list of websites it believes sponsor the jihadist cause.[119] GhostSec, an Anonymous affiliate, is thought to have collaborated with American intelligence and police forces to avert ISIS-planned terrorist attacks in Tunisia and New York.[120]

Cyber criminals and organised crime

Online crime has been abetted in its development over recent years by the ease in communications, the possibility of easily remaining anonymous and obtaining the tools for engaging in illegal activities in cyber space. All this has contributed to making online crime one of the most profitable sectors of the world's economy. Criminal networks who operate almost exclusively in the virtual world have existed for years now. The fulcrum of online crime consists of a group of individuals who meet mainly on the web and very rarely in person. Expert hackers who rarely commit the actual crimes, but act for the most part as coordinators, usually manage these criminal organisations.[121] The weaknesses of various systems are exploited

[115] Pierluigi Paganini, "Anonymous collective hit Israel as part of #opIsrael", in *Security Affairs*, 8 July 2015, http://securityaffairs.co/wordpress/35776.

[116] The attack was confirmed by the Canadian authorities. See: Pierluigi Paganini, "#OpC51 Anonymous hit systems at Canadian Government", in *Security Affairs*, 18 June 2015, http://securityaffairs.co/wordpress/37883.

[117] Paganini Pierluigi, "Anonymous Hacks US Census Bureau against TPP/TTIP", in *Security Affairs*, 25 July 2015, http://securityaffairs.co/wordpress/38817.

[118] Pierluigi Paganini, "Update Charlie Hebdo Tango Down – Anonymous promises to avenge the massacre", in *Security Affairs*, 11 January 2015, http://securityaffairs.co/wordpress/32006.

[119] Pierluigi Paganini, "Anonymous supports FBI investigation of US CENTCOM hack", in *Security Affairs*, 19 January 2015, http://securityaffairs.co/wordpress/32403; Pierluigi Paganini, "Anonymous vigilantes are fighting against the ISIS propaganda", in *Security Affairs*, 30 March 2015, http://securityaffairs.co/wordpress/35486.

[120] Pierluigi Paganini, "Anonymous's team GhostSec thwarts Isis terror", in *Security Affairs*, 26 July 2015, http://securityaffairs.co/wordpress/38860.

[121] Tatiana Tropina, "Cyber Crime and Organized Crime", in *Freedom from Fear*, No. 7 (July 2010), p. 16-17, http://f3magazine.unicri.it/?p=310.

ISSN 2280-6164

with the help of malware such as viruses, trojans, keyloggers[122] and botnets.[123] One of organised crime's main activity is industrial espionage for profit. With massive financial resources at its disposal, it is capable of hiring highly skilled hackers to ensure success. Critical infrastructures can become targets of attacks on behalf of competitors in the same sector, along with trade secrets and confidential data.[124]

Cyber-crime continued to evolve over 2015 with the use of more efficient tactics capable of ensuring ever-richer profits. Competition between vendors of malware has spurred innovation, in some cases going as far as to adopt the use of techniques mainly employed by the most complex government actors. While cyber criminals seem to be interested predominantly in commercial and financial institutions, according to US CERT, there were cyber criminals among the actors that attempted to attack the ICS/SCADA systems of critical American infrastructures in 2014.[125]

3.3 Status of the cyber threat to ATM/ATC systems

Analysis of ISIS and Al-Qaeda's cyber space activities reveal that their hacking skills do not pose an imminent threat to critical infrastructures such as ATM/ATC systems. The level of sophistication of these operations has been well below the amount of media limelight they have enjoyed.

Analysing the Cyber Caliphate accessing of the US Central Command (CENTCOM) Twitter account, various experts have stressed that in order to "violate" the accounts of that famous social medium it is necessary to either guess or otherwise obtain a user's access credentials (password plus username/email/telephone number). That, however, cannot nearly compare to as being able to penetrate much more heavily protected military networks, both classified (NIPRNet) and non-classified (SIPRNet) ones.[126] Regarding the alleged dissemination of classified material, CENTCOM reported that no system had been altered, and that the episode was to be considered "an act of pure vandalism."[127] As for ISHD's alleged theft of data in August 2015, official sources stated immediately after the data were disseminated that no

[122] "Software or hardware that tracks keystrokes and keyboard events, usually surreptitiously / secretly, to monitor actions by the user of an information system." See "keylogger" in NICCS *Cyber Glossary*: https://niccs.us-cert.gov/glossary#keylogger.

[123] "A collection of computers compromised by malicious code and controlled across a network." See "botnet" in NICCS *Cyber Glossary*: https://niccs.us-cert.gov/glossary#botnet.

[124] ICS-CERT, *Cyber Threat Source Descriptions*, cit.

[125] EMC, "Cybercrime 2015. An Inside Look at the Changing Threat Landscape", in *RSA White Papers*, April 2015, http://www.emc.com/collateral/white-paper/rsa-white-paper-cybercrime-trends-2015.pdf; ICS-CERT, *ICS-CERT Monitor, September 2014-February 2015*, cit.

[126] David C. Gompert and Martin C. Libicki, "Decoding the Breach: The Truth about the CENTCOM Hack", in *The Rand Blog*, 3 February 2015, http://www.rand.org/blog/2015/02/decoding-the-breach-the-truth-about-the-centcom-hack.html.

[127] Emma Graham-Harrison, "Could Isis's 'cyber caliphate' unleash a deadly attack on key targets?", in *The Guardian*, 12 April 2015, http://gu.com/p/47at3/stw.

ISSN 2280-6164

list of names and other data had been obtained by cyber attack.[128] In confirmation of this, in October 2015, Kosovo national Ardit Ferizi was arrested in Malaysia for supplying Junaid Hussain with the personal data of 1,351 American soldiers, data subsequently posted on Twitter by the ISIS computer expert.[129] According to the American Department of Justice, Ferizi obtained these data by hacking into the computer system of an American company and not a protected military network.[130] In an another episode, namely the attack on TV5 Monde, in which it seemed the Cyber Caliphate had achieved a much higher level of sophistication than normal web defacement, some analysts have suggested the attacks happened because the passwords of some TV5 users had been broadcast by accident during filming in the television studio.[131] It goes almost without saying that these attacks have nothing to do with attacks on ATM/ATC systems. Therefore, knowing how to access some networks or web services is not proof a hacker has the expertise necessary to penetrate systems with the multi-strata defences that various critical infrastructures have. At most, such violations show the effect – not least the media impact – of damaging the reputation of an individual entity or the "national economic system."

In the case of ISIS then, in none of the cases analysed (which, according to available sources, are the most notorious) did the terrorist organisation demonstrate a technical maturity that would indicate its ability to successfully attack systems subject to much more stringent security policies than a television network or Twitter account are. The same consideration could be made for Al-Qaeda, which has proved less active in cyber space than ISIS, at least over the course of 2015. In conclusion, terrorist organisations have thus far exploited cyber space mainly to make their command and control operations more effective, spread their propaganda and attract financing and recruits. Before they were capable of launching an attack that could produce effects of a certain import, it is probable that there would be signals indicating a significant increase in the sophistication of the attackers' technological skill. Although it is widely recognised that states' critical ICT infrastructures are among the sensitive targets of terrorist organisations, these have not yet demonstrated the intention to specifically attack ATM systems. Nevertheless, this does not rule out an interest in attacking the civil aviation sector in general.

Analyses and assessments by institutional authorities and experts confirm the above. In 2012, the head of American intelligence, James Clapper, maintained that some terrorist organisations appeared to have a growing interest in developing cyber "offensive" capabilities, but that they would probably be hampered by their lack of

[128] "US military data stolen by Daesh's 'Hacking Division'", in *PressTV*, 13 August 2015, http://www.presstv.com/Detail/2015/08/13/424575/ISIL-Hack-US-Military.

[129] US Department of Justice, *ISIL-Linked Hacker Arrested in Malaysia on U.S. Charges*, 15 October 2015, http://www.justice.gov/opa/pr/isil-linked-hacker-arrested-malaysia-us-charges.

[130] Ibid.

[131] "Des mots de passe de TV5 Monde sous les images de France 2 et BFM TV", in *Télé Satellite et Numérique*, 10 avril 2015, http://www.telesatellite.com/actu/45271-des-mots-de-passe-de-tv5-monde-sur-les-images-de.html.

ISSN 2280-6164

resources, organisational limitations and diverse priorities.[132] That judgement does not seem to have changed in 2015, and the threat does not appear to have become more serious: "Terrorist groups will continue to experiment with hacking, which could serve as the foundation for developing more advanced capabilities. Terrorist sympathizers will probably conduct low level cyber attacks on behalf of terrorist groups and attract attention of the media, which might exaggerate the capabilities and threat posed by these actors."[133] According also to US-CERT, known terrorist groups have more primitive cyber capabilities than other actors, and it is less likely they will use cyber space as opposed to other means for achieving their goals. The level of threat posed by these actors is therefore low.[134] Many other analysts share the American authorities' assessment.[135]

Considering the differences in their intentions and targets, hacktivists have demonstrated a higher level of technical skill than the terror-motivated actors analysed above. In addition to web defacement, which does not require much sophistication, acts of DoS/DDoS against institutional websites and data theft from more complex domains such as the Twitter accounts of US CENTCOM and Newsweek continue to be observed, along with a more general and steady increase in these actors' technical prowess. Despite the 2014 ICS-CERT announcement that hacktivists had attacked critical American infrastructures, there has been no confirmation that ATM/ATC systems constitute a specific target. Mainly as regards the Anonymous case-study, according to available sources to date the group has given no indication of their intention to strike targets in a manner that could endanger human lives; rather, that their intention is to target institutions and/or individuals not aligned with their ideology.

In general, according to the American authorities, hacktivists constitute a medium-level threat, given their capability for isolated, albeit damaging, attacks against critical infrastructures. Individuals or small groups of hackers, on the other hand, do not appear to pose a critical threat, although the level of danger increases

[132] James R. Clapper, *Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence*, 31 January 2012, https://www.hsdl.org/?abstract&did=699575.

[133] James R. Clapper, *Worldwide Cyber Threats*, Statement for the Record, House Permanent Select Committee on Intelligence, 10 September 2015, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/ClapperOpening09102015.pdf.

[134] ICS-CERT, *Cyber Threat Source Descriptions*, cit.

[135] Also according to Tobias Feakin, ISIS and their affiliates are not capable of launching complex attacks against vital networks. See: Tobias Feakin, "A Deadly Mistake: Don't Underestimate ISIS in Cyberspace", in *The Buzz Blog*, 1 June 2015, http://nationalinterest.org/node/13014. The same assessment is offered by Pano Yannakogeorgos, according to whom the terrorists do not currently have the necessary skills to gather data on exploitable vulnerabilities of complex ICT systems and/or to create malware to use against them. See: Pano A. Yannakogeorgos, "Rethinking the Threat of Cyberterrorism", in Thomas M. Chen, Lee Jarvis, Stuart Macdonald (eds.), *Cyberterrorism. Understanding, Assessment, and Response*, New York, Springer, 2014, p. 56. For an opposing view, see computer security expert Mikko Hyppönen: Pierluigi Paganini, "Mikko Hyppönen warns the ISIS has a credible offensive cyber capability", in *Security Affairs*, 26 October 2015, http://securityaffairs.co/wordpress/41438.

ISSN 2280-6164

significantly when considering the hacker community in its entirety.[136]

Finally, the vast world of cyber crime has continued to evolve technologically, as highlighted by the use of instruments previously reserved for more sophisticated actors. Even if it is difficult to draw exact conclusions on the acts of a number of especially skilled actors, the techniques and instruments cyber criminals are using reflects their primary objective: profit. In keeping with this logic, the interruption of air traffic control and management services would not seem to correspond with their ultimate aims, but only expose them to unwanted visibility.

Nevertheless, in light of their ability to carry out industrial espionage, and the financial resources available for their recruitment of skilled hackers, cyber criminals and organised crime do pose a medium-level threat.[137]

4. The Italian Case Study

This chapter attempts to respond to the questions raised in the introduction to this study. The first section will outline the role of ENAV, the company that provides ATM/ATC services in Italy, along with the architecture and systems employed by the organisation.[138] The second section confronts the issue of the cyber threat to Italy. The third section summarises the main points of the previous two, and assesses the eventual vulnerability of ENAV ATM/ATC systems and the extent to which the non-state actors considered have the technical capability to attack them.

4.1 ENAV and air traffic management in Italy

Eurocontrol, an intergovernmental organisation with a membership of 41 European countries and neighbours (Turkey, Armenia and Georgia), is principally engaged in developing and maintaining an efficient European-level air traffic management system. It operates in collaboration with each member's national civil aviation authority (ENAC in Italy[139]), ATM/ATC service agencies and providers (ENAV and

[136] ICS-CERT, *Cyber Threat Source Descriptions*, cit.

[137] Ibid. In general, when considering the civil aviation sector specifically, the ICAO "Threat and Risk" working group concluded that the cyber risk was low for 2015.

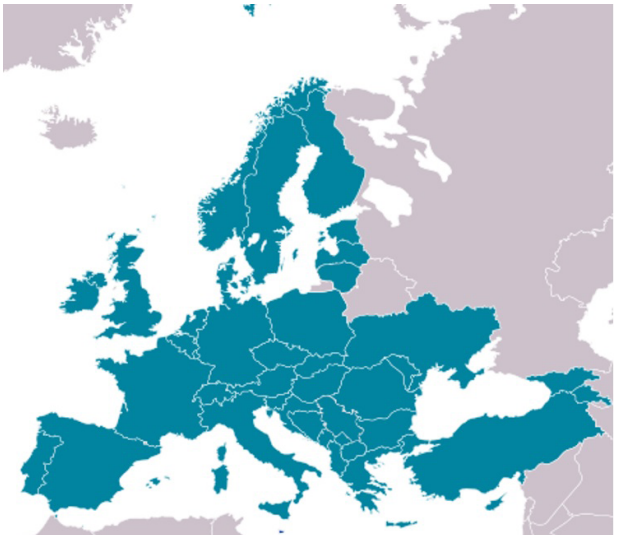
[138] Within the limitations of the laws on confidentiality regarding the technologies used by critical infrastructures.

[139] Italy's Civil Aviation Authority, ENAC, is subject to the control of the Ministry of Infrastructure and Transport. Its main areas of authority are: 1) technical regulation, inspection and maintenance of registers/professional associations; 2) rationalisation and modification of procedures pertaining to airport services; 3) coordination with ENAV and the Air Force; 4) relations with national and international agencies, companies and organisations operating in the civil aviation sector; 5) preliminary evaluation of acts concerning duties, taxes and airport charges; 6) setting and monitoring of airport and air transport service quality parameters; 7) regulation and evaluation of regulatory, intervention and airport investment plans. The Navigation Code also establishes ENAC as the sole acting authority in technical regulation, certification and vigilance in the civil aviation

ISSN 2280-6164

the Air Force in Italy), users of civilian and military air space, the industrial sector, professional associations and designated European institutions.[140]

Figure 4 | Eurocontrol Member States



Eurocontrol is responsible for the study and analysis of air navigation and management services security. On European Commission mandate, Eurocontrol is in charge of the Network Manager Operations Centre (NMOC), a unit whose purpose is to harmonise and optimise flight plans concerning Europe, and the Central Route Charges Office (CRCO), a system for the recovery of ATM services' costs made available to airspace users. A member state convention created the Safety Regulation Commission (SRC) to generate reports and recommendations on improving air traffic control security and to propose the adoption of regulations based on the requirements established by the Eurocontrol Safety Regulatory Requirements (ESARR).

ATS in Italy is mainly provided by ENAV,[141] which generally deals with civilian, non-operational military and government national air space traffic (approximately 751,000 km^2), including authorised airports.

ENAV manages four ACCs located at the Milano-Linate, Padova/Abano Terme, Roma-Ciampino and Brindisi-Casale airports. Air space is vertically subdivided into upper and lower air space. Lower air space is subdivided into the three FIRs of Brindisi, Roma and Milano. The first two ACCs are managed respectively by the Brindisi-Casale and Roma-Ciampino FIRs, while the western section of the Milano

sector.

[140] Eurocontrol was established with the Eurocontrol Convention (13 December 1960). Data available here: http://www.eurocontrol.int.

[141] At smaller airports, such as Aosta and Tortolì, ATS services are provided locally by airport management companies.

ISSN 2280-6164

FIR is managed by Milano-Linate and the eastern by Padova/Abano Terme.[142] FIR upper horizontal airspace is similarly subdivided.[143]

Figure 5 | ACC air space subdivision

ATM/ATC services

ENAV provides pilots and aeronautics operators with an aeronautics information service, whose data are prepared by the Aeronautical Operational Information System (AOIS). This is a national online system consisting of a central, ENAV-owned database that handles all aeronautics data essential to ensuring safe air traffic flow (flight plans, Notices To Air Men (NOTAM), ATFM slots, meteo bulletins). The AOIS Data Processing Centre works on the company's network, with satellite backup in case of disruption. The AOIS makes data available to the four ACCs and 42 airports where ENAV manages air traffic services. AOIS data are made available to the entire aviation community (Italian Air Force, aeronautics operators, airport handling companies and aviation authorities) either electronically or through the ENAV Air Traffic Services Reporting Offices located in the Milano-Linate and Roma-Fiumicino airports, where air traffic services data and flight plans are received before take-offs.[144]

The ATS Message Handling Service (AMHS) standard was established at European level with a view to modernising ATS message exchanges (NOTAMs, flight plans, meteo bulletins, slot messages, etc.), in the context of the aeronautical

[142] Italy has adopted ICAO classification, although it does not use classes B or F, as follows: class G for the three FIRs, classes C and G for the three UIRs and classes A, D and E for TMAs.

[143] Italian UIRs are further subdivided vertically into two portions.

[144] Vitrociset note, July 2015.

ISSN 2280-6164

telecommunication fixed service, which is based today on the Aeronautical Fixed Telecommunication Network (AFTN) and the Common ICAO Data Interchange Network (CIDIN) standards. The AMHS system is currently flanked by the AFTN/CIDIN network, although this latter will gradually be phased out in accordance with ICAO directives, up to its complete replacement within 2020.[145] According to ICAO ATN SARPS manuals,[146] the AMHS implements the X.400 protocol communication standard,[147] which is employed for ATS message exchanges on an ATN in store-and-forward mode. Various European ANSPs have been using AMHS systems for years now, relying on a network based on TCP/IP. In addition to the technological advantages over AFTN/CIDIN, AMHS offers a broader range of functions that allow for increased message exchanges, binary data exchanges, or messages from authentication mechanisms.[148]

ATM/ATC system architecture

ENAV telecommunications connectivity is ensured by a new integrated operational communications network known as E-Net, which is in the process of being completed. The E-Net programme aims to connect all ACCs, airports, air control tower radio and radar centres through a per-site and per-service modular telecommunication system. The final objective is to improve the reliability and availability of communications on local sites, access to the geographic network and national transportation.

To ensure the maximum resilience, the logical level of the access components is based on Internet Protocol (IP) technology for some services (AFTN, AOIS, weather, OLDI, Radar, etc.) and on pure Asynchronous Transfer Mode (ATM) technology for others (operational telephony, Air Control Tower radio, etc.).[149]

[145] Ibid.

[146] Standards and Recommended Practices (SARPS) Aeronautical Telecommunication Network (ATN).

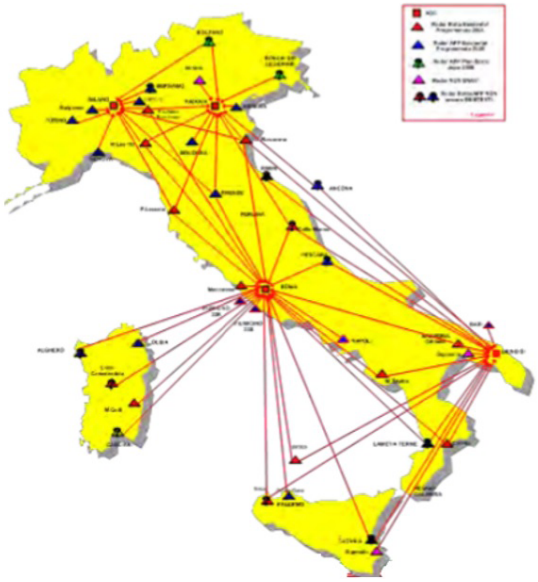
[147] X.400 is a series of recommendations by the Telecommunication Standardisation Sector of the International Telecommunication Union (ITU-T) for the creation of a standard Message Handling Systems analogous to Internet email.

[148] ENAV stipulated an accord with Vitrociset calling for an upgrade of the AFTN/CIDIN (previously provided by Vitrociset) to the new AMHS system. See: Vitrociset, *Vitrociset provides to ENAV the AMHS system (ATS Message Handling System)*, 26 January 2010, http://www.vitrociset.it/dett_editoriale.php?id_editoriale=71.

[149] Ibid.

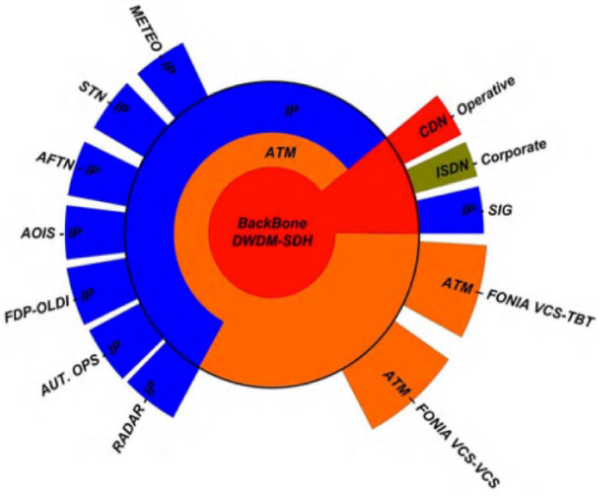
ISSN 2280-6164

Figure 6 | E-Net networks in Italy



Source: Enav.

Figure 7 | E-Net network protocols and association with operational services

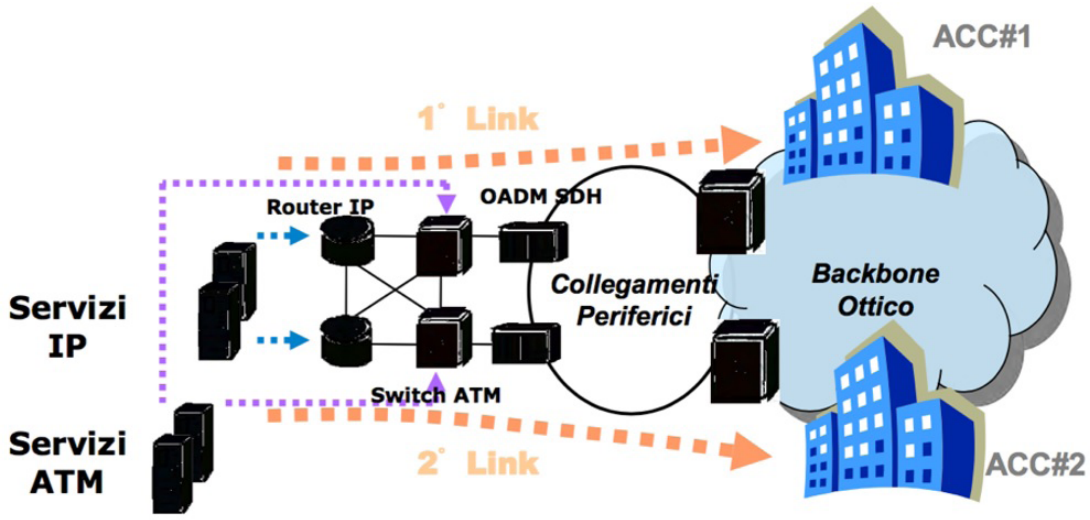


Source: Vitrociset.

The E-Net is distinguished by a national "backbone" consisting of an high-capacity protected connection between ACCs and airport flight assistance systems, as well as ground connections between airports, radar rooms, air control tower radio centres and backbone sites.

DOCUMENTI IAI 15 | 23E - DECEMBER 2015
ISSN 2280-6164

Figure 8 | E-Net ground connection layout between airports, radar rooms, air control tower radio centres and backbone sites



The new network architecture connects ENAV to the integrated European network for ground-to-ground communication (Pan European Network Services, PENS), which links the various Eurocontrol locations and the sites of the various European ANSPs.[150]

E-Net pursues the following objectives:[151]

- creation of a national network for ENAV operational communications;
- elimination of current "single points of failure"[152] in telecommunications infrastructure;
- duplication of the type of transmission support ("protection") for more critical applications (Voice/Tower-Air and radar data);
- assurance of service quality by means of specific service-oriented contracts for each application;
- compliance with Eurocontrol and national safety and security requirements for Gate-to-Gate and Single Sky frameworks according to the EATMP Communications Strategy;
- development of collaborative decision-making modes with other aviation actors, particularly airports, in anticipation of the new generation System-Wide Information Management (SWIM).

[150] Eurocontrol, *Pan-European Network Services (PENS)*, http://www.eurocontrol.int/node/1514.

[151] ENAV, "Nel programma E-Net le soluzioni abilitanti per le applicazioni aeronautiche del futuro di Enav", in *Cleared*, Vol. VI, No. 9 (October 2009), p. 4-5, http://www.enav.it/ec5/enav/it/pdf/cleared/CLEARED_5_09.pdf.

[152] Individual components (hardware or software, in general) that in case of malfunction or anomaly cause the dysfunction of the entire system.

ISSN 2280-6164

The ENAV approach is to keep the internal operational and management networks separate, making a clear physical and logical border between the two. Two Points of Presence (PoP), called External Network Interfaces (ENI), have been created on the public network[153] for communication purposes. The two PoPs offer both connection and traffic flow services between E-Net and the infrastructure of each third party connected, as well as an E-Net perimeter protection service. In addition to ensuring greater connection flexibility, the two PoPs are also geographically redundant for some services in the case that one of the two terminals crashes. The ENI Security Modules (SM), in addition to providing firewalling[154] with very high granular traffic analysis, also have advanced Intrusion Detection Systems (IDS)[155] to analyse traffic at application level. Access is permitted exclusively to "trusted" entities according to responsibility/authorisation configurations and stringent traffic policies. The ENAV Security Operation Centre (SOC) receives and analyses events recorded by ENI-MS IDSs and looks out for abnormal or malicious activity, with "behavioural" checks[156] based on a pre-codified alarm scale.[157]

The AOIS service makes aviation navigation data available to users. These data are contained in a database that uses Web/Linux J2EE technology with an Oracle database located in the Ciampino ACC, to which several of the airport terminals have access. Data flow uses a TCP/IP protocol.[158]

The AOIS service has three distinct types of infrastructure:
- the Ciampino ACC houses the AOIS mainframe[159] and terminals;
- remote ACCs (Brindisi, Padova, Milano);
- C/M type airports and S type airports.

The network infrastructure foresees a Local Area Network (LAN) in the Ciampino ACC that connects the AOIS mainframe (being phased out) and the terminals. This system uses the E-Net to disseminate data, and alternatively the public network in cases of emergency, with the appropriate dedicated Internet security and segmentation arrangements. Remote connections rely on routers and a series of switches,[160] which are protected by security checks based on the latest generation

[153] PoPs are interface access points.

[154] Firewalls are systems that analyse data traffic between an internal and external network in function of a set of security rules, and they block any communications that violates those.

[155] Intrusion Detection System technology is used to detect harmful intrusions into a system (Host IDS) or network (Network IDS).

[156] Behaviour-based IDS attempt to detect intrusions based on anomalous behaviour by systems or users or, in any case, different to expected behaviour.

[157] Interview, November 2015.

[158] Vitrociset note, cit.

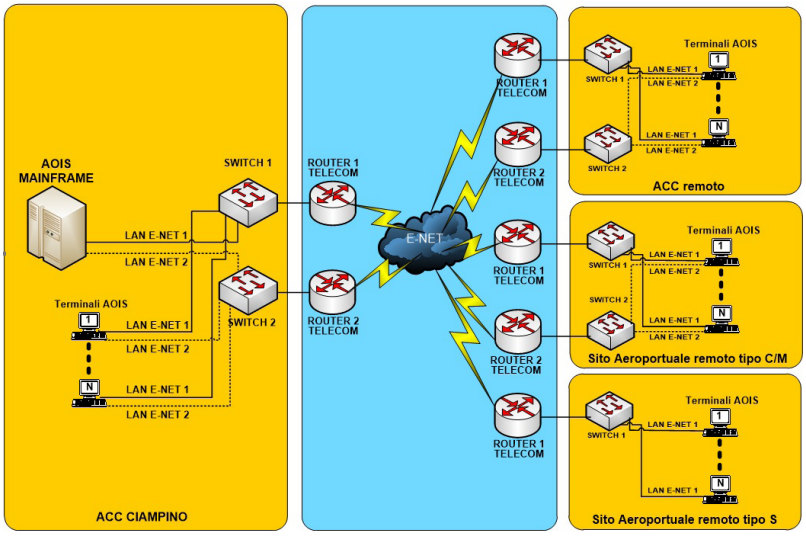
[159] Computers, typically very large and with vast computational capacity, used by major organisations for critical activities and massive processing, to which users connect from remote terminals. The name derives from the first mainframe computer's similarity to a large wardrobe.

[160] Ibid. Routers and switches are devices used to connect networks. Routers are typically used to connect a local network with another that provides external connectivity. Switches are used to segment and separate local high-speed networks.

ISSN 2280-6164

firewall, centrally managed and monitored by the SOC.

Figure 9 | AOIS E-Net service



Note: The figure does not show the security component, which exists and is redundant at every site interface.

The AOIS data processing centre ensures continuity of its activities through the E-Net and a satellite network[161] as backup. The AOIS places data at the disposal of the four ACCs and 42 airports (43 from 10 December 2015, with the addition of the ATC service of the Brindisi-Casale former military airport) ENAV handles the aviation navigation services for. AOIS data are made available to the entire aviation community (Air Force, aeronautic operators, airport management firms and aviation authorities) either electronically or at ENAV's ARO offices. Using a high-speed connection with the International Communications Centre (ICC), ENAV is linked with the aviation telecommunications network, known as the AFTN, which transmits all ATSs (flight plans, NOTAMs, meteo bulletins and slot messages) worldwide. The AOIS system handles approximately 50,000 incoming and approximately 7,000 outgoing messages daily.[162]

The AOIS system makes it possible to:

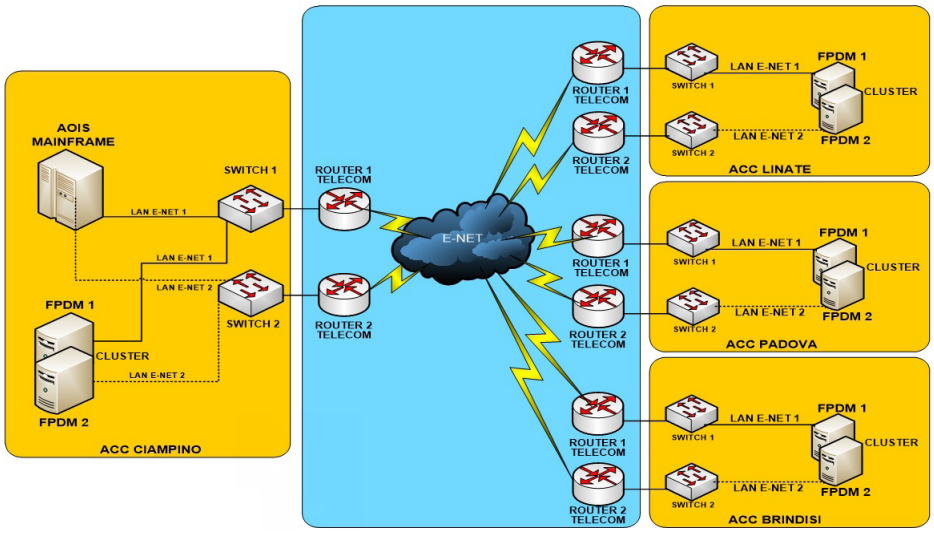
- submit flight plans directly for Eurocontrol validation;
- obtain flight security data in real time (NOTAMs, flight personnel advisories);
- visualise ATFM slots assigned to outgoing planes in the case of flights subject to flow regulation;
- consult weather bulletins.

[161] A digital telecommunications network, now partially obsolete, that provides telephony, telefax, teleconference and additional services (caller ID, call-forwarding, multi-number) and low speed data transmission (two bidirectional channels at 64kb/s and another at 16kb/s).

[162] ENAV, *Aeronautical Information*, http://www.enav.it/portal/page/portal/PortaleENAV/Home_EN/ServiziEAttivita_EN?CurrentPath=/enav/en/services/aeronautical_information.

ISSN 2280-6164

Figure 10 | AOIS-FPDM services on E-Net



Note: This figure omits the, nevertheless existing, stratum of security provided by centrally managed redundant modules.

The network infrastructure consists of highly reliable circuitry and redundant systems designed to ensure continuity of operations, to be immune from interferences and to reduce to a minimum the possibility of service interruption, even when owing to serious malfunction, according to strict backup, disaster recovery and configuration management standards that apply to all ATC centres.

The integrated AFTN-CIDIN-AMHS central system of the Roma Ciampino ICC, which operates on a Linux platform, permits both national and international users AMHS message exchanges, and ensures inter-operability with the national and international AFTN/AMHS network.[163]

The AFTN-CIDIN-AMHS central system allows for linkage of the following ATM/ATC systems:

- the integrated AFTN-CIDIN-AMHS central system of Fiumicino, through dual Wide Area Network (WAN) system on E-Net;
- User Agent stations (AMHS terminals at airport AROs) of the national periphery through E-Net;
- AOIS system of the Roma Ciampino ICC;
- Rome FDP system;
- Milan FDP system;
- Brindisi FDP system;
- Italian Air Force ReSIA's AFTN system;
- Italian Air Force's CNMCA weather centre;[164]
- SETINET system for AMHS connection to the Geneva AMHS;

[163] Ibid.

[164] National Centre for Aviation Meteorology and Climatology.

ISSN 2280-6164

- European PENS network for AMHS Europe connection;
- Bankok AMHS system by means of a dedicated circuit made available by ENAV at the Roma Ciampino ICC (TCP/IP connection).[165]

With regard to flight data, ENAV provides a simple and innovative Self-Briefing service it calls "The New Generation of Pre-Flight Information Systems," a dedicated portal by which aeronautical operators, pilots and organisations may access pre-flight data. With this system, Users can independently provide aeronautic information and pre-flight documentation in few steps.[166]

Figure 11 | The New Generation of Pre-Flight Information Systems

The service comes in the form of a web application that uses a Transport Layer Security (TLS) for secure log-on,[167] and ensures communication privacy, integrity of exchanged data and server identity. User IDs are checked by means of a traditional, single-factor username/password authentication system. The system does not refer to the flight plans submitted by airlines, but to those submitted by users, and contains measures for verifying data, in compliance with international standards established in the technical annexes of the Chicago Convention.

Since it accepts user input (at least insertion of identification credentials) and uses Javascript, the web application is potentially vulnerable to (D)DoS, SQL-injection, cross-site scripting, cookie hijacking and other forms of command injection attacks.[168] These could have consequences ranging from the service temporary

[165] ENAV, *Aeronautical Information*, cit.

[166] ENAV issues a disclaimer on the service's access page saying that, during the validation and testing phase of the service, it relieves itself of all responsibility for the correctness, completeness and accuracy of the data provided through the Self Briefing portal. ENAV assumes no responsiblity of any kind either implicit or explicit.

[167] Defined in RFCs 2246, 4346, 5246 and 6176 of the Internet Engineering Task Force (IETF).

[168] "Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web

ISSN 2280-6164

suspension and system compromise, including its supporting database, to attacks on the browsers the user employs to connect to the service. However, penetration tests conducted according to OSSTM[169] and OWASP[170] guidelines have ascertained the absence of known vulnerabilities, according to the security ENAV security standards.[171]

ATC systems

The following is a description of ATC systems, inclusive of the control, communication and surveillance systems, used during the various phases of air traffic control.

The FDP is the ATC system that processes flight plan data for a variety of purposes, and it supplies air traffic controllers with a broad range of flight plan information. The FDP system provides a 30/60-minute forecast of air traffic conditions that make it possible to anticipate danger situations and take effective traffic planning decisions.[172]

The Control Working Position (CWP) is the air traffic control station whose monitors display current air traffic conditions, integrating the tactical data emitted by radar systems and by the FDP. It integrates the multiple systems the controller needs for its activities: radar screens, aeronautical charts and maps, electronic strip displays, weather conditions, airport surface traffic, communication systems, systems for predicting possible medium to short term flight trajectory conflicts, which help controllers resolve flight separation issues.[173]

application uses input from a user within the output it generates without validating or encoding it." See OWASP, *Cross-Site Scripting*, https://www.owasp.org/index.php/Cross-site_Scripting_(XSS). "The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token. Because http communication uses many different TCP connections, the web server needs a method to recognize every user's connections. The most useful method depends on a token that the Web Server sends to the client browser after a successful client authentication. A session token is normally composed of a string of variable width and it could be used in different ways, like in the URL, in the header of the http requisition as a cookie, in other parts of the header of the http request, or yet in the body of the http requisition. The Session Hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server." See OWASP, *Session hijacking attack*, https://www.owasp.org/index.php/Session_hijacking_attack.

169 The Open Source Security Testing Methodology of the Institute for Security and Open Methodologies, a non-profit organisation registered in Spain: http://www.isecom.org/research/osstmm.html.

170 The Open Web Application Security Project is the best known community on the theme of web application security: https://www.owasp.org.

171 Interview, November 2015.

172 Vitrociset note, cit.

173 Ibid.

© 2016 IAI ISSN 2280-6164 DOCUMENTI IAI 15 | 23E - DECEMBER 2015

ENAV is especially attentive to ground-air telecommunications, which are fundamental for air traffic management. These work on the E-Net network and following an approach based on physical and logical redundancy.[174]

Every aircraft is equipped with a receiver/transmitter apparatus that permits communication between pilots and ground control using an analogue system operating on VHF/UHF frequencies. In an effort to improve service and reduce VHF voice communication congestion, the tendency is to use the Controller Pilot Data-Link Communication (CPDLC) system that allows for the exchange of digital messages.[175]

Air traffic radar control combines data of various radar sensors, which are later elaborated by specific systems and then made available to air traffic controller. Radar control continues throughout the cruise until landing.[176] Aircraft surveillance is a rapidly expanding sector, with efforts (Galileo-Egnos, Aireon, Glonass, among others) under way across the world to develop collaborative systems using geostationary satellite constellations in order to permit the precise and resilient recognition of aircraft. Various working groups are analysing these systesm aspects, including security. ENAV directly participates in two programmes: Galileo-Egnos, through the European Satellite Services Provider (ESSP) consortium[177] and Aireon,[178] of which it is a stakeholder.[179]

The Advanced Surface Movement Guidance and Control System (ASMGCS) is a ground surveillance system that receives and correlates data from various surveillance sub-systems.[180]

The ATM Surveillance Tracker and Server (ARTAS) is a system designed by Eurocontrol to provide an accurate "air situation picture" in a well-defined geographical area, and to disseminate that data to a series of appropriately connected systems.[181]

[174] The control of frequencies is provided by the Ministry of Economic Development from its central and regional offices. ENAV has an agreement with the Department of Public Security that provides, through the Postal and Communications Police Service, for the rapid intervention by police, not least in cases of radio-electrical interference phenomena. Law No. 110/1983 entitled "Defence of Radio Communications Relative to Flight Assistance and Security" permits supplementary administrative and judiciary bans on interference in air traffic control radio networks.

[175] Vitrociset note, cit.

[176] Ibid.

[177] ESSP, *Company Structure and Ownership*, http://www.essp-sas.eu/company_structure.

[178] Aireon, About Aireon, http://aireon.com/company.

[179] Interview, November 2015.

[180] Vitrociset note, cit.

[181] Ibid.

ISSN 2280-6164

The ATIS is an automated system that provides pilots with continuous meteorological and operational data concerning on a particular airport. It uses a dedicated frequency or can be associated with a VOR transmitter[182] (the D-ATIS transmits via data link).[183]

The Satellite Distribution System (SADIS) is a satellite system that transmits updated information and high-resolution weather images.[184]

ENAV security strategy

ENAV security strategies are based on detailed definition of the principles by which the company ensures data security. The provision of aviation navigation services, as described by law, is a public service that serves the national interest.[185]

European regulation is especially severe in requiring ATM/ATC services suppliers a "security management system" compliant with the common requirements, which is laid down in Article 4 of Annex I of EU Regulation 1035/2011.[186] In order to keep their certification as ATM/ATC services providers, ENAV and other ANSPs must comply with this regulation.[187]

This principle laid the foundation of ENAV's decision to undergo a certification process according to ISO international standard 27001:2014, with the objective to rendering its entire "security life-cycle" objective and measurable, even by third-party assessment. This process also extends to evaluation of aspects related to physical security, human factor and processes, and is heavily integrated with other ENAV's management principles: quality measurement ISO 9001 and the "Safety Management System" regarding aviation operational security.[188]

The entire security process takes place in compliance with a method known as the "Deming Cycle", which requires the commitment of the company's management and a particularly rigorous and pervasive process of risk analysis. The approach hinges on simple principles, which intend to go beyond the traditional perimeter-defence and multi-strata security approach and aim to secure networks, systems, software and processes by adopting a detailed risk management plan inspired by

[182] VHF Omnidirectional Radio Range.

[183] Vitrociset note, cit.

[184] Ibid.

[185] Regulation (EC) No 550/2004 on the Provision of Air Navigation Services in the Single European Sky, 10 March 2004, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32004R0550.

[186] Commission Implementing Regulation (EU) No 1035/2011 laying common requirements for the provision of air navigation services..., 17 October 2011, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32011R1035.

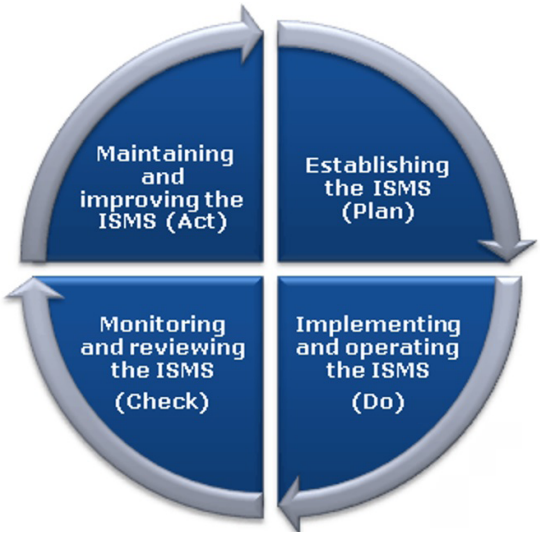
[187] It must also be kept in mind that, according to Article 40 of the Penal Code, being in a position to guarantee obligates the adoption of all practicable measures, in as much as "Failing to prevent an event which one has a legal obligation to prevent shall be equivalent to causing it."

[188] Interview, November 2015.

ISSN 2280-6164

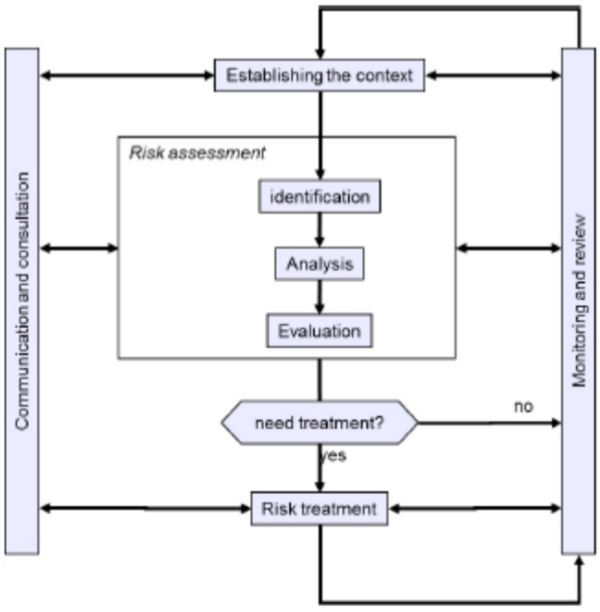
ISO standard 31000,[189] as the following figure illustrates.

Figure 12 | Deming cycle for an information security management system



ENAV is the only certified provider in Europe, which has allowed it to design a process for targeting weaknesses based on risk analysis, with a security management that fosters best practices and their dissemination.

Figure 13 | Risk management process (ISO 31000)



[189] ISO, *ISO 31000 - Risk management*, http://www.iso.org/iso/iso31000.

© 2016 IAI
ISSN 2280-6164
DOCUMENTI IAI 15 | 23E - DECEMBER 2015

As regards risk assessment, ENAV employs the Magerit method and the Pilar application,[190] which allows immediate assessment of the relationship between risks, assets, risk management and mitigation, with particular attention to "operational continuity management" measures.

There is a corporate function specifically designed for logical security management that strictly applies the "separation of duties" principle[191] and that relies on a multifunctional SOC. The SOC is integrated with "physical security" and it was established in 2009.[192]

ENAV's SOC manages security in a centralised manner through specific processes, procedures and technologies, and cooperates with various internal and external actors/entities. The SOC's monitoring domains are the security of non-operational services, operational services and the E-Net network. Its functions include the centralised management of access control and intrusion detection; alarms and advisories; security events; coordination of police forces and ATS unit surveillance personnel; crisis management support; and physical security events management. It also performs intelligence activities by correlating physical and logical events, employing a multi-strata architecture with a massive use of open source software and certified resources, all of which are internal.

The SOC supports all the company's information security activities, and contributes, in the presence of specific mandate from the managerial leadership, to define the domain and secure software requirements, as well as to suggest security checks in the design phase. It also issues automatic vulnerability and compliance monitoring assessments. The following figure illustrates the support services provided by the ENAV SOC.

Along with other actors operating in the security and defence domain, ENAV participates in the implementation process of the national cyber strategy,[193] as it is part of the national security and defence network, in accordance with the organisation's nature and mission.[194]

[190] Magerit is a risk analysis and management method created by Spain's Consejo Superior de Administración Electrónica to minimise risk in the use of Information Technologies, with a special focus on government administration. Magerit provides the "Pilar" application for the purpose.

[191] A principle on the basis of which the design of systems and their use, and the proposal of security requirements and their monitoring must be entrusted to separate organisation actors in an effort to reduce, if not eliminate, potential conflicts of interest.

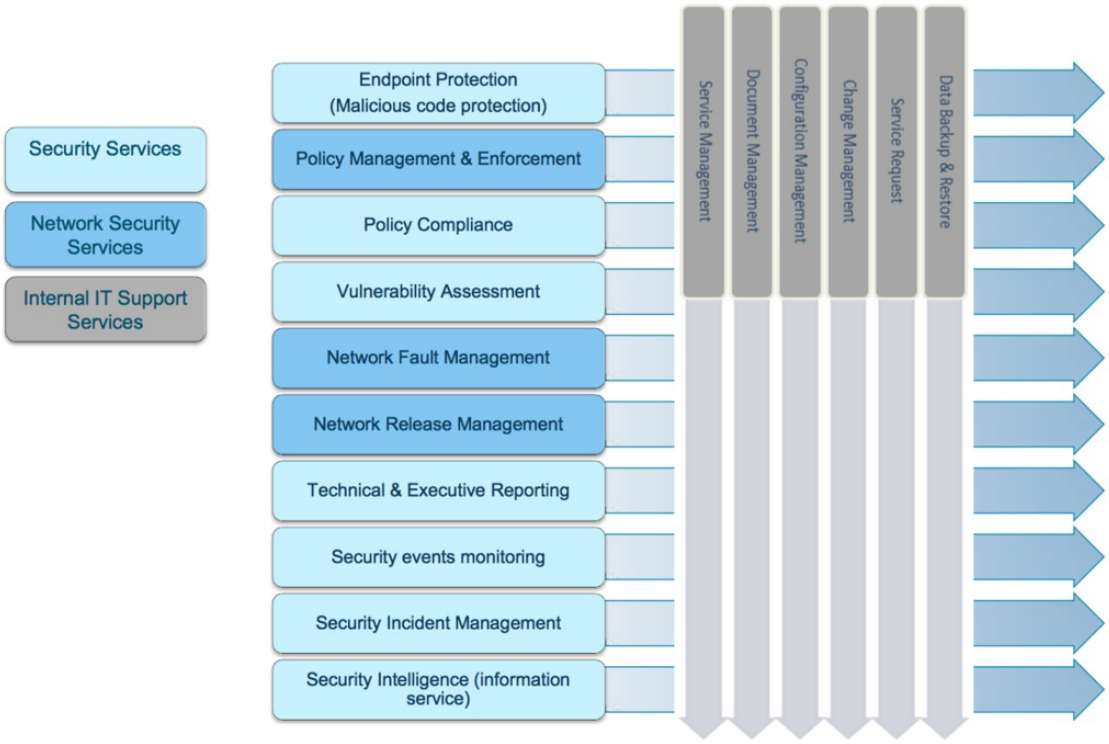
[192] Interview, November 2015.

[193] Italian Presidency of the Council of Ministers, *National Strategic Framework for Cyberspace Security*, cit.; and *National Plan for Cyberspace Protection and ICT Security*, December 2013, http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf.

[194] Polizia di Stato, *Sicurezza: rinnovato l'accordo tra Polizia di Stato ed Enav*, 22 January 2015, http://www.poliziadistato.it/articolo/view/37318; Stefania Ducci, "Moving Toward an Italian Cyber Defense and Security Strategy", in Daniel Ventre (ed.), *Cyber Conflict. Competing National Perspectives*, London, Wiley / Hoboken, Iste, 2012, p. 165-191.

ISSN 2280-6164

Figure 14 | Catalogue of ENAV SOC Services



4.2 Cyber threats to Italy

Terrorist organisations (ISIS and Al-Qaeda)

ISIS considers Italy a legitimate target based on its role in the coalition against the terrorist organisation in Syria and Iraq and because of the symbolic value of Rome.[195]

As has happened with other governments participating in military operations in the Middle East, Italy too was allegedly a target of ISIS cyber attacks in 2015. The most noteworthy episode took place in May 2015 when ISIS supporters posted a document signed by ISHD on Twitter containing the personal data of ten Italian military personnel. In the document, ISHD claimed they had accessed a "secure server" in the same way they had when they posted the data of some American military personnel in August 2015. The document, posted on the Justpaste.it website, was later tweeted under the hashtag #WeWillBurnRome.[196] It read as

[195] Italy's Intelligence System for the Security of the Republic, *Relazione sulla politica dell'informazione per la sicurezza 2014*, February 2015, p. 31, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2015/02/relazione-2014.pdf.

[196] Steven Stalinsky and R. Sosnow, "Hacking in the Name of the Islamic State (ISIS)", cit.; Site Intelligence Group, "'Islamic State Hacking Division' Calls for Attacks on 10 Italian Army

ISSN 2280-6164

follows (translated from the Italian):

> "We will conquer Rome, and Aqsa, we will destroy your crosses, with the blessing of Allah. I'm back although the disbelievers dislike it. We swear on Allah that we would enter [sic] and would conquer [sic] Rome and it won't be long... A message to the lone wolves we await your surprises Italy has declared war and we declared long ago Aljihad Aljihad Aljihad. Thus it will be us who will bring the jihad to your land. You have said that the hand of America is long and can reach everywhere, so know that our knives are sharp: they cut the hands and throats of disbelievers."[197]

Apart from this episode, "offensive" (or so-alleged) cyber activity on the part of ISIS or their supporters and affiliates, has mostly been in the form of low-level computer attacks. Examples include the web defacement of the sites of the Lombardy Region, the Tuscany division of the Democratic Party and the Accademia della Crusca.[198] Nevertheless, it cannot necessarily be taken for granted that these acts are ascribable to ISIS or that they were meant to target Italian institutions. Indeed, it is possible that groups of hackers that support the jihadist cause launched online programmes that automatically affected web sites lacking in any particular protection.[199]

The cyber activities of ISIS and their supporters have mainly taken the form of threats that have used the web as a propaganda tool. In 2015, significant examples included intimidating threats against Italy and Europe (identified as possible targets of ISIS "missiles"), Italian foreign minister Paolo Gentiloni (described as the "minister of the Italian crusade") and, finally, Italy in general (in a book available online that calls for ISIS to team up with the Mafia to conquer Rome).[200] A Tunisian and a Pakistani arrested in July were, according to the authorities, "at very serious risk of carrying

Personnel", in *Dark Web & Cyber Security*, 1 June 2015, https://ent.siteintelgroup.com/Dark-Web-and-Cyber-Security/site-6-1-15-ishd-calls-for-attacks-on-10-italian-army-personnel.html; Alessandro Burato, "Islamic State Hacking Division ai 'lupi' di IS: 'Colpite i soldati italiani'", in *ITSTIME*, 20 July 2015, http://www.itstime.it/w/?p=1962.

197 Alessandro Burato, "Islamic State Hacking Division ai 'lupi' di IS: 'Colpite i soldati italiani'", cit.

198 "Hacker pro Isis su sito web Lombardia", in *Ansa Cronaca*, 2 February 2015, http://www.ansa.it/sito/notizie/cronaca/2015/02/02/hacker-pro-isis-su-sito-web-lombardia_7035dab0-d8de-4c8c-84ab-6c28ccc2d5c6.html; "Hacker su sito Pd Toscana, sigla Isis", in *Ansa Toscana*, 7 March 2015, http://www.ansa.it/toscana/notizie/2015/03/07/hacker-su-sito-pd-toscana-sigla-isis_afb49349-360d-4dd8-9d5e-89893b96983f.html; "Hackerato sito Crusca, simboli", in *Ansa Toscana*, 9 August 2015, http://www.ansa.it/toscana/notizie/2015/08/09/hackerato-sito-crusca-simboli-isis_1042b667-394e-4fba-99b7-0c8828df693c.html.

199 "Hackerato sito Crusca, simboli", cit.

200 "Terrorismo: ancora minacce web, 'missili sull'Italia'", in *Ansa Cronaca*, 3 February 2015, http://www.ansa.it/sito/notizie/politica/2015/02/02/terrorismo-ancora-minacce-web-missili-sullitalia_90b0483d-6617-4127-9618-9993f953e334.html; "Isis,Gentiloni "ministro Italia crociata", in *Ansa Cronaca*, 14 February 2015, http://www.ansa.it/sito/notizie/topnews/2015/02/14/isisgentiloniministro-italia-crociata_4c7e0481-7371-4aba-8025-47301deb31eb.html; Marta Serafini, "Isis: 'Per conquistare l'Italia dobbiamo allearci con la mafia'", in *Corriere.it*, 26 April 2015, http://www.corriere.it/esteri/15_aprile_15/isis-per-conquistare-l-italia-dobbiamo-allearci-la-mafia-91641e80-e383-11e4-8e3e-4cd376ffaba3.shtml.

ISSN 2280-6164

out attacks against the public safety for the purposes of terrorism."[201] The two had posted photos on Twitter in front of symbolic sites such as the Milan Duomo and Rome's Colosseum threatening possible attacks against those monuments. They had also expressed the desire to attack the Ghedi Air Force base in northern Italy. A particularly important 64-page document that circulated in April, also attributable to ISIS and written in fluent Italian, was entitled "Lo Stato Islamico, una realtà che ti vorrebbe comunicare (The Islamic State, a reality that wishes to communicate to you).[202]

Al-Qaeda cyber strategy has been meant, on the one hand, to offset losses among its historic nucleus and, on the other, to avoid being upstaged by the Arab spring and ISIS. The group has been disseminating anti-Western propaganda as its main activity. The messages spread over chat-rooms and forums have continued to be the primary vehicle of radicalisation both in Islamic and Western countries. From this point of view, the greater danger seems to lie in solitary cyber terrorism. Indeed, in 2012, the Italian judiciary police opened an investigation into two individuals (an Italian of North African descent and an Italian convert) suspected of propaganda and "operational recruitment" "operations" on the web. Al-Qaeda's online activities in Italy, in line with its global activities in general, in any case appear quantitatively inferior than those of ISIS.[203]

Hacktivists

Anonymous began operating in Italy in 2009-2010, years in which the first attacks were launched against government agencies and institutions, as well as foreign and Italian corporations, that the masked hackers claimed were guilty of "anti-democratic" behaviour.[204] Anonymous chooses its targets and attack modes in online forums and chats and, in Italy, the group has taken on an "umbrella" function for other similar groups. As such, it has become a point of reference on the Italian hacktivist panorama precisely for its ability to aggregate.[205]

201 "Terrorismo: due arresti a Brescia, sostenevano l'Isis su twitter", in *Corriere.it*, 22 July 2015, http://www.corriere.it/cronache/15_luglio_22/terrorismo-due-arresti-brescia-sostenevano-l-isis-f7003642-3032-11e5-8ebc-a14255a4c77f.shtml.

202 "L'Isis parla italiano, 64 pagine di propaganda sul web", in *Ansa*, 1 March 2015, http://www.ansa.it/sito/notizie/cronaca/2015/02/28/isis-documento-di-propaganda-in-italiano-sul-web_6e00ea79-8fef-42fb-8fd7-0b88b3739403.html. In March, the author of the document, a 20-year old Italian of Moroccan origin, was apprehended. See: "Isis, arrestato autore documento propaganda italiano", in *Ansa Piemonte*, 25 March 2015, http://www.ansa.it/piemonte/notizie/2015/03/25/isis-arrestato-autore-documento-propaganda-italiano_022c59db-bbdb-4578-bd47-c9f70670ac18.html.

203 Intelligence System for the Security of the Republic, *Relazione sulla politica dell'informazione per la sicurezza 2011*, 28 February 2012, https://www.sicurezzanazionale.gov.it/sisr.nsf/category/relazione-annuale.html.

204 Ibid.

205 Intelligence System for the Security of the Republic, *Relazione sulla politica dell'informazione per la sicurezza 2014*, cit.

ISSN 2280-6164

The collective's main motivational impetus, originally the freedom of online information, has expanded over the years and led to target other particularly sensitive objectives such as, for example, the military sector.[206] Anonymous began to use cyber space for propaganda purposes in 2013, and as a vehicle for the expression of a social discontent that had deepened further with the economic downturn. Between November and December 2013, the hacktivist movement shifted from the struggle for freedom of information to support for other types of undertakings, such as the "No TAV" movement, which took the form of computer attacks on politicians and institutions.[207] Their online campaigns have often coincided with street demonstrations, as in the case of hackings against institutions taking place during the October 2013 protests in Rome, which were set to campaign for the right to affordable housing and against the economic crisis.[208] This trend has continued in 2014 when some movement's members sympathising with anarchical ideas attacked political party representatives and institutions.[209]

Anonymous' 2015 activities were aimed mostly at two targets: the websites of Expo 2015 and various Italian ministries. The hacktivists' campaign (#OpItaly) against the Expo began in May, when they succeeded in defacing the padiglioneitaliaexpo2015.com website.[210] They later successfully penetrated the systems of Best Union, the company handling the online sale of tickets to the Expo, using Twitter to post the data of private citizens who had bought tickets online.[211] In the same month of May, the collective posted a series of data stolen from the server of the subdomain eu2014.difesa.it of the Ministry of Defence, which the press reported as an SQL-injection attack. The exfiltrated data included the names, email addresses and, in some cases, telephone numbers of the Defence Ministry staff and companies doing business with the armed forces. Anonymous' intention was to impact on the "military-industrial complex" and cyber defence industry.[212] Following the arrest of

[206] Intelligence System for the Security of the Republic, *Relazione sulla politica dell'informazione per la sicurezza 2012*, 28 February 2013, https://www.sicurezzanazionale.gov.it/sisr.nsf/category/relazione-annuale.html.

[207] Intelligence System for the Security of the Republic, *Relazione sulla politica dell'informazione per la sicurezza 2013*, 6 March 2014, https://www.sicurezzanazionale.gov.it/sisr.nsf/category/relazione-annuale.html.

[208] Ibid.

[209] Intelligence System for the Security of the Republic, *Relazione sulla politica dell'informazione per la sicurezza 2014*, cit.

[210] In an online communiqué, the collective called Expo "the disgusting expression of the oppressors' dirty conscience", fiercely criticising its sponsor: "Behind the sweet hypocritical discourse on nutrition, human rights and respect for the environment are the bloody usurping hands of the industrial powers". See: Andreina Baccaro, "Expo, i 7 informatici di Best Union in guerra contro Anonymous", in *Corriere di Bologna*, 5 May 2015, http://corrieredibologna.corriere.it/bologna/notizie/cronaca/2015/5-maggio-2015/expo-7-informatici-best-union-guerra-contro-anonymous-2301345920346.shtml.

[211] Pierluigi Paganini, "Expo 2015 – Anonymous has stolen 1TB data from Best Union ticketing service", in *Security Affairs*, 18 May 2015, http://securityaffairs.co/wordpress/36907.

[212] Carola Frediani, "Anonymous colpisce il ministero della Difesa", in *La Stampa*, 19 May 2015, http://www.lastampa.it/2015/05/19/italia/cronache/anonymous-colpisce-il-ministero-della-difesa-qlFNgswyvu20wnQiNYK1kL/pagina.html.

ISSN 2280-6164

two of the group's prominent members, Fabio Meier and Valerio Camici – known online by the nicknames Otherwise and Aken – Anonymous declared "war" on the Italian government. Attacks recorded thus far have been on infomercatiesteri.it, partner site to that of the Ministry of Foreign Affairs, and several other sites (ferrovie.it, statoregioni.it and mobilita.gov.it).[213] Another operation (entitled "Summum ius, summa iniuria") launched also as a reprisal for those arrests, is alleged to have led to the exfiltration of data and web defacement of sites associated with the Interior and Justice Ministries (siap-polizia.org, giustizia.lazio.it, caltanisetta.giustizia.it, sap-nazionale.org, assopolizia.it, carabinieri-unione.it and uilpolizia.it).[214] The operation has allegedly been carried out by emerging groups within the Anonymous Italia collective, and has exploited the "historic weaknesses" of those sites, including unencrypted passwords.[215] It is worth recalling that even ENAV's website has been unsuccessfully targeted by Anonymous.[216]

Over recent years, the group has reduced its actions quantitatively but not qualitatively, as the constant increase in the technical skill of its attacks shows. Their development of specific malware has been facilitated by the market's absence of specific antidotes, and new techniques for maintaining anonymity have helped to conceal the true perpetrators of operations.[217] At the same time, a shift has been observed from DoS and web defacements to SQL-injection attacks, as well as worms and spear-phishing to steal sensitive data. Nevertheless, these activities have shown that only a small portion of the movement has an advanced level of hacking expertise, while sympathisers appear limited in their technical prowess.[218]

Cyber criminals and organised crime

Considering the targets and tactics of online crime, the danger associated with cyber criminals and organised crime mainly regard aspects of economic security rather than of national defence. Easy access to malware, ransomware,[219] and trojans (etc.) in the deep web has permitted their use also by those criminal organisations

[213] Site Intelligence Group, "Partner of the Italian Ministry of Foreign Affairs Targeted as Part of "Operation Italy", in *Dark Web & Cyber Security*, 9 June 2015, http://ent.siteintelgroup.com/Dark-Web-and-Cyber-Security/site-6-9-15-partner-of-the-italian-ministry-of-foreign-affairs-targeted-as-part-of-opitaly.html; Marta Serafini, "Anonymous attacca siti del governo per vendicare I compagni arrestati", in *6gradi*, 4 August 2015, http://seigradi.corriere.it/?p=10142.

[214] The news was reported on the Anonymous blog. Interview, November 2015.

[215] Interview, October 2015.

[216] Interview, November 2015. See also: "Anonymous, tutti i dettagli dell'operazione Tango Down", in *Zeus News*, 17 May 2015, http://www.zeusnews.it/n.php?c=19252.

[217] Intelligence System for the Security of the Republic, *Relazione sulla politica dell'informazione per la sicurezza 2012*, cit.

[218] Intelligence System for the Security of the Republic, *Relazione sulla politica dell'informazione per la sicurezza 2013*, cit.

[219] "Ransomware is malware for data kidnapping, an exploit in which the attacker encrypts the victim's data and demands payment for the decryption key." See "Ransomware" in *WhatIs.com*: http://whatis.techtarget.com/definition/ransomware-cryptovirus-cryptotrojan-or-cryptoworm.

ISSN 2280-6164

that previously did not use them.[220] The most frequently employed anonymity techniques include the Virtual Private Network (VPN)[221] and the Tor network.[222] Organised crime mainly participates in industrial espionage campaigns that do not rule out their being commissioned by firms struggling for a market slice in the same market sector.[223] Attacks reported within this context have been on mobile phones and mobile banking services. Even the latest developments seems to confirm that organised crime continues to pose more of a financial than a security threat, as witnessed by the recruitment of hackers by Mafia bosses for credit card cloning activities.[224]

4.3. What danger to ATM/ATC systems in Italy?

4.3.1 Short-term assessment

The technology factor

ENAV's high technological component, also considering the multiplicity of its systems, including various legacy software[225] and other commercial-off-the-shelf (COTS) products,[226] conceal vulnerabilities that could affect the availability and integrity of data and, consequently, jeopardise air navigation services.

The analysis of the technologies employed by ENAV, and in particular of the E-Net and some air traffic control applications, whose details are confidential and, for obvious reasons, cannot be published in this study, included the following aspects that are worth underlying:

- the E-Net's physical availability is currently ensured through a telecommunications provider with which ENAV has specific agreements on the technical monitoring of ordinary operations and performance assessments;

[220] Intelligence System for the Security of the Republic, *Relazione sulla politica dell'informazione per la sicurezza 2014*, cit.

[221] Ibid.

[222] "The Tor network is a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet. Tor's users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy. Along the same line, Tor is an effective censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content. Tor can also be used as a building block for software developers to create new communication tools with built-in privacy features. See Tor Project website: https://www.torproject.org/about/overview.html.en.

[223] Intelligence System for the Security of the Republic, *Relazione sulla politica dell'informazione per la sicurezza 2013*, cit.

[224] Salvo Palazzolo, "I boss reclutano una banda di hacker e clonano migliaia di carte di credito", in *Repubblica.it*, 29 September 2015, http://palermo.repubblica.it/cronaca/2015/09/29/news/i_boss_reclutano_una_banda_di_hacker_e_clonano_migliaia_di_carte_di_credito-123895964.

[225] Custom-designed software not commercially available.

[226] Commercial products that do not allow for personalisation but are sold on the open market by producers who permit at most their configuration.

ISSN 2280-6164

- there is coordination between the two SOCs and crisis management procedures are in place in the case of an incident, from the initial signals onward, as well as substantial service levels (contract service level agreement);
- connection with external network is heavily monitored with highly restrictive traffic policies, third-party checks, and internet traffic analysis through the use of Splunk data analysis software and specific open source applications that ENAV employs for the dynamic control of user and application behaviour, in the context of an advanced Security Information and Event Management (SIEM) system;
- the use of IDS layer 7 and Proxy layer 7[227] effectively strengthens the perimeter and results in the significant reduction of attack surfaces;
- COTS system patching are closely checked, in addition to intelligence activities aimed at revealing emerging threat vectors, both by means of product and domain analyses and through information from qualified national and foreign sources.[228]
- the Milano and Roma PoPs are evaluated as elements of maximum attention, with management of admissible ports based on exceptional criteria and the principle of least privilege,[229] which allows for the limitation by type, nature and recognisability of the traffic admitted through ports by respective firewalls.
- periodic "black box" resilience tests allow to evaluate the expected effectiveness of the various security layers.

The experimental Self Briefing portal was then analysed. Although soon to be replaced by a different application, evaluating the portal is useful in describing how ENAV uses its applications on public networks. It should be pointed out that the Self Briefing is not situated on an operational network and is not directly linked with other operational systems.

As is true of any web application, the Self Briefing portal could be attacked by many possible means, notably (D)DoS, SQL-injection, cross-site scripting, cookie hijacking and other forms of command injection.

In the case of successful (D)DoS attacks, the consequences appear fairly limited, as the application becomes inaccessible to the majority of legitimate users. However, if this occurs, the situation is remedied by methods in use also by other countries and prescribed by ENAV contingency plan. Even the application's eventual complete inaccessibility does not appear to present any real problem. The situation would be much more serious if the (D)DoS attack were on the entire FDP system,

[227] Here "layer 7" refers to the application layer of the Open Systems Interconnection (ISO/OSI) model for network architecture (ISO 7498).

[228] With particular regard to the preventive measures provided by national organisations within the cyber strategy framework, notably CNAIPIC, DIS and CERT.

[229] The principle of least privilege is the practice of limiting access to the minimal level that will allow normal functioning and, however, exclusively to the information the user needs and a right to know. A corollary to the principle is that, with any change in role of those authorised, their authorisation must immediately be reviewed and, in the case of cessation of service, revoked.

ISSN 2280-6164

thus preventing the insertion, elaboration and visualisation of flight plans. This is what moved ENAV, in addition to strengthening the perimeter with substantial "demilitarised zones"[230] and firewalls, to create a clear separation between the E-Net and non-operational networks such as the Self Briefing or those used for more traditional management services (commercial MPLS). The Self Briefing portal is not directly connected to the FDP since flight plans are issued by the Eurocontrol Network Manager Operations Centre.[231]

SQL-injection attacks are among the most dangerous since they can lead to an attacker's successful and unlawful authentication and access to applications. Once recognized as a legitimate user thank to the SQL-injection attack, it could enter accurately fabricated data, or even erase/modify data. Nevertheless, the Self Briefing system is monitored by an IDS sensor capable of detecting such attacks. Moreover, the system does not indiscriminately accept data contained in any flight plan whatsoever: every flight plan undergoes a multi-level operational validation in accordance with the international standards laid down in the technical annexes of the Chicago Convention.[232]

According to available data, the cross-site scripting vulnerability should be limited to that variant, often exploited through social engineering actions, which subjects the victim's browser to harmful stress with minor or no significant consequences to the Self Briefing portal. The possible consequences for the target computer include malware installation, data exfiltration and registration on a botnet. If this were to happen, it would have an irrelevant impact on ATM/ATC services and would, in any case, be visible through traffic management and behavioural modelling systems.[233]

Cross-site scripting becomes more dangerous when associated with cookie hijacking operations. Once legitimate users are authenticated, they may receive session cookies in their browsers, possibly containing an authentication token.[234] The use of cross-site scripting, along with full compliance with Same Origin Policy (SOP),[235] could allow an application open on another panel of the same browser to appropriate the cookie, displaying its contents to the server to prove it has already completed authentication. Such an operation would constitute theft of credentials

[230] When giving external access to internal network servers or services, it is necessary to create a security stratum capable of ensuring that applications located in the "demilitarised zone" do not allow attackers access to the internal network. This isolation allows access to the endangered services exclusively in the "demilitarised zone", while any non-trusted access to other services is precluded. Thus the exposed servers become "bastions" that form "outposts" for the networks of organisations that must necessarily be exposed externally but will, nevertheless be defended.

[231] Interview, November 2015.

[232] Interview, November 2015.

[233] Interview, November 2015.

[234] Random number generated by the server and delivered to the browser, often by means of a cookie, to be displayed subsequently as proof of previous authentication.

[235] Security criterion used by web pages, by which a script from one web page cannot refer to other web sites.

ISSN 2280-6164

and make it possible for a third party to replace the legitimate user. Other forms of command-injection offer attackers similar results (authentication, database access, credential theft). Penetration testing (both "black box" and "white box,"[236] especially those carried out by external third parties) have, for the moment, ruled out the risk of exposure, taking into account the known-vulnerabilities and employing advanced technology, including Metasploit and Burp, which are tools dedicated specifically to web application analysis.

Again, with regard to the technology factor, it must not be forgotten that ATC activities depend heavily on the availability of current and continually updated data. Theoretically, the possibility of a well-orchestrated DoS attack capable of interrupting the flow of data to ATC operations does exist. Nevertheless, this situation is addressed in the contingency plan, which calls for an alternative flight data entry mode, with limited impact on ATC systems.

Also important to consider are the problems associated with the aforementioned AMHS project, which, with the introduction of digital technology into communications, necessitates data security measures designed with particular regard for the integrity and authenticity of data, identification of communication partners and the eventual need for confidentiality and access control. To that end, the identification and consideration of security requirements must be part of the design phase.

Over the short-term, therefore, although accesses to the public network might be regarded as potential targets, considering non-state actors' limited level of skill and the substantial counter-measures put in place by ENAV, the probability of attack should be considered low.

The human factor

The study found that the human factor was a critical element and keystone of ENAV cyber defence.[237] In a highly technological environment such as air navigation services, the human factor is extremely delicate, requiring an ever-increasing effort not limited to the sole dimension of awareness but, and above all, the full compliance with strict policies, which comes with the constant promotion of a security culture.[238] Consistent with this are ENAV's set of procedures and processes implementing the principles of 27001 ISO standard.

[236] Knowing the exact internal architecture, compilation codes and structure of the software.

[237] Underscored by a slogan displayed in the ENAV SOC: "there hasn't been a firewall yet invented that can protect against stupidity."

[238] To that end, it has been hypothesised that Stuxnet malware might be introduced not only through the web but through removable supports (USB drives). Farhad Manjoo, "Don't Stick It In. The dangers of USB drives", in *Slate*, 5 October 2010, http://www.slate.com/articles/technology/technology/2010/10/dont_stick_it_in.html.

ISSN 2280-6164

The study also confirms the presence of identification procedures for controllers entering control rooms, where they have access to the various consoles, receive data and assist aircraft. This takes place in compliance with measures designed to ensure the proper performance of an avionic system.

After all, an air traffic controller who decides to provide an aircraft with "poisoned" or in any case counterfeit data, would hardly conceal it from his/her controller partner.[239] Moreover, even if this were feasible, the possible results do not appear dangerous, since the worst effect the false data would have would be to place the aircraft on the wrong route. Nonetheless, even in this case, with subsequent passage to another ACC, another controller would communicate the pilot the wrong route. Equally unconvincing is a hypothetical terrorist's forcing a controller to crash the aircraft into an obstacle or place it on improbable route to exhaust fuel. In fact, the pilot has the final say in the aircraft's security and in such a situation would be capable of reacting appropriately, further modifying the route, possibly by making radio contact with another ACC or control tower.

Another possible scenario is that of multiple coordinated actions that, if properly executed by controllers, could create complex situations in which, for example, aircraft separation is reduced to a minimum, leaving no room for manoeuvre. This, nevertheless, would be an extreme case. How could multiple controllers be induced to provide pilots with tampered information? Operational standards oblige controllers to use the instrumentation assigned for ATC purposes, categorically ruling out the use of smartphones or other personal devices on the workplace. It would therefore be problematic for the cyber attacker to employ social engineering to convince controllers of unrealistic situations in which they may feel obliged to send aircraft data different from those expected. Indeed, ENAV in-house policies ban the well-known practice of Bring-Your-Own-Device (BYOD), which today represents a risk factor in many organisations with high security requirements.[240] In short, BYOD means to bring possible unsecured devices into the workplace, allowing many malicious actors to send messages through unsecured applications now in widespread use on smartphones.

Taking due account of the policies already enacted by ENAV, when considering the human factor it is, nevertheless, recommended that everyone within the organisation's and its suppliers will be kept acutely aware of the promotion and enhancement of cultural practices, and of the indispensable need to elevate security as a value.

[239] Flight controllers always work in pairs.

[240] BYOD is currently rather controversial, since its supporters appeal to the increases in productivity it can generate. In the case of critical infrastructure, however, it should be risk assessment alone that determines whether or not to ban BYOD.

ISSN 2280-6164

The monitoring of suppliers, and the desirable collaboration of police and intelligence forces in verifying their reliability, could represent a verifiable improvement, also in the context of the national cyber strategy framework.

The cyber threat

The case-study presented in part 4 shows that Italy is not exempt from the cyber threat associated with jihadist terrorist organisations. Although the danger of Al-Qaeda seems to have faded, the online activism of ISIS still sounds an alarm. The most significant episode took place in May 2015, when ISHD claimed to have successfully penetrated Defence Ministry IT systems and stolen the addresses and photos of some Italian military personnel. In its intentions, this act was very similar to the alleged exfiltration of data that allowed the same group to post the names, email addresses and other personal data of American military staff, which was later revealed to be false. The Italian case also raises strong doubts. Indeed, there is reasonable certainty that one or more individuals managed to profile the Italian military personnel from open sources and channel the data to the ISHD in emulation of the actions of Ardit Ferizi. The exfiltration of data from a protected network is therefore highly improbable.[241] Nevertheless, this episode is proof – if ever that were needed – that like other countries engaged in the anti-ISIS coalition in Iraq and Syria, Italy too has become a terrorist target. This means that, exactly as in the case of the United States, the United Kingdom and other Western countries, the (more probable future than present) intention to attack Italian critical ICT infrastructures is real. As seen in part 3, however, no indications thus far point to imminent attack on Italian civil aviation or infrastructure. Apart from the alleged attack on the Defence Ministry, ISIS cyber activity in Italy too has been limited to propaganda and recruitment, and has not thus far revealed a high level of technical sophistication. From what has been observed to date, terrorist groups such as ISIS and Al-Qaeda do not seem to have developed any particular malware for striking specific targets in Italy, nor do they seem capable of doing so, which leads to the assumption that they are relying exclusively on external hackers to carry out their cyber space operations.

Finally, and as much as it may seem paradoxical, Anonymous' recent "policing" of ISIS affiliates and supporters has added an ulterior element of difficulty to the planning and execution of ISIS and Al-Qaeda cyber operations, although some observers have pointed out how the group's actions could interfere with those of intelligence or law enforcement agencies.[242]

In line with the discussion in part 3, hacktivists in Italy display greater technical skill as compared with Islamic terrorist organisations, as the case of the SQL-injection attack on the Defence Ministry showed. That skill notwithstanding, there is no

[241] Interview, October 2015.

[242] Larry Greenemeier, "Anonymous's Cyber War with ISIS Could Compromise Terrorism Intelligence", in *Scientific American*, 19 November 2015, http://bit.ly/1I1bCql.

ISSN 2280-6164

certainty of their ability to violate complex IT networks that require, in addition to a certain technical expertise, a well-developed capacity for harvesting data that are not easy to obtain in the case of facilities associated with national security. An additional element not to be overlooked is hacktivists' underlying motivation. The Anonymous movement, in particular, was born of an ideological belief in the freedom of information. Although it has been observed that Anonymous Italia have expanded their objectives against various government institutions (i.e. the Defence Ministry) and non-governmental concerns (No TAV, Expo, etc.), the possibility that these actors will direct their attacks against ICT facilities such as ATM systems – attacks capable of placing human lives at risk – appears to run counter to the collective's logic. And even though the level of the threat they pose can be assessed as "concrete, immediate and real in a medium/long-term projection,"[243] as hacktivist expert Gabriella Coleman has said, "taking down a website is not terrorism [...]. Attacking an electrical grid is, but that has never happened. If Anonymous were to do that they would be doomed as political activists."[244]

The same considerations seem to apply to cyber criminals and organised crime. Their need to ensure parts of the digital black market has given major innovative impetus to the creation and development of new malware. This dynamic has lifted the technical skill level of cyber criminals to the point of allowing them to master instruments that have previously been nearly the sole precinct of governments. Yet, although the threat posed by cybercrime in association with organised crime could be deemed high due to possible recruitment of highly skilled hackers,[245] it is improbable that cyber criminals are a danger to the ENAV ATM systems. An attack would jeopardise their anonymity and risk "blowing the cover" of more profitable and less risky operations.

A holistic assessment of the weaknesses of ATM/ATC systems and threats against them must include the role of government authorities such as the postal and communications police and the Security Intelligence Department (DIS) in preventing and countering potential cyber terrorism events.

The Italian postal and communications police – and particularly the CNAIPIC – work to prevent and counter ordinary, organised and terror-related cyber attacks against national critical ICT infrastructure. Their range of intervention includes preventing the spread of propaganda and recruitment messages and illegal activities aimed at damaging, compromising and exploiting the web.[246] Constant web monitoring began in 2007 and is more active than ever today, with a 24-hour/7-day a week task

[243] Intelligence System for the Security of the Republic, *Relazione sulla politica dell'informazione per la sicurezza 2014*, cit., p. 85.

[244] Carola Frediani, "Vi racconto le mille facce di Anonymous", in *l'Espresso*, 12 November 2014, http://espresso.repubblica.it/visioni/tecnologia/2014/11/10/news/vi-spiego-le-mille-facce-di-anonymous-1.187319.

[245] Intelligence System for the Security of the Republic, *Relazione sulla politica dell'informazione per la sicurezza 2014*, cit., p. 86.

[246] Italian association for ICT security, *Rapporto Clusit 2015 sulla sicurezza Ict in Italia*, cit.

ISSN 2280-6164

force of over 20 staff and the additional support of the DIS and Prevention police.[247]

Table 1 | Postal police activity against ISIS cyber crime (January-October 2015)

Web space	Number	Monitored	Blocked
Sites	20	19	1
Forums	32	10	22
Blogs	6	6	/
Media	18	18	/
Twitter	10,939	350	6,386
Facebook	275	85	/
Reported to A.G.	10		
Total	11,300	488	6,409

Source: Italian Ministry of Interior.

These monitoring activities are carried out in collaboration with other international entities, such as Interpol and Europol, which offer real-time information exchanges, with the further enhancement of a Europol database containing the results of the activities of various other member countries.[248] Although it is not within the scope of this research to fully evaluate CNAIPIC's work, the more than 200 investigations of cyber attack against government bodies and firms, and the 114 persons brought before the courts are an indication of the level of police activity. In the specific case of this study, the arrest in 2015 of a Tunisian and a Pakistani for alleged online pro-ISIS propaganda and recruitment bears witness to the effectiveness of the postal police, whose role was further reinforced in the latest counter-terrorism decree.[249]

The DIS also plays an essential role in cyber threat prevention and intelligence, both as regards the public sector as well as industry and strategic private sector entities. A recently drafted (and yet to be finalised) protocol of understanding between the DIS and the CNAIPIC is aimed at consolidating threat containment and intelligence activities. What's more, the DIS has established a special Cyber Collaboration Platform with national public services and critical infrastructures, including ENAV, that allows for information and technical data sharing in order to boost cyber security.[250]

[247] Roberto Di Legami, "La minaccia corre sul Web", in *Poliziamoderna*, February 2015, p. 12-17, http://www.poliziamoderna.it/articolo.php?cod_art=3757.

[248] Ibid.

[249] Decree No. 7 of 18 February 2015, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2015-02-18;7; Enzo Quarantino, "Polizia Postale, così scoviamo jihadisti su web", in *Ansa Cronaca*, 22 July 2015, http://t.co/HkCAiv2tz5.

[250] Intelligence System for the Security of the Republic, *Relazione sulla politica dell'informazione per la sicurezza 2014*, cit., p. 107.

ISSN 2280-6164

In this context, the collaboration that ENAV has put in place with CNAIPIC, since 2008 on the basis of the Pisanu Decree,[251] and with DIS, on the strength of Art. 13-bis of Law no. 124/2007, add a further degree of security.[252]

To conclude, the security measures adopted by ENAV, the limited technical skills of ISIS, different objectives of hacktivists and cyber criminals and the prevention efforts by Italian authorities, make it possible to assert that the level of danger to which Italian ATM/ATC systems are subject is low, at least over the short-term.

4.3.2 Medium- to long-term assessment

Civil aviation's ATM systems are facing a long transformation process that will pose considerable problems as regards their cyber security.

Next Generation Air Transportation System (NextGen) is a new ATM system the United States intends to implement in the years to come, which calls for a transition from radar-based to satellite navigation, voice to digital communications and the creation of a highly integrated management system.[253] According to an April 2015 GAO report, these new technologies risk exposing ATM systems to some inherent dangers and, according to the American authorities, the FAA's failure to develop an adequate security model will lead to serious risks. In the same way, modern aircraft's growing interface with the Internet will increase the possibility of unauthorised remote access to avionic systems.[254]

Similarly, in 2004, the European Commission launched the Single European Sky (SES) programme whose aim is to reform the entire European ATM complex.[255] The subsequently created Single European Sky ATM Research (SESAR) should produce a new ATM system capable of managing a constant increase in air traffic at a lower cost.[256] The programme intends to overcome existing national fragmentation and channel sector research and development (R&D) toward modern, homogeneous air traffic control systems. The goal is to cope with a capacity for three times the current traffic, to lower route unit costs, to have ten times higher security coefficient and an a ten times lower environmental impact.[257] The new technology will permit a

[251] Polizia di Stato, *Sicurezza: rinnovato l'accordo tra Polizia di Stato ed Enav*, cit.

[252] Stefania Ducci, "Moving Toward an Italian Cyber Defense and Security Strategy", cit.

[253] FAA, F*act Sheet: NextGen*, 19 August 2015, http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=19375.

[254] GAO, *FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen*, April 2015, http://www.gao.gov/assets/670/669627.pdf.

[255] SESAR Joint Undertaking, *Background on Single European Sky*, http://www.sesarju.eu/node/37.

[256] ENAV has been highly present since the programme's inception and actively participates in significant security undertakings; those especially noteworthy include cooperation with Eurocontrol and air navigation services providers on the creation of a European ATC CERT, closely connected with those of non-European countries.

[257] ENAV, *SESAR*, http://www.enav.it/portal/page/portal/PortaleENAV/Home_EN/ServiziEAttivita_EN?CurrentPath=/enav/en/services/international_activities/KPP/sesar.

ISSN 2280-6164

greater exchange of information not only among flight controllers and aircraft, but also with other entities and actors.[258] The new system, slated for implementation within 2020, will not be without a certain amount of risk due to a number of factors that increase its efficiency but also its vulnerability in a manner similar to the American NextGen.[259]

This brief study shows that the future of aviation, and ATM systems in particular, is unlikely to be exempt from risk. The United States and Europe will be adopting new ATM systems in an attempt to reduce costs and improve the efficiency of managing air traffic, which is destined to increase by 5 percent annually over the coming 20 years.[260] The transition from one communication mode to another, along with the increased interface among the system's parts, will multiply the number of vulnerabilities exploitable by actors with criminal intent. An evolution of this sort will make the relationship between civil aviation and cyber security even closer, with the latter playing an increasingly important role in the defence of citizens and of national security.

In terms of cyber threats, critical infrastructure could be more exposed to danger over the medium and long terms. Some more advanced countries are investing heavily in ICT security in an effort to make both private sector and government systems more secure. Western nations such as the US and Great Britain are allocating major resources to university education aimed at raising levels of expertise in response to a steadily rising demand.[261] Other not western countries, such as India for instance, already boast a relatively high ICT literacy level. The greater the need for protection, the greater the probable presence of educated experts qualified to ensure it. More advanced technical sophistication will also be associated with gradual interdependence, as more and more devices will be linked and the majority of services will be provided and managed online. Consequently, it will become a top national security priority to avoid that none of that growing number of highly skilled technicians is tempted to join the ranks of terrorist or criminal groups. The case of Briton national Junaid Hussain of Birmingham, an ICT expert lured in by ISIS, is emblematic.

Although the threat posed by ISIS or Al-Qaeda is currently not high, it could increase over the medium to long-term. One of Al-Qaeda's leaders, Omar Bakri Muhammad, was already claiming back in 2005 that thousands of Al-Qaeda sympathisers were studying computer technology in order to make their contribution to the "holy

[258] SESAR, *SESAR: The future of flying*, July 2010, http://ec.europa.eu/transport/modes/air/sesar/doc/2010_the_future_of_flying_en.pdf.

[259] SESAR Joint Undertaking, *Study launched to address cyber-security in SESAR*, 22 May 2015, http://www.sesarju.eu/node/1821.

[260] Airbus, *Global Market Forecast 2015-2034*, http://www.airbus.com/company/market/forecast.

[261] White House, *The Comprehensive National Cybersecurity Initiative*, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative; Gareth Halfacree, "UK government pledges funds for cyber security education", in *bit-tech*, 23 September 2015, http://www.bit-tech.net/news/bits/2015/09/23/cyber-security-education/1.

ISSN 2280-6164

war,"[262] and specialised research centres confirm that Al-Qaeda's cyber activities will become daily fare.[263] A rise in the level of technical expertise could also come rapidly for ISIS, all the more so if those of the new well-trained generations were to espouse the cause, as indeed thousands – even from Western nations – have already done.[264] It is considered highly probable that ISIS will develop the sort of tactics and tools that have led to major cyber space successes – for the most part media spectacles – or convince online sympathisers to launch attacks in its name.[265] According to FBI director James Comey, ISIS "is waking up" to the idea of launching critical infrastructure attacks using complex malware.[266] At a conference in October 2015, a high-ranking official of the US Department of Homeland Security said that ISIS had made attempts to attack the American energy industry, nevertheless underscoring a low credibility due to lack of technical expertise.[267] Further evolution could come with ISIS' achievement of true statehood. For the time being, the terrorist organisation could not be including the significant upgrade of ICT capacity among its priorities, given its heavy involvement in military operations in Syria and Iraq.[268] In the case it were to succeed in consolidating as a state, it might establish cyber warrior units such as those of other governments. However, at this point, that kind of evolution is currently difficult to foresee. Finally, it remains to be seen what impact the August 2015 killing of alleged ISHD chief Junaid Hussain will have on the evolution of ISIS' technical capabilities. According to US sources, Hussain helped ISIS raise its guard against Western electronic surveillance and assembled malware to be use in attacking computer systems. He is also believed to have supported the encryption of communication among ISIS members, promoted the recruitment of ICT experts, including hackers and programmers, and trained ISIS members himself. In one online conversation, he is alleged to have discussed a zero-day exploit.[269] In short, Hussain is thought to have consolidated and institutionalised ISIS' interests in the cyber sphere. Nevertheless, this does not tell us whether Hussain ordered the alleged ISIS cyber operations or carried them out himself. Some believe the Birmingham native dealt mainly with propaganda and recruitment, and would have left hacking operations to other "crews" not under

[262] Roland Heickerö, "Cyber Terrorism: Electronic Jihad", cit., p. 558.

[263] Steven Stalinsky and R. Sosnow, "From Al-Qaeda to the Islamic State (ISIS), Jihadi Groups Engage in Cyber Jihad", cit.

[264] ICS-CERT, *Cyber Threat Source Descriptions*, cit; Aaron Y. Zelin et al., "Up to 11,000 foreign fighters in Syria; steep rise among Western Europeans", in *ICSR Insights*, 17 December 2013, http://icsr.archivestud.io/2013/12/icsr-insight-11000-foreign-fighters-syria-steep-rise-among-western-europeans.

[265] Cory Bennett and Elise Viebeck, "ISIS preps for cyber war", in *The Hill*, 17 May 2015, http://thehill.com/node/242280.

[266] Steven Stalinsky and R. Sosnow, "Hacking in the Name of the Islamic State (ISIS)", cit.

[267] "ISIS is attacking the U.S. energy grid (and failing)", in *CNN Money*, 16 October 2015, http://cnnmon.ie/1PjyZmf.

[268] Emma Graham-Harrison, "Could Isis's 'cyber caliphate' unleash a deadly attack on key targets?", cit.

[269] Margaret Coker, Danny Yadron, Damian Paletta, "Hacker Killed by Drone Was Islamic State's 'Secret Weapon'", in *The Wall Street Journal*, 27 August 2015, http://on.wsj.com/1WVAfhO.

ISSN 2280-6164

direct ISIS control.[270] If he was, in fact, the key player in ISIS online campaigns, it is possible that his death will slow the terrorist organisation's technological evolution, although it will be a few months before that can be ascertained. On the other hand, if ISIS-led operations have been carried out by affiliated hackers, it is probable that they will continue in the coming months.

Understanding Italian hacktivism's future prospects at this particular moment in history is no simple task. Anonymous Italia suffered heavy losses with the arrest of Fabio Meier and Valerio Camici who, according to investigators, loomed large on the national and international hacktivist panorama and are being held responsible for the recent operations against Expo and the Defence Ministry.[271] If the supposition that Anonymous Italia is made up of niches of expert hackers and a less technically adept general membership is correct, it is possible that this coup by the Italian authorities will have major repercussions. Anonymous has already declared war on the Italian government for the detention of the two hackers, and appealed to the rest of the collective for their support. If the global movement reacts to the arrest of these two members, it is probable that there will be campaigns of a certain importance against Italian institutional sites, although to date there does not seem to have been any particular response internationally.[272] As regards the judgement that the future elevated capability acquired by digital activists will be "enough to render them vulnerable to manipulation and influence by organised entities for the pursuit of objectives other than online protests,"[273] it is difficult to predict whether this could result in attacks against critical infrastructures such as ATM systems.

It is probable that cyber criminals will continue to evolve technically, and that organised crime will increasingly rely on hackers for its illegal activities. If the recent trend continues, the threat associated with this type of actor will grow more serious by virtue of the rising number of interconnected devices and the mounting competition in the malware market. There is also the possibility that cyber criminals will gain access to highly sophisticated instruments such as those made available after Hacking Team, a Milanese firm specialised in surveillance software, suffered a cyber attack that was followed by the online distribution of products normally sold only to police and intelligence agencies.[274] That said, the danger posed by these actors to the air traffic system will probably remain relatively low in the future.

[270] Interview, October 2015.

[271] Polizia di Stato, Polizia delle Telecomunicazioni, "Comunicato Stampa: Operazione Unmask", in *Valtellina News*, 19 May 2015, http://www.valtellinanews.it/assets/Uploads/Comunicato-stampa-UNMASK-Finale-20-maggio-2015-1.pdf.

[272] Interview, October 2015.

[273] Intelligence System for the Security of the Republic, *Relazione sulla politica dell'informazione per la sicurezza 2014*, cit., p. 85.

[274] It appears that some Chinese hacker groups have already begun to use some of the firm's data harvesting tools. See: James Griffiths, "Chinese hackers used tools leaked after attack on Italian cybersecurity firm Hacking Team", in *South China Morning Post*, 20 July 2015, http://www.scmp.com/node/1838426.

ISSN 2280-6164

Finally, an eventuality that should be avoided at all costs is the combination of all the possible options, something that has thus far never taken place. Essentially, police and intelligence agencies will have to make sure that those who intend to attack critical infrastructure do not have the ability to do so, and that those who do have such capability do not find a reason to use it maliciously. To date, there does not seem to be any solidarity between hackers of a certain proven expertise and terrorist organisations or powerful criminal groups targeting critical national infrastructure. Any alliance of that sort would result in capabilities and resources that would place national and international cyber infrastructure in serious peril.

Conclusions

The purpose of this study was to respond to a question as simple in its formulation as it is complex in its analysis: are the ENAV ATM/ATC systems safe from the cyber threat? The obvious answer to this kind of query would be that a system is without risk only when it has been turned off – if a hacker has not managed to penetrate it before that. Even a system considered secure and protected can be violated with a zero-day. The idea that protection can never be complete, however, does not mean that various levels of protection reduce the enormity of such a threat, do not exist or cannot be developed.

On a scale from low, to medium to high, this study maintains that the short-term possibility that ENAV ATM/ATC systems will be successfully attacked by non-State actors is low, and this thesis is supported by a series of factors.

In the first place, from the technological point of view, ENAV has the methodologies and instruments necessary for confronting this type of threat; and even though the system remains at risk given the impossibility of achieving total security, the study did not find vulnerabilities that set off any significant alarms. Conversely, this result must also take into account the need for constant, and indeed increasing, vigilance over the technological, and process and system-related aspects of national interests. Such vigilance calls for the constant assessment of risk and of changing weaknesses, especially in light of an increasing openness and interoperability with other systems.

Defence, therefore, must not be the sole variable considered, since a complete analysis must also include assessment of possible attackers' technical skills. Civil aviation authorities have identified terrorist organisations, hacktivists and cyber criminals as posing the greatest threat to that sector. None of these actors, however, currently constitutes a serious threat to the ATM/ATC systems of any country, including Italy. The cyber capabilities of terrorist organisations such as ISIS and Al-Qaeda have thus far been shown to be limited, despite their actions having earned them considerable media attention. While Anonymous' technical prowess is decidedly higher, and could pose a threat to civil aviation, it is improbable that

ISSN 2280-6164

the hacktivist collective would be interested in compromising ICT systems in ways that would endanger people's lives. Cyber criminals and organised crime could have an interest in attacking the civil aviation sector, but mainly at commercial and financial levels. Finally, the efforts of institutions such as CNAIPIC and DIS are a further obstacle to possible attacks against critical ICT infrastructure.

That these assessments are valid for the short term does not mean the situation will remain unaltered in the future. For that reason, an attempt has been made to offer some points for reflection and to give a glance at the medium-long term.

In the not-too-distant future, US and European ATM/ATC systems will undergo a deep technological transition that will render them more efficient, but also more interconnected and potentially more vulnerable. This will inevitably increase the level of risk, with the consequent need to reinforce those systems' defences.

It is reasonable to expect that, in the medium-long term, educational systems will respond to ICT market demands by turning out more computer science specialists. From a national security standpoint, it is going to be essential to ensure that those future experts avoid and resist the attraction of extremist or radical ideologies – the case of Junaid Hussain being emblematic of the problem – keeping in mind all the difficulties inherent to identifying and stopping phenomena that often germinate at an individual level.

It cannot be ruled out a priori that ISIS will acquire the skills to make it a serious threat to critical infrastructure. This will depend on many variables, among which its ability to establish statehood, attract well educated members or continue to obtain support from hackers distributed in the most disparate regions of the world. Obviously, all these factors cannot be taken for granted, and although there are some who doubt the likelihood of these conditions, the authorities concerned with preventing and countering illegal online activity will, in any case, have to monitor those virtual spaces from which the first alarming signals could come.

The future of Anonymous Italia is uncertain after the arrest of two high-profile figures on the Italian hacktivist panorama. It is difficult to predict how, while there is no real hierarchy, the collective will regroup after the loss of two members that have certainly provided a certain amount of leadership, at least at a technical level. Although the level of hacking may vary, and perhaps decrease, what most probably will not change are the hacktivists' intentions regarding critical ATM/ATC infrastructures, which it is believed (and hoped) will continue to be absent from their operational objectives.

The technical skill of cyber criminals will continue to improve in the years to come, if for no other reason than because competition between malware vendors and a continually expanding online black market will be an incentive to develop ever more sophisticated tools. Although their potential for access to technical expertise makes it necessary to keep a watchful eye on these actors, it is also improbable that cyber criminals will allow sensitive targets such as air traffic control systems in the

ISSN 2280-6164

future to distract them from much more profitable and less risky targets such as the commercial and financial divisions of civil aviation.

This study has certainly not exhausted all the possible topics worth examining in the context of the relationship between cyber security and civil aviation. The present report proceeded from a broad-based perspective to analyse some of the sector's many vulnerable elements, such as the internal computer systems of airports and on-board aircraft systems. Future sector studies will presumably continue to investigate these aspects in order to paint the broadest possible picture of the cyber threat to civil aviation.

Future efforts at analysis will also have to consider the possibility not only of non-state, but also of state and para-state actors posing a threat to critical national infrastructure. As remote as this eventuality may currently appear, the recent conflicts in Georgia and Ukraine and the diplomatic skirmishes in the South China Sea have led to consideration of how space and cyber weapons might be used in conflict situations.[275] Since governments, as a result of their resources and national security objectives, will be the driving force behind cyber innovation in the coming years, experts in the defence of critical ICT infrastructure will inevitably have to factor in the degree of sophistication of these actors in their efforts to render their systems as secure as possible. This while combining the maintenance of a high quality logical, physical and process security, in line with the best sector standards.

Updated 5 May 2016

[275] CrowdStrike, "Rhetoric Foreshadows Cyber Activity in the South China Sea", in *CrowdStrike Blog*, 1 June 2015, http://t.co/Ifl4L5xDr7; Kenneth Geers, "Strategic Analysis: As Russia-Ukraine Conflict Continues, Malware Activity Rises", in *FireEye Threat Research Blog*, 28 May 2014, http://ow.ly/xlq1T; David Hollis, "Cyberwar Case Study: Georgia 2008", in *Small Wars Journal*, 6 January 2011, http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

ISSN 2280-6164

Acknowledgements

The authors would like to thank all those who kindly contributed to making this study possible, in particular:

The Italian Air Force
The Italian Air Navigation Service Provider (ENAV)
The Italian Civil Aviation Authority (ENAC)
The Italian Ministry of Interior
The Italian Ministry of Transport
The Office of the Prime Minister

Special thanks also go to:

Francesca Bosco, Project Officer, United Nations Interregional Crime and Justice Research Institute (UNICRI)
Jean Pierre Darnis, Deputy Director, Security and Defence Programme, Istituto Affari Internazionali (IAI)
Pierluigi Paganini, Chief Information Security Officer at Bit4Id and member of the Treat Landscape Stakeholder Group of European Union Agency for Network and Information Security (ENISA)
Stefano Silvestri, Scientific Advisor and past President, Istituto Affari Internationali (IAI)

Other contributors to the study include Daniele Fattibene, Francesca Monaco, Nicolò Sartori and Alessandra Scalia, IAI Security and Defence Programme.

This study was done with the support of Vitrociset.
The report was translated from Italian to English with the support of ENAV.

ISSN 2280-6164

ISSN 2280-6164

DOCUMENTI IAI 15 | 23E - DECEMBER 2015

Istituto Affari Internazionali (IAI)

Founded by Altiero Spinelli in 1965, does research in the fields of foreign policy, political economy and international security. A non-profit organisation, the IAI aims to further and disseminate knowledge through research studies, conferences and publications. To that end, it cooperates with other research institutes, universities and foundations in Italy and abroad and is a member of various international networks. More specifically, the main research sectors are: European institutions and policies; Italian foreign policy; trends in the global economy and internationalisation processes in Italy; the Mediterranean and the Middle East; defence economy and policy; and transatlantic relations. The IAI publishes an English-language quarterly (The International Spectator), an online webzine (AffarInternazionali), two series of research papers (Quaderni IAI and IAI Research Papers) and other papers' series related to IAI research projects.

Via Angelo Brunetti, 9 - I-00186 Rome, Italy
T +39 06 3224360
F + 39 06 3224363
iai@iai.it
www.iai.it

Latest DOCUMENTI IAI

15 | 23e Tommaso De Zan, Fabrizio d'Amore and Federica Di Camillo, *The Defence of Civilian Air Traffic Systems from Cyber Threats*

15 | 23 Tommaso De Zan, Fabrizio d'Amore e Federica Di Camillo, *Protezione del traffico aereo civile dalla minaccia cibernetica*

15 | 22 Eleonora Poli and Maria Elena Sandalli, *Financing SMEs in Asia and Europe*

15 | 21 Anna Gervasoni, *Alternative Funding Sources for Growth: The Role of Private Equity, Venture Capital and Private Debt*

15 | 20 Umberto Marengo, *Italian Exports and the Transatlantic Trade and Investment Partnership*

15 | 19 Irene Fellin, *The Role of Women and Gender Policies in Addressing the Military Conflict in Ukraine*

15 | 18 Nicoletta Pirozzi e Lorenzo Vai, *Proposte di riforma della Politica europea di vicinato*

15 | 17 Pier Domenico Tortola and Lorenzo Vai, *What Government for the European Union? Five Themes for Reflection and Action*

15 | 16 Silvia Colombo, *La crisi libica e il ruolo dell'Europa*

15 | 15 Serena Giusti, *La Politica europea di vicinato e la crisi in Ucraina*