gbf
Attorneys-at-law

Cyber risks in aviation

gbf Aviation Law Afternoon Workshop

Marco Novoselac
3. May 2017

“There are two types of companies: those that have been hacked and those who don't know they have been hacked.” (John Chambers, Chairman CISCO)

“There are two kinds of big companies in the United States. There are those who've been hacked by the Chinese, and those who don't know they've been hacked by the Chinese.” (James Comey, FBI Director)

Cyber risks represent a clear and present danger to the aviation industry.

Cyber risks will increase strongly in the future.

Cyber risks must be addressed on an international, national, industry- and enterprise-level – now.

Cyber risk definition

Any risk emerging from the use of information and communication technology (ICT) that compromises the confidentiality, availability, or integrity of data or services.

Cyber risk is either caused by natural disasters (e.g. floodings or earthquakes) or is man-made. Man-made cyber risk can emerge from human failure (employees, contractors, supply chain partners), cyber criminality, cyberwar or cyber terrorism.

Types of cyber risks in aviation industry

- Hacking

Unauthorised intrusion into a computer or network

- DDoS-attack

Denial of service is typically accomplished by flooding the targeted machine or resource with requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled

- Malware

General term. Malicious software used to disrupt computer, gather, sensitive information, gain access to computer systems. Includes virus, trojan, worms, ransomware

- Cyber-jacking

Taking control of an aircraft by electronic means

- Spoofing

Broadcasting a false GPS signal and deceive the GPS receiver

- Extorsion

Attack or threat of attack coupled with demand for money to avert or stop attack

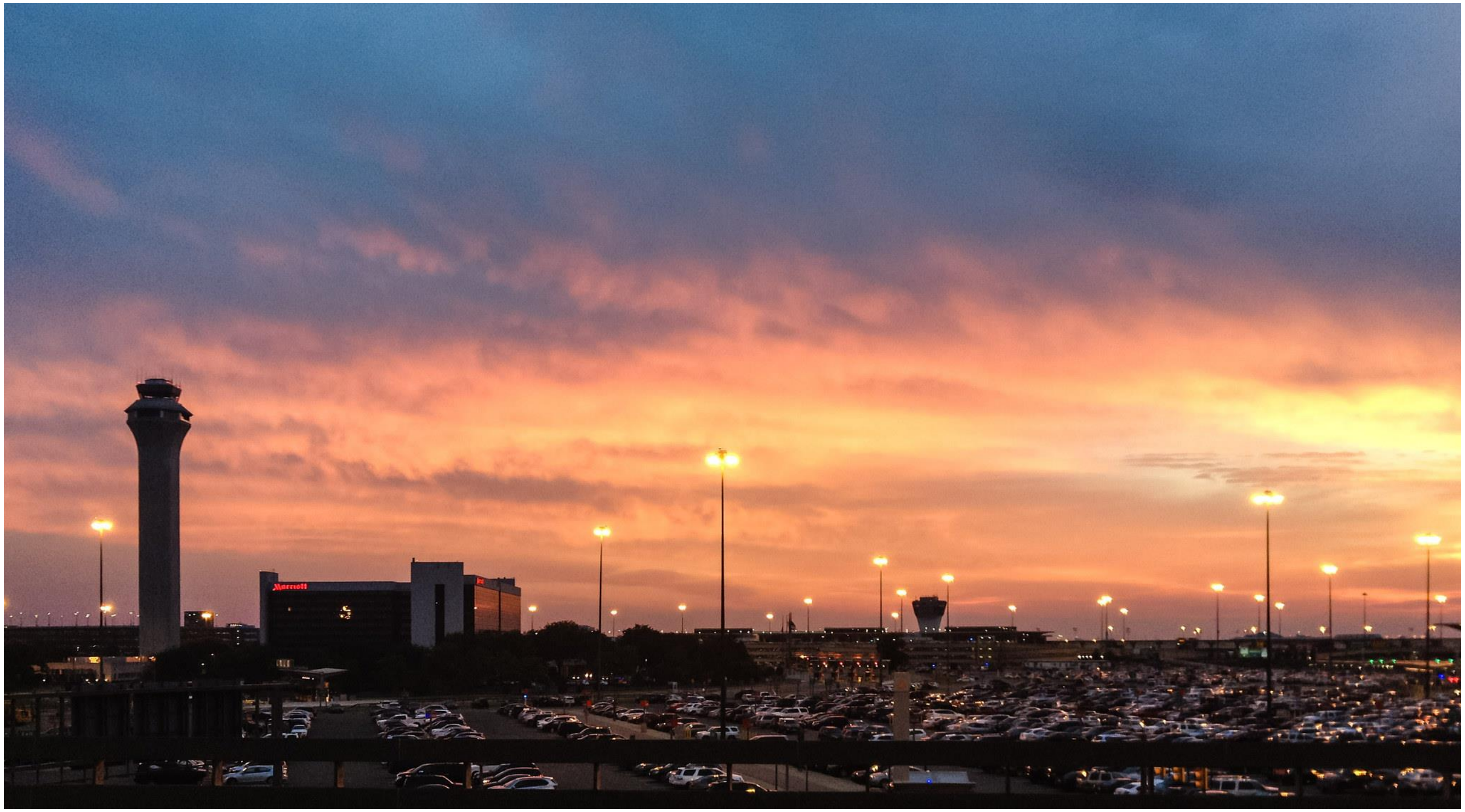
- Network downtime
- Data theft/loss/damage
- Violation and theft of IP

Spanair 5022 crash

Spanair 5022 crash

- 20 August 2008
- Madrid Barajas Airport
- MD-82 crash just after take-off
- 154 people killed
- Central computer system used for monitoring technical problems on board of the aircraft was infected with malware – may have prevented the detection of technical problems

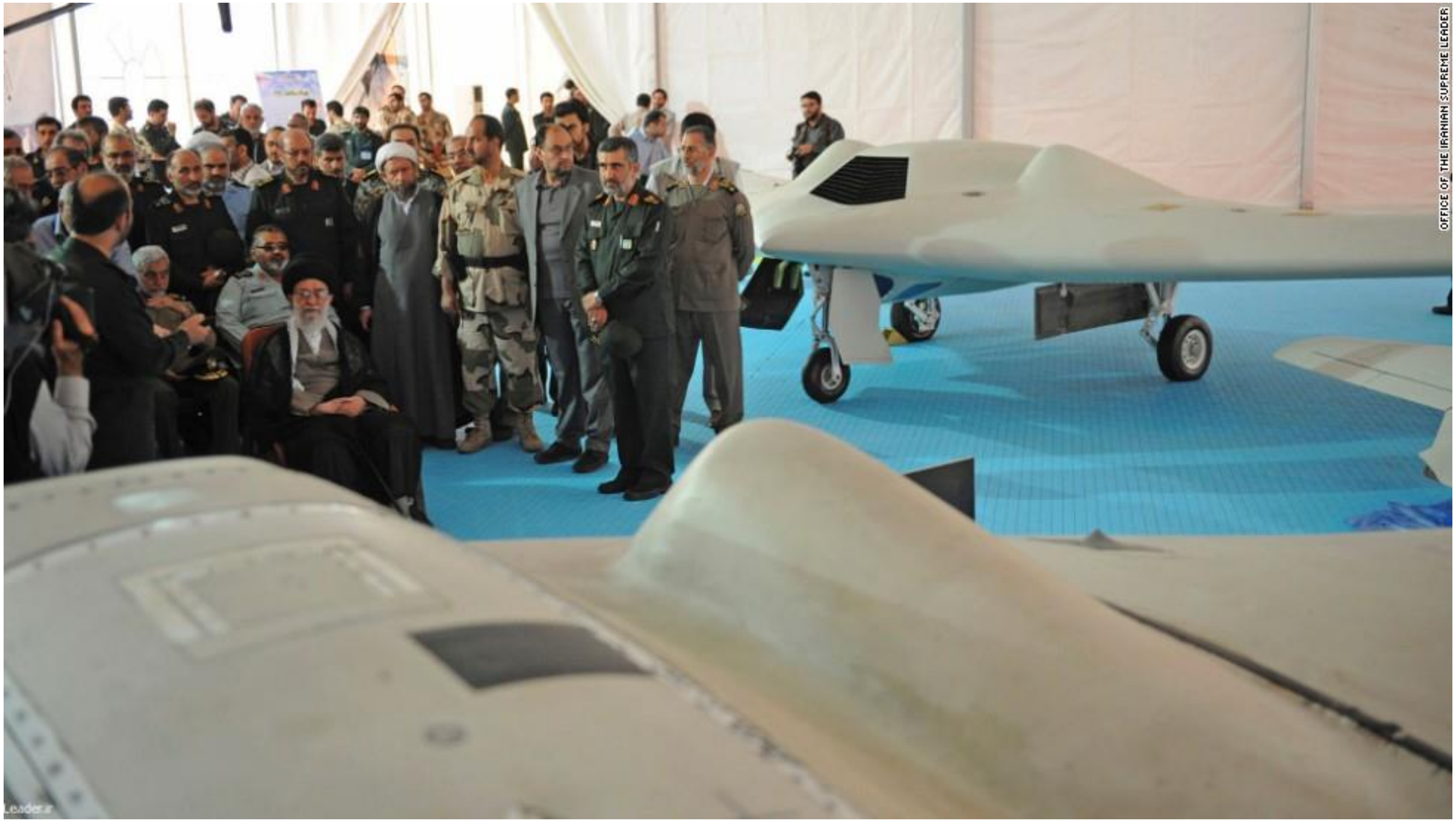
Newark Airport GPS jamming



Newark Airport GPS Jamming

- 2009
- Sporadic outages of GPS Groud-based Augmentation System used for precision approach landing
- Every day at same time
- FAA discovered the cause was a GPS jammer used by a truckdriver to avoid being tracked by employer

Iran US drone capturing



OFFICE OF THE IRANIAN SUPREME LEADER

Iran US drone capturing

- 2011
- Iran stated it captured a US drone by spoofing the GPS signals and make it land in Iran at what the drone thought it was its home base in Afganistan

Hugo Teso‘s hack demonstration

- 2013
- Security researcher
- Simulated hacking into ACARS-System (Aircraft Communications Addressing and Reporting System) and communicating with the FMS (Flight Management System)
- Gained remote access into cockpit system, gained control and remotely programmed flights from ground using simple application and off-the-shelf electronic equipment
- Manufacturers stated that the hack cannot be reproduced in real life

MH 370 mystery

MH 370 mystery

- Boeing 777
- Disappeared at 1.21 AM, 8 March 2014
- 227 passengers, 12 crew members
- Up to 7 hours from disappearence automatic signals to a satellite
- 1 hour after disappearence login into ground station
- Aircraft accident investigators assume aircraft was brought off-course by a person on board, direction was changed several times and communication systems (ACARS and transponder) were switched off
- Theories of cyber-jacking, no evidence

MH 370 mystery

- 2013 and 2014 Boeing request to FAA to incorporate changes to aircraft designs citing security reasons (possibility of in-flight entertainment systems being connected to other critical systems of aircraft)
- April 2015 US Government Accountability Office (GAO) in a report warned FAA that late model aircraft may be vulnerable to cyber attacks that could affect operation of avionics systems: „modern communications technologies, including IP connectivity, are increasingly used in aircraft systems, creating the possibility that unauthorized individuals might access and compromise aircraft avionics systems"

MH 370 mystery

- In its latest Security Briefing IFALPA (International Federation of Air Line Pilot’s Associations) states that highly sensitive systems should be physically separated from the Internet and networks that have access to the Internet. This includes separation of in-flight entertainment systems and their communications from all other aircraft systems

DDoS attack on LOT

- 21. June 2015
- Hackers attack computer System of LOT
- Grounding of 10 aircraft and delay of 12 flights
- Inconvience to 1500 passengers

Istanbul Ataturk Airport hack

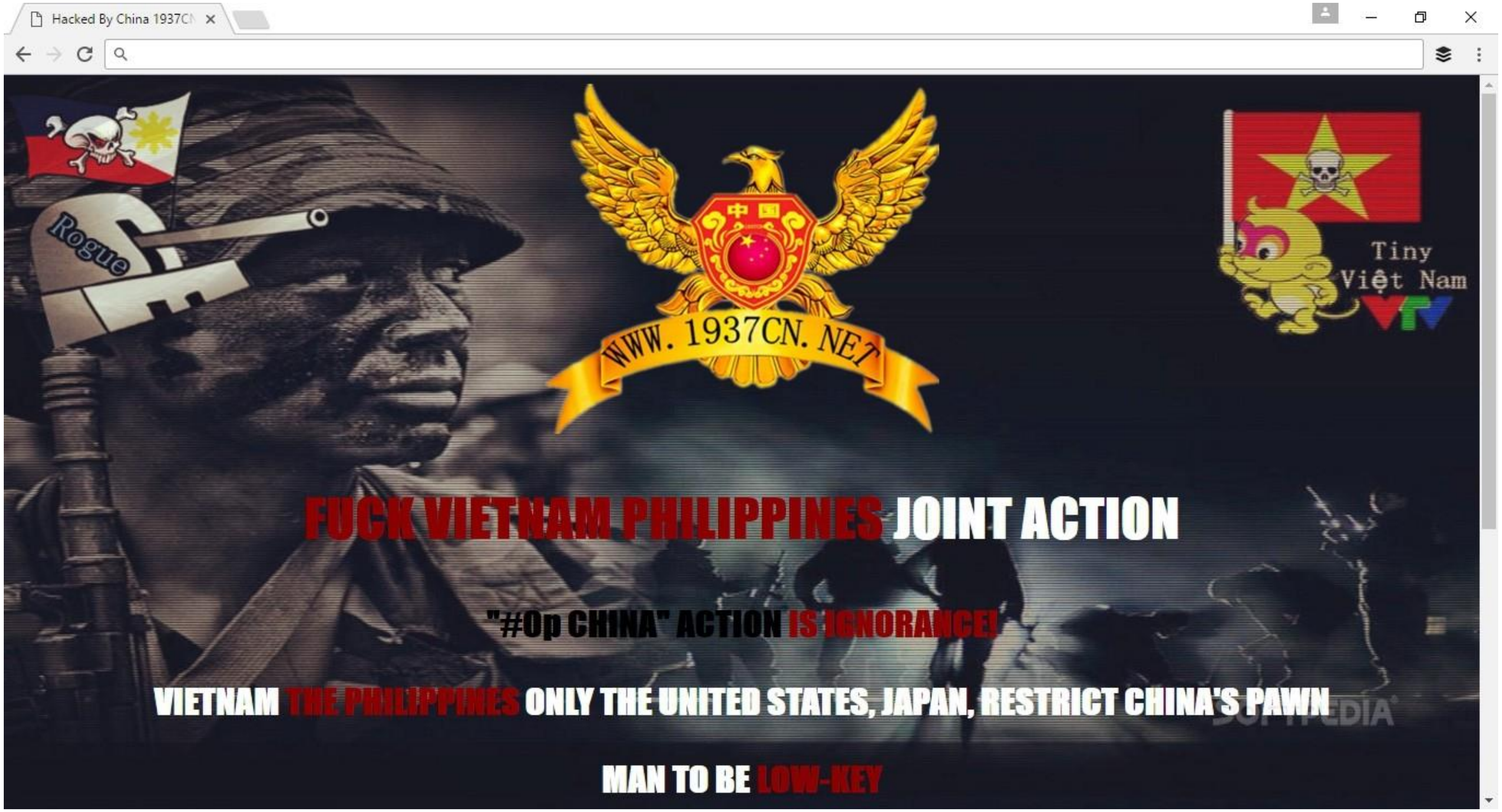
Istanbul Ataturk Airport hack

- July 2013
- Passport control shut down at departure terminals
- Cyber attack
- Delays

British Airways hack

- 27 March 2015
- Accounts of BA‘s frequent flyer programme were compromised
- Tens of thousands of BA Executive Club accounts were broken into
- Attackers managed to redeem member‘s reward points

Vietnam Airlines hack



FUCK VIETNAM PHILIPPINES JOINT ACTION

"#Op CHINA" ACTION IS IGNORANCE!

VIETNAM THE PHILIPPINES ONLY THE UNITED STATES, JAPAN, RESTRICT CHINA'S PAWN

MAN TO BE LOW-KEY

Vietnam Airlines hack

- 29 July 2016
- Website breach by hackers
- Release of confidential customer data of 400‘000 members of Vietnam Airlines‘ frequent flyers‘ club
- Hackers also accessed screens displaying Vietnam Airlines‘ flight information and took over tannoy system, airing political messages

United Airlines Grounding

United Airlines Grounding

- 8 July 2015
- United Airlines grounds all planes
- 4900 flights impacted
- Network connectivity issue

Delta Airlines Computer Outage

- August 2016
- Power Outage caused system failure
- 2000 flights canceled over three days
- $150 million costs

Most cyber incidents in the aviation sector have so far been low-level and caused limited impact, but the consequences of a cyber incident in civil aviation could potentially be catastrophic.

Cyber risks future developments

- Cybercrime losses estimated 2014: $400 billion; 2019 $2 trillion
- Cyber insurance market: $2 billion to $20 billion in next 10 years
- Increasing number of travelers (2016: 3.7 billion Passengers - 2050: 16 billion) and freight (2016: 50 million tons - 2050: 400 million tons)
- Creation of new modern, digitalised airports, introduction of more complex aircraft (flight software lines of code increased 10 times in ten years; 1960 to 2000, functionality provided by software to pilots grew from 8% to 80%)), use of advanced ICT, use of GPS technology

Cyber risks future developments

- More and more interaction between people, devices and services and more connection of things to the network, (currently 15 billion connected devices in the world – expected to increase to 50 billion in 2020) – increase of entry points
- ICT systems become more interconnecetd -> security lapses in one system are very likely to affect others (supply chain risk)
- Greater impact from ICT systems failures due to increased reliance on them

Efforts against cyber risks in aviation

ICAO‘s efforts

International Civil Aviation Organisation, branch of the UN, formed 1946 to regulate civil aviation

ICAO's efforts

- The Beijing Convention, 2010 (Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation)
  - Criminalization of certain terrorist actions against civil aviation, including using aircraft as a weapon, transport of dangerous material
  - Cooperation between States
  - Problem of cyber threats implicitly addressed: Offence committed when person destroys or damages air navigation facilities or interferes with their operation, if any such act is likely to endanger the safety of aircraft in flight or person communicates information known to be false, thereby endangering safety of an aircraft in flight
  - Not yet in force – 16 states ratified – 22 must to enter into force

ICAO‘s efforts

- Amendment 14 to Annex 17 to the Convention on International Civil Aviation (2014)
  - „Each Contracting State should, in accordance with risk assessment carried out by its relevant national authorities, ensure measures are developed in order to protect critical information and communications technology systems used for civil aviation purposes from interference that may jeopardize safety of civil aviation“
  - States shall identify their critical information and communications technology systems, including threats and vulnerabilities thereto, and develop protective measures (security by design, supply chain security, network separation, remote access control)

ICAO‘s efforts

- Roadmap on cybersecurity
  - On 5 December 2014, ICAO signed with four other Organizations (Airports Council International (ACI), the Civil Air Navigation Services Organisation (CANSO), the International Air Transport Association (IATA), and the International Coordinating Council of Aerospace Industries Associations (ICCAIA)) - an agreement to establish a ‘Roadmap’ on cybersecurity
  - The five organizations signed the Civil Aviation Cyber Security Action Plan and accompanying Roadmap
  - Cooperation enables the participating parties to draw together all elements of the aviation industry to ensure a shared vision, strategy and set of commitments to tackle the cyber threat

EASA‘s efforts

EASA‘s efforts

- 10 February 2017: Memorandum of Cooperation with the Computer Emergency Response Team of the EU Institutions (CERT-EU)
- CERT-EU's mission: support the European Institutions to protect themselves against intentional and malicious attacks that would hamper the integrity of their IT assets and harm the interests of the EU
- EASA and CERT-EU cooperate in the establishment of a European Centre for Cyber Security in Aviation (ECCSA)

IATA‘s efforts

International Air Transport Association
(trade association for world‘s airlines)

IATA‘s efforts

- Many players in the field of cybersecurity taking different approaches
- Frameworks emerging from many organizations, but little coordination of approach
- IATA exhorted ICAO to recognise the compelling need for the development of specific measures and best practices focusing on the aviation industry
- In 2015, IATA published the second edition of the Aviation Cyber Security Toolkit to assist airlines in raising awareness and understanding and better defining the cyber risks to their organizations

EU legislative efforts

- Directive on security of network and information systems (NIS Directive)
  - To be implemented until 9 May 2018
  - Operators of essential services (incl. air carriers, airport managing bodies, airports, entities operating ancillary installations contained within airports, traffic management control operators)
  - Appropriate technical and organisational measures to manage cyber risks and minimise impact of incidents
  - Notify competent authority of incidents with significant impact on the continuity of the essential services
  - Designation of national competent authorities on security of network and information systems and of computer security incident response team (CSIRT) and creation of CSIRT network

EU legislative efforts

- General Data Protection Regulation (GDPR)
  - Applies from 25 May 2018
  - Data processors must report personal data breaches to data controllers
  - Data controllers must report personal data breaches to supervisory authority
  - Data controllers must maintain internal breach register
  - Implementation of technical and organisational measures to ensure data protection by design and default
  - Non-compliance can lead to administrative fine up to EUR 10 million or 2% of total worldwide annual turnover
  - Claims for non-pecuniary loss

Switzerland‘s efforts

- Revision of FADP in progress
- Federal Council in 2012 commissioned the national strategy for the protection of Switzerland against cyber risks pursuing the following strategic goals:
  - Early identification of threats and dangers in the cyber field
  - Improvement of the resilience of critical infrastructure
  - Effective reduction of cyber risks, especially cyber crime and cyber sabotage
  - Risk and vulnerability analyses shall be carried out in critical sectors - air transport concluded in January 2016
  - FOCA is responsible for integrating provisions to minimise cyber risks into the national aviation safety programme, and to implement them in consultation with the industry

Conclusions

- Cyber incidents in the aviation industry are taking place and will increase in the future
- Cyber incidents in the aviation industry can have catastrophic consequences
- Many efforts, but not very coordinated and not very specific
- International and national laws relating to cyber security and it‘s breach are inadequate or non existent - law needs to catch up with rise of cyber-dependent systems
- The key to a cybersecurity strategy is consultation, coordination and cooperation between governments, governments and industry and within industry and standardization and harmonization, and this is yet to be achieved in aviation security

Suggestions

- Need of the hour: assessment of spectrum of risks (complete picture by understanding, identifying and accepting existence of cyber risks)
- Understanding of implications of increased connectivity and dependency on ICT in light of evolving cyber risks
- Comprehensive cyber strategy in every company
- Concerted effort by airlines, OEMs, MROs, air traffic controllers, airport authorities and operators and third-party suppliers
- Separate Security Architecture for aviation based on common standards -> closed structure and subject to strict regulation and control

Thank you for your attention!

Marco Novoselac
Partner
Attorney-at-law, M.B.L.-HSG
novoselac@gbf-legal.ch

gbf
Attorneys-at-law

P.O. Box 1661
Hegibachstrasse 47
8032 Zurich
Switzerland

T +41 43 500 48 50
F +41 43 500 48 60

P.O. Box 1911
Route de Pré-Bois 20
1215 Geneva Airport
Switzerland

T +41 22 533 48 50
F +41 22 533 48 54

contact@gbf-legal.ch
www.gbf-legal.ch