JYX
JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

**This is a self-archived version of an original article. This version may differ from the original in pagination and typographic details.**

**Author(s):** Henselmann, Gerhard; Lehto, Martti

**Title:** Where Cyber Meets the Electromagnetic Spectrum

**Year:** 2019

**Version:** Published version

**Copyright:** © The Author(s) 2019

**Rights:** In Copyright

**Rights url:** http://rightsstatements.org/page/InC/1.0/?language=en

**Please cite the original version:**

Henselmann, G., & Lehto, M. (2019). Where Cyber Meets the Electromagnetic Spectrum. In T. Cruz, & P. Simoes (Eds.), ECCWS 2019 : Proceedings of the 18th European Conference on Cyber Warfare and Security (pp. 209-218). Academic Conferences International. Proceedings of the European conference on information warfare and security.

# Where Cyber meets the Electromagnetic Spectrum

Gerhard Henselmann, Martti Lehto
University of Jyväskylä, Jyväskylä, Finland
office@ghenselmann.de
martti.j.lehto@jyu.fi

**Abstract**
Cyber linked with Information Technology, computers and the internet are the most commonly understood potential threats that everybody is aware of nowadays. In the case of National Cyber Strategy most efforts are given to these potential battlefields and threats. But is it enough to stay with these paradigms? Cyber warfare will look for utmost effects for chaos and misalignment of economy and therefore we cannot exclude the facts, that there is a potential threat also possible in the cut volumes between the information technology, the electromagnetic spectrum and its linked infrastructure and processes. We understand the technology for mobile telecommunications and data transfer, as the providers and linked business models are transparent and an open source and therefore a potential threat in the sense of cyber-attacks. All these services are based on the message transfer in the Electromagnetic Spectrum (EMS). It will be more challenging to enter in secured networks and modern data communication protected by encrypted and secured data links, hardened equipment and architecture. But as those systems, like the avionics and communication subsystems in airborne vehicles and commercial aircrafts are highly interlinked and interoperable based on data networks, it will be necessary to understand the architecture and weaknesses in detail. Of course, these principles are not fixed only to the airborne platforms and relevant applications; you may find the same technical pandemics in data transmission and data engineering in the physics of any data transfer chain, like satellite communication, radio transmission links. The paper will discuss the technical background in principle and identify potential weaknesses in aviation electromagnetic spectrum. We propose measures for attention and the implementation of relevant procedures and quality in order to overcome bottlenecks and grey area dull which helps the opponents to weaken society and open a sideshow for conflicts introduced by “simple cyber threat handling”.

Keywords: Electromagnetic Spectrum, aeronautics, avionics, Electronic Warfare, Cyber Warfare

## 1. Introduction

### 1.1 Background

Research in the interface between the electromagnetic spectrum and the electronics engineering in radio transmission links and data link applications have shown areas where unfriendly third parties, eventually called opponents can make use of open source knowledge and enter networks for hacking, influencing and destroying them, if they are able to lock into the protocol. Of course, those areas of threat potential might be considered by “critical infrastructure” analysis and subsequently covered in protection and work-arounds for measures. The consequence of getting access into this computer-based infrastructure will cause loss of control and this fear is real in nowadays Internet of Things (IoT) applications with low protection devices. Nowadays Artificial Intelligence (AI) based autonomous systems are becoming part of business and industry. Examples can be found from road transportation, maritime, industrial processes as well as from aviation, where automation has made flying safer than ever before.

So, we are entering in a new era. We are in the transition of the information technology cycle entering into the digital age, where our activities, skills and performances are based very much on computer-based support and the internet, even if we are aware on the cited reality. The Internet is among the few things humans have built that they don’t truly understand. (Schmidt and Cohen, 2014)

Regardless of the question on how the digital revolution expresses itself in core economic data and whether its benefits are even reflected in national accounts, from a technical point of view the process of technological transformation has so far expanded exponentially. This is not justified only by the increase in computational, storage and communication capacities, but by the ability to digitally intersect technological areas where information can be created, stored, accessed, processed and shared. The combination of embedded software systems for sensor-based monitoring and control of physical reality with global digital network infrastructures – the cyberspace. It allows a variety of applications and problem solutions with high economic potential and strong innovative power. On the supply side, more and more opportunities for using and linking data are created, enabling new business models. Previous media and technology breaches and related activities of

data collection and transformation are eliminated. It is believed that in 2002, for the first time, it was possible to store more information digitally than in analogue format - a clue to the beginning of the digital age. (Hilbert and López, 2011)

The consequence of getting access into the computer-based infrastructure will cause loss of control and this fear is real in nowadays IoT applications with low protection devices. The Internet of Things has a security problem, it is here - in future everywhere, but it is not secure (Hofmann, 2017). Consequently, the result of those interactions might be “fake news” for the public, misleading the society eventually into chaos and/or for operators behind the consoles bad and misleading starting point for their decision making.

**1.2 Electromagnetic Spectrum**

The electromagnetic spectrum is a broad area of activity characterized by physically observable activities such as visible light and lasers and unobservable phenomena such as microwaves and electromagnetic energy. EMS manifests through various frequencies and wavelengths produced by natural sources like solar storms or artificially by hardware such as radar or nuclear weapons. (Stuckenberg et al. 2018)

As most of the applications are not only connected to the world of data transfer by the internet but also via data link, VoIP-phone lines and the means of the EMS. The electromagnetic spectrum is the range of frequencies (the spectrum) of electromagnetic radiation and their respective wavelengths and photon energies. The EMS is involved everywhere e.g. with datalinks, with sensors, with data transfer on the WLAN and the established VoIP. (see Figure.1)

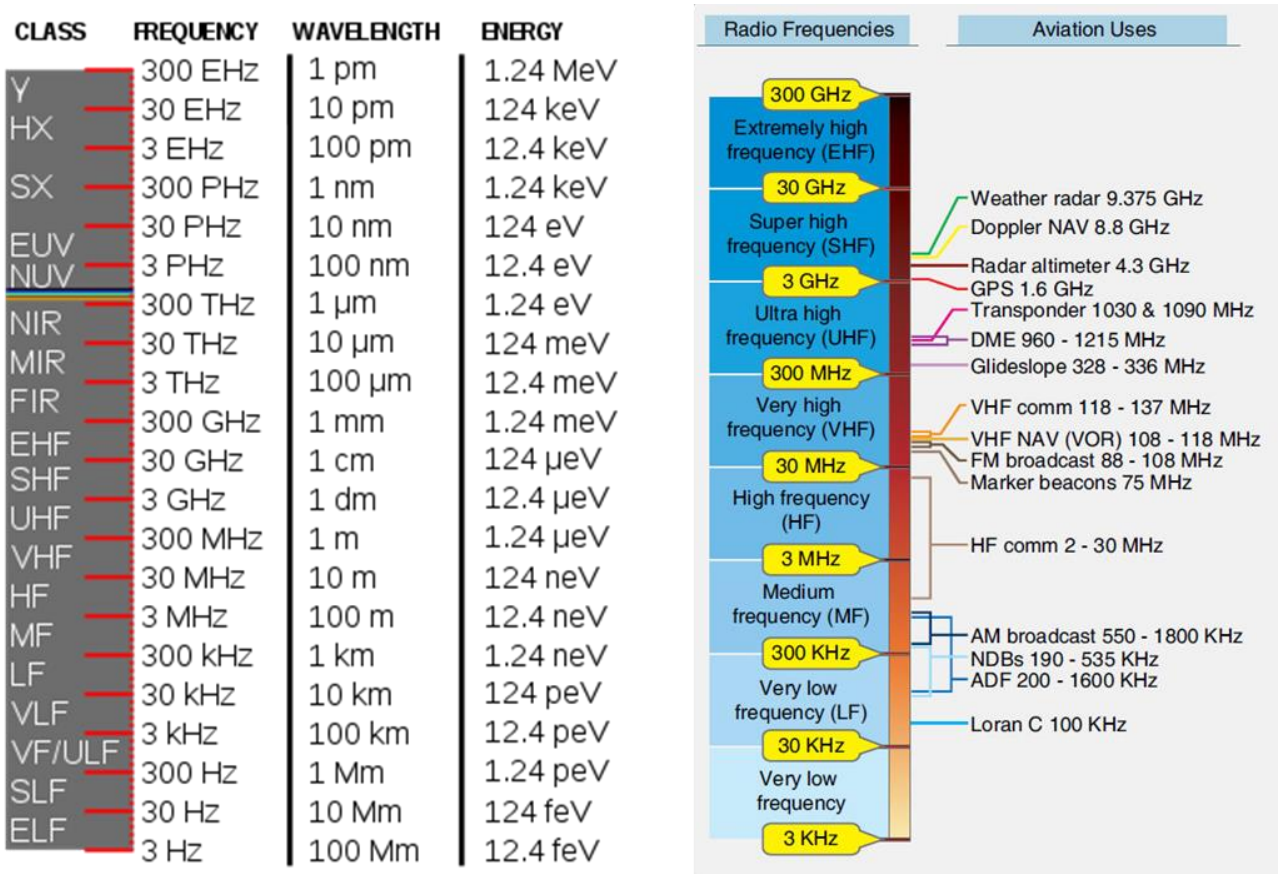


Figure 1. The Electromagnetic Spectrum and radio waves in communication and navigation[1]

And moreover, thinking a step beyond, the same physics and potential risk area is embedded in the communication and data link in aerospace and commercial flights. Aircraft but also automotive have been certified according to specific release protocols and a fixed set of configurations. Whenever a change to this configuration will apply, it needs to be checked against the certification and safety and airworthiness need to be assured by relevant testing and qualification and verification processes. Any change of take-over by

[1] https://en.wikipedia.org/wiki/File:Light_spectrum.svg
http://www.flight-mechanic.com/radio-communication-radio-waves/

configuration items based on a cyber-attack will endanger life and certainly will limit or even expire the authorization releases for operation.

In the beginning of the research, the focus was more on the hardware driven factors based on “kill switch” or built-in components without a clear configuration status, which were already described in research papers and speeches (Henselmann, 2017b). But searching more in the interface between the EMS and the computer-based networks, as there are avionics bus structures (AFDX, ARINC429, ARINC629), Milbus system in the (military) airplanes or the central information system in the automotive, the problem of spoofing and taking over the controls became clearer and is identified as a real threat, also described in the threat analysis assessment on weapon systems. (Koch and Golling, 2016)

The scheme for entering via the electromagnetic spectrum could be a combination of jamming the original messages in the frame and constellation of the message code and the intrusion of fake information messages via the EMS. But there could be expected alternative procedures and tools too. Cyber-attacks are responsible for delivering information on global end to end capabilities including the provision of SatCom, electromagnetic spectrum and networks to support the business model such as; booking system, Air Traffic Control (ATC) information, maintenance, repair and overhaul (MRO), monitoring systems and military operations.

In countering EMS challenges, some windows of opportunity needed to compete with our adversaries are closing. Meanwhile, EMS threats that have existed since the 1960s and earlier, such as nuclear-EMP and geomagnetic storms, have regained prominence. The salience of these threats has returned due to several factors, including (Stuckenberg et al. 2018):

(1) Near-universal integration of electromagnetically sensitive silica-based technologies into most modern hardware,
(2) Adversaries’ increased understanding of how to exploit critical vulnerabilities and
(3) The emergence of novel technologies, many of them poorly understood.

Having passed through into the third generation of information warfare, we must consider now, what a fourth generation might look like – and we need to be aware of the consequences and not forget it in the prevention and in our National Cyber Security Strategies. Where we are now is not unlike trench warfare, only in cyber space (Ryan, 2015). Where we will go next will emerge in an international landscape that is considering the implications of current capabilities on notions of just warfare, sovereignty and individual freedoms.

## 2. Description of the research and the objectives

Digitization has led to the convergence of cyber and information activities to such an extent that it is important that we adapt our concepts and doctrine to the changing environment. Electromagnetic spectrum is much more than a congested resource: today it is also constrained and continuously changing and every civilian, military, intelligence, homeland security operation relies on the capability to access and exploit the EMS. Because of physical (air/land/sea/space) and virtual (cyberspace) domains of warfare increasingly depend on the access and control of the EMS, the Cyberspace Electromagnetic Activity (CEMA) will be imperative for operational success. CEMA concept integrates elements from offensive and defensive cyber warfare, electronic warfare and intelligence (Seffers, 2018)

Our literature review revealed the definition of complex infrastructure and means for the daily life and business in the IoT, but it does not cover the electromagnetic activity in cyberspace and therefore this research is focused more on EMS environment – fake information by radio station, ATC and new services (GPS navigation, news distribution), where someone has to expect manipulation to allow entry points for cyber-attack.

We therefore would like to introduce the enlargement of the traditional scope, cyber environment and propose to use the add-on version with indication of radio systems, datalink, ATC etc. on this already complex mapping. As the EMS will provide in the future a major part of cyber application and could even be the starting point for chaos and cyber warfare, it needs to be considered in more detail in this scope and for this paper.

This research is based on literary analysis and reports made in cyber defense and electronic warfare related symposiums, conferences and workshops. The objective from this research will be focused on the perimeter “how cyber warfare might be injected by the EMS on airborne platforms like commercial/ military aircraft and cruise missiles” and what to be recommended for the National Cyber Security Strategy, especially considering legacy products in place and operation for at least the next 20 years of life.

## 3. Cyber-Electromagnetic Environment

### 3.1 Background

It is those unsolved problems in our life, such as; airplane accidents, which are not physically possible to get investigated because they only disappeared from the ATC radar screens or incidences were not made public. On the other side, military attacks with lethal weapons like cruise missiles delivered in the very recent past were not fully successful in delivery within the expected circular error probable (CEP), which brought up the idea to research the possible influencing factors and bring-up some hypothesizes and discuss them in a theoretical research method.

The major effort shall be focused on the interface of cyberspace and electromagnetic spectrum. Therefore, it will be necessary to first provide a definition of this interface. The cyberspace is a domain characterized using electronics and electromagnetic spectrum to store, modify and exchange data via networked systems and associated infrastructures. Cyberspace can be thought of as an interconnection between humans through computers and telecommunication without regard of physical geography.

### 3.2 Electronic Warfare

Electronic warfare is based on the understanding, controlling and shaping of the electromagnetic spectrum and has become increasingly important to winning on the modern threat scenario everywhere and on the traditional military battlefield environments. Advanced systems, which are in a steady loop for upgrading and adaptation for the latest technologies and methodologies, will provide an improved protection for society and for the military forces by jamming, suppressing or otherwise denying an adversary the full use of the electromagnetic spectrum.

While today we are facing the transition phase from Electronic Warfare into Cyber Warfare. Best practice proposals are provided in the Australian Defence White Paper (Scott, 2013) on the application of cybernetics in cyber criminology. Following the consequences and efforts put into this cyber perimeter today, it will come up with more “self-learning” and cyber warfare based on AI (Russell and Norvig, 2003) and empathy AI based decision-making (Hagengruber, 2017).

While the Electronic Warfare already knows and improves in updating its technologies and methodologies since decades the measure and countermeasure philosophy (jamming) in the radar and communication EMS (radar signals/R-ECM, communications/C-ECM), this technology is evolving for IR signatures by DIRCM-jamming and datalink by spoofing (DeMartino, 2012). EW capabilities include directed energy, decoys, and radio-frequency (RF) jamming to deny, disrupt, or deceive an adversary’s electromagnetic capability (Arnold, 2009)

The challenge for the EMS and cyber perimeter will be the understanding of where and how to disturb the information technology (internet, computer networks) by jamming algorithm and inject false information, subroutines into the relevant protocol during jamming. This sophisticated procedure is not immensely complicated in open source protocols as we have them available in commercial business to provide services and solutions, but it is more complex in the military application, where equipment and services are based on classified sources, protocols and requirements.

### 3.2 Cyber Warfare

There is no generally accepted definition for Cyber Warfare (CW). For some, cyber warfare is war which is conducted in the virtual domain. But also, it is the counterpart of conventional ‘kinetic’ warfare. EW and cyber operations need to be able to operate at the tactical, operational, and strategic levels both for offensive and defensive activities (Arnold, 2009). Cyber warfare can be divided into strategic and operational-tactical warfare, depending on the role assigned to cyber operations in the different phases of war. State actors launch offensive cyber operations in situations where the states are not at war with each other. In this case, the cyber-attacks constitute a cyber conflict in a low intensity conflict, as was the case with Estonia in 2007. (Lehto, 2015)

The cyber environment and cyberwar capabilities have created a new dimension where it is possible to act within the sovereign territory of another country, employing different military and non-military means of pressure to attain political and military goals. (Lehto, 2018)

### 3.3 Non-kinetic warfare in EMS environment

The new capacities of armed forces create new possibilities, both the kinetic and non-kinetic use of force in cyberspace. Cyber era capabilities make possible operations in the new non-linear and indefinite hybrid cyber

battlespace (Lehto, 2018). In electromagnetic spectrum can be understood to incorporate both CW and EW, thereby establishing non-kinetic warfare in EMS environment (Hay, 2016).

For this research, we defined that Cyber Warfare and Electronic Warfare form a non-kinetic warfare in EMS environment. The figure 2 illustrates that environment.

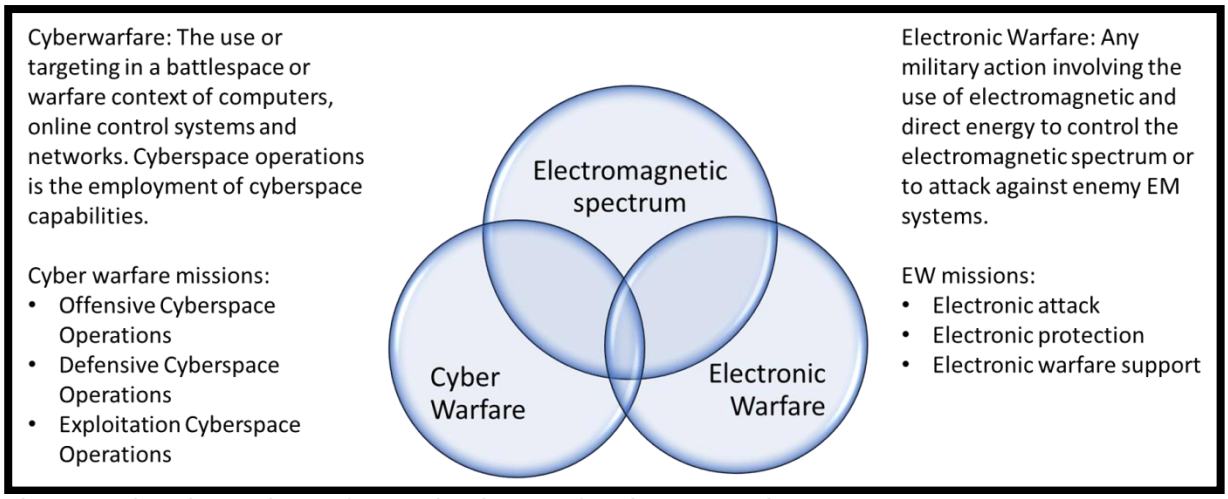

Figure 2. The Electronic Warfare and Cyber Warfare in EMS environment

## 4. Cyber relevant EMS interaction

### 4.1 The principle of the cyber relevant electromagnetic spectrum interaction

It is stated that EM is a natural physical maneuver space that is visualized through the concepts of EMS. As a natural physical space, the EM environment or also called domain cannot merge with other environments. But will it be possible to use tools and technologies in order to maneuver with the Cyber-EM environment? Today we know a huge variety of EM support systems like radars, communication devices, any kind of radar or communication jammers and GPS, which are networking utilizing the cyberspace and the cyberspace is increasingly utilizing the EM by wireless networks. The trend therefore could be called a technological sharing, and therefore the definition should incorporate that we do not speak about a converging but a sharing of both environments. With the above provided examples already existing in real life, we can easily say, that cyber systems are becoming more and more dependent on the EMS. (Arnold, 2009)

For focusing on the principle of the cyber relevant electromagnetic spectrum interaction, it is suggested to prepare the case in the aerospace environment and transfer the findings onto the other relevant areas like automotive security devices and IoT. Three things to be considered in this respect:

1. Open architecture of the system to be targeted for influencing,
2. Availability of a non-encrypted data link or radio communication old standard or the SW defined radio based
3. Technical knowledge on the interoperability of these systems.

### 4.2 Assessment analysis

More sophisticated approaches might have dedicated preparation packed during the design phase of a product and embedded by algorithm and sub-routines, which will be triggered from a dormant mode into a take-over mode of operation. The target for this EMS based cyber-attack either in the simple or in the more sophisticated preparation will be the take-over of control and utilize the weakness for supporting chaos, hijacking or blackmailing authorities. In any case these objectives are possible to achieved either in a camouflaged way, while authorities will not communicate the problem openly, or it will blow-up and the safety and trust in the relevant mobility system is gone and related business area and consequently the economy will be negatively influenced. In order to achieve this, an investigation on potential risk areas on an airborne platform must be prepared and validated.

This weakness analysis is starting to define the system level and cluster for analysis. The next step based on a risk assessment matrix needs to be a Failure Mode Effect and Criticality Analysis (FMECA) which will provide in detail the area of interest, where no redundancy is available but interfacing with either the internal network – like avionics bus system, AFDX etc. and/or the interface to external support devices, called Aircraft Ground

Equipment (AGE) for data exchange or mission data transfer is possible. Wherever this ground-based infrastructure is based on open-source Windows products and moreover Internet connection is available or possible, i.e. for updating or data exchange could be possible, the effort for a deeper analysis is recommended.

The assessment is a complex evaluation with deep skills and knowledge on the aerospace design world, but you may find experts worldwide consulting for any kind of ATA chapters with their support. But also, with available free time “everybody” with some expert knowledge could be able to study some level of details with accessible information sources on the global internet by searching some studies and keywords. As an example, for this first introduction, the information provided is based on Airbus A380 training material available on Internet is utilized.

The final result of the assessment will not be displayed in the article for confidentiality reasons. But some interesting statements and exclusion-matrix for more or less interesting areas are summarized. Pre-assessment is available by research and briefing within the German Cyber Defence Community during a lecture and poster session in 2017 (Henselmann, 2017a).

It needs to be noted and it is clear without doubts that the airworthiness on aircrafts will be intensively checked-out by testing and verification on all integration level and the installation/integration checks includes EMI/EMC testing (Electromagnetic Interference/Compatibility) on a certain power and frequency level.

### 4.3 Airborne platform

Our hypothesis is that wherever there is an interface between the airborne platform and relevant on-aircraft system, the most effective threat positioning could cause a cyber conflict or crime, by either implementing disharmonies, in case of redundant Command-Monitoring systems or overriding the original functionalities and provide fake information by malware and DDOS in a running system independent from the internet. Major points of interest could be:

- Mission data up-/download
- Routing, navigation data, Jeppesen on mobile tablets
- On-board active sensors linked with on-board bus system (radar, Traffic Alert and Collision Avoidance System (TCAS), Airborne Collision Avoidance System (ACAS)
- Up-/downlink of maintenance or engine data
- Radio communication device, Software defined radio
- Inflight entertainment system
- SW-loading station on-ground (AGE, test systems)

It seems possible that with some training and research, skilled people might get the information necessary to prepare and operate such an attack either on-board or from the ground. For preparation of any kind of this operation, it is helpful that nowadays the flight tracks, airplane position including flight altitude, direction vector and call-sign are available on the free internet for everybody, this is an additional support and could be misused as a threat for the safety.

Information about the avionic devices, the Integrated Modular Avionics concept (IMA) (see Figure 3) and its relevant Air Transport Association’s ATA42 chapter as well as the architecture and block diagrams from avionics and flight control of aircrafts like Airbus A380 are available on the Internet. (Airbus, 2006)

IMA shared resources are the avionics communications network. The solution selected is Avionics Full Duplex Ethernet (AFDX), and it is fully compatible with Ethernet Network of Open World and based on common switch modules. IMA modules are i.e. Core Processing & Input/output Modules (CPIOM), Input/output Modules (IOM) for hosting of several applications and signal acquisition/transmission.

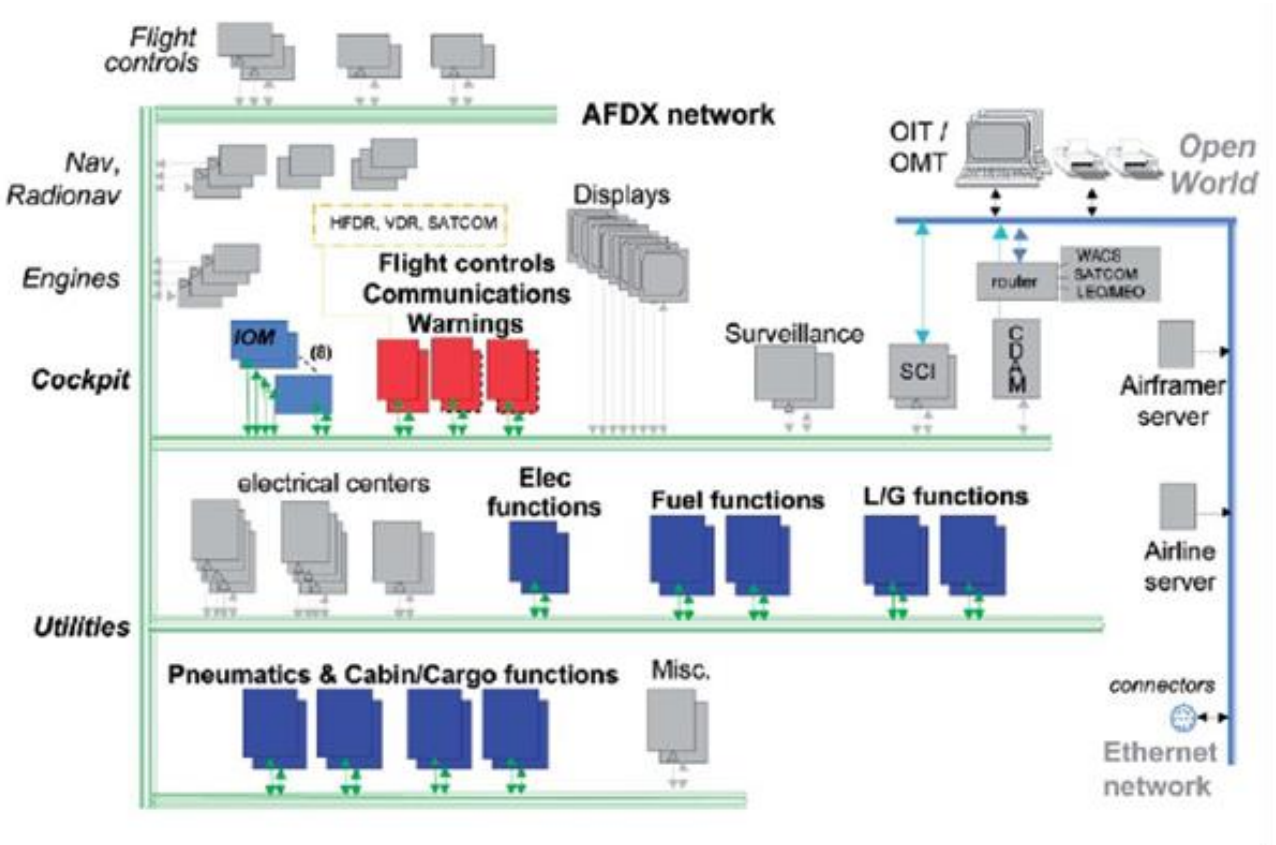


Figure 3. Integrated Modular Avionics – A380 airbus

Another most problematic support is available for training of opponents utilizing the free-internet by publishing information packages from the annual DEFCON meetings, where the cyber-attack relevant information lectures for aircraft and drones hacking are provided by video training. (See http://www.youtube.com/watch?feature=player_embedded&v=1pVP2DhR9Us)

With a dedicated analysis by FMECA and the pre-selection of potential entry points for Cyber Attack by EMS, the more detailed analysis and recommendation will be elaborated. It would also be possible to investigate with a dedicated Failure Tree Analysis (Liggesmeyer, 2009) the weak interfaces between the sensors and the avionics system in ATA42/IMA and ATA23/Communication, which are the breakdown structure for the design, verification and airworthiness rules by EASA and FAA.

## 5. Aviation threat environment

Applying the FMECA methodology on the preselected risk areas from the on-aircraft evaluation, the questions have been raised about the safety of prolonged use of life-time consideration and legacy equipment, which might have experienced upgrading and improvements. It is a most problematic area, when you have the legacy requirements from one or two decades ago and look for a replacement due to obsolescence and need to procure a microprocessor with a lot more computing power and dataspace, most probably defined and produced in an area of the world, where you do not have direct access to the foundry. This may cause additional threat potential, as the principle of embedded subroutines and lay-out for “kill-switch” methodologies must be excluded. The procedure for doing so is not implemented in all the relevant companies and relevant procurement and QA processes nowadays, but relevant services are going to be build-up in specialized companies with forensic experiences. (Kudelski, 2017)

Avionics flight control, the most critical system in a commercial and military airplane, has been moving from a partial by-wire to a more complete fully in electronics by-wire architecture. A level overview of an aircraft’s electronic flight control system interaction, which is very similar in lay-out, functionality and risk pattern and redundancy in the sense of signals from cockpit to the control surfaces and feedback loop. A most modern architecture is shown in the design criteria for an airplane like the Airbus A380, where computers compare differences between the commands, which must last for an enough long period before the command and monitor pair disconnects are forming a fail-fast module, while another command and monitoring computer is

in the stand-by as so-called hot spare. The computers are running a self-test loop, whenever the plane is energized. (Airbus, 2006)

An additional aspect for reliability is that the alarms awareness messages and fault-recovery are provided and executed real-time to allow very fast and safe failure compensation. Two primary command and monitor computers, which are available in a pair of secondary command and monitor computers, based on different hardware ICs. Each of the four pairs has different SW developed by different SW development teams and with different tools. This is already a very advanced methodology, which is not so common in legacy products either on commercial aircraft or military aircraft designs, where redundancy is build-up by common design but duplicated only and organized in Master-Slave functionality.

Design diversity in aircraft design is a very important aspect for its system designs, which is based on dissimilar computers and the physical separation of redundancy features, multiple software baselines, compilers during the development cycle and the data diversity. Airbus A380 concepts are based on commercial dual redundant ethernet data networks and Windows for non-critical applications. Those systems like the entertainment system, flight log for cockpit aircrew or the passenger list for flight attendants need to be considered in more details, as it is known in public, that the different versions of Windows application gives way for hacking by open problem descriptions published in open sources. It is this kind of awareness, which is utilized by hacker groups to identify open door entry inside the ethernet bus-system network which might not yet shielded or hardened in the most secure way. The efforts for assessment therefore need to consider the possibility to enter with devices from the EMS into the bus-system/network for manipulating access and data integrity. (Airbus, 2006)

The sensors related to ATM and collision avoidance are possible target of the attack. Especially the spoofing of GPS navigation signals could be a form of attacks, which will cause severe problems during flight. More delicate will be the coordinated take-over of 3D-situation data (flight vector, speed and altitude) in the Collision Avoidance Systems, which by nature are not well hardened as those are transmitting the data between the aircrafts in flight to do the job. In combination with the already mentioned transparency of flight radar tracker, a combined spoofing and fake data uploading is possible to introduce and prepare incidents or near-miss between aircrafts in a same region with same flight vectors and Flight Levels.

The threat is real in the aviation industry, like the rest of the world, it is becoming more and more interconnected, which increases attack vectors to enter systems. When you understand the domain, you are operating in and when you understand the weaknesses and vulnerabilities you can build defenses, but it needs core strengths — engineering and technology (Delorge, 2018). While disrupting air traffic and crippling the economy is frightening enough, the greater fear is that hackers could crash airplanes or make them vanish from radarscopes. One solution, the Cyber Intrusion Detection System, is a cyber-attack warning system that alerts pilots if anything on the aircraft has been hacked or is doing something it shouldn't.

During military operations, a cyber-attack on an aircraft could trick pilots into not trusting their instruments and aircraft. If they don’t trust their aircraft, then the mission fails. According to assessment it is identified that malware could be introduced through the supply chain, since aircraft parts are manufactured by many different sources around the world. Therefore, detection systems looking for anomalies on the special on-aircraft bus-systems are necessary. These communication systems control, monitor and transfer data between different electronic components in the aircraft and remote terminals. Many devices connect to those buses, such as annunciators, flaps, lights and landing gear.

In simpler terms: to protect planes and everything around them as attentively as people protect their smartphones. “On my phone, I’m constantly being pushed updates to improve the device’s security,” Delorge said. “We need that same diligence and vigilance in aviation.” Delorge believes the aviation industry should implement a layered approach to cybersecurity, which use several defense mechanisms such as access restrictions, two-factor authentication, encryption, proactive threat hunting, insider threat monitoring, and managed detection and response. (Delorge, 2018)

The most critical clusters is in aerospace, but these findings could be transferred also to automotive technology, as there are similar trends in autonomy driving in the future with the data transfer and management for positioning and flight/driving vectors. In combination with the GPS or future GALILEO navigation data support incidents can be prepared by utilizing the EMS for intrusion of fake data and malware in unprotected, less hardened systems.

Software defined radios in principle are an entry point for data and information transfer linked with the communication and on-aircraft bus-system. There are different levels of protection and hardening, but in principle they are an interesting source for getting attacked and utilized for influencing situation awareness; artificial intelligence could help in the future to control the identified critical areas and support the mentioned identification of disharmonies and wrong corrective measures identification as a cyber-attack warning system (Tyugu, 2015).

These problems might be covered under sabotage, but where not part of any consideration for risk assessment (Altfeld, 2010) and mitigation during last decade. Therefore, it will be worthwhile to evaluate the potential influences also in this respect and discuss about potential dormant problem areas embedded in legacy systems from today's point of view.

**Conclusion and recommendation**

The potential for an adversary to inflict damage on states through EMS attack has grown significantly. Today, all aspects of society, governance, and security have dependencies on EMS. However, power grids, telecommunications, and many command-and-control systems have not been designed to survive a hostile EMS environment. (Stuckenberg, 2018)

In all the different literatures on assessment and research, the conclusion was unique and everybody in the relevant business cluster, once the real problem could raise up and the preparation done nowadays is not sufficient and late compared to the problems embedded by legacy systems and missing regulation but also the indicated sources in the free internet for teaching and supporting hacking. Relevant networks and workshops with the experts are established meanwhile since 2016 and EASA has performed a workshop identifying the needs and procedures for cyber relevant measures like: standardization, training-awareness-education, civil-military interoperability, risk assessment and methodology, testing (EASA, 2017). IATA has established a 360° training and awareness support for airlines with procedures, training material and provides information for a proactive approach to avoid cyber risks. (IATA, 2017)

Are industry and relevant circles with the link to knowledge-based information exchange and training? As there is a closing up between cyber systems and their dependency on the EMS, as those evolved from wired to wireless architectures (NEC, WLAN, situation awareness sensors), this EM dependency is the real essence of the Cyber-EMS relationship. As nearly most of the devices and capabilities uses the EM environment, as well as the EM systems that provide EM control are not inherent dependent on the cyber space, it is not necessary that an EM system has access to cyber space. That access would not be necessary to enable the embedded ability to maneuver in the EM environment.

From an EM environment point of view, cyber systems reside strictly in the data exchange layer and even the prospective cyber-attack options possibly delivered by radiofrequency jammers are performing a communication function and therefore most parts of the cyber systems are only the EMS users, because datalinks, data networks and information exchanges need access to the EM environment to move around the metadata with information content. It is an experience coming out of the Iraqi battlefields by being confronted with the radio-controlled improved explosive devices, that an opponent or adversary will always seek to exploit the areas of the EM environment where the society, military, federal administration and also the commercial business area yields operational control. Therefore, it is recommended to draw down these virtual boundaries in the discussion forums and bring together the people working in cyber, EW. It is a unique maneuver space upon which all the other military, paramilitary and law enforcement organizations depend.

While EMS vulnerabilities and threats have matured, national and even international capabilities to deny or mitigate such threats and vulnerabilities remain highly dispersed or incomplete (Stuckenberg et al. 2018). Therefore it could be most beneficial to enlarge the scope of relevant assessments for National Cyber Security Strategies and include the relevant paradigms from cyber in the EMS, because only awareness of potential risks and not covered risk mitigation will be helpful for cyber attackers to generate the only target they want to achieve – harm and chaos for entering in control and suppress the society and established rules and welfare. When European states renew their cyber strategies, it is imperative that they consider the entire cyber and electromagnetic environment. This is how CyberSec. as a whole can take care of as part of national security.

## References


Airbus (2006). A380-Level III-ATA42 Integrated Modular Avionics & Avionics Data Communication Network. A380 technical training manual. https://de.scribd. com/document/ 226105294/A380-Level III. 2006

Altfeld H-H. (2010). Commercial aircraft projects- managing the development of highly complex products. Taylor & Francis Ltd.

Arnold J. T. (2009). The Shoreline: Where Cyber and Electronic Warfare Operations Coexist, A Research Report, Air War College Air University, Montgomery, Alabama, 17 February 2009

Delorge B. (2018). Interview Raytheon VP of Transportation and Support Services

De Martino A. (2012). Introduction to modern EW systems. Artech House

EASA (2017). Cyber-security Workshop – Final Report.

Hagengruber R. (2017). Künstliche Intelligenz – wann übernehmen die Maschinen? Univ. Paderborn. Science on - DFG Podiums Diskussion 12.7.2017

Hay T. E. (2016). Determining Electronic and Cyber Attack Risk Level for Unmanned Aircraft in a Contested Environment, Air Command and Staff College, Air University, Montgomery, Alabama, August 2016

Henselmann G. (2017a). Cyber Security in Aeronautics – a generic approach to identify the weaknesses in legacy systems. DWT Cyber Security Workshop, Bonn, 12.-13.12.2017

Henselmann G. (2017b). Devising and Implementing a National Cyber Security Strategy. Lecture in GSCP, Geneva, 5.10.2017

Hilbert M. and López P. (2011). The World's Technological Capacity to Store, Communicate, and Compute Information. In: Science, 332(6025), pages 60–65

Hofmann R. (2017). Cybersecurity of Things-part 1. An introduction to challenges and techniques for building and operating devices securely. High Assurance Systems/ebook MKT1012.1. www.high assure.com.

IATA (2017). Proactive approach key to mitigate cyber risk. http://airlines.iata.org/news/proactive-approach-key-to-mitigating-cyber-risk-0?_ga=2.94774549.808867565.1529068694-1381224138.1529068694

Koch R. and Golling M. (2016). Weapon systems and Cyber Security – a challenging union. 8th Intern. Conference on Cyber Conflicts, 2016. Pages 191 ff

Kudelski Laboratories. (2017). Kill switch forensic. www.kudelskisecurity.com/sites/default/files/files/Kudelski_Security_MSS_Endpoint_Breach_Detection_EN.pdf

Lehto M. (2015). Phenomena in the Cyber World, in M. Lehto, P. Neittaanmäki (Edit.) Cyber Security: Analytics, Technology and Automation, Springer, Berlin, pages 3-29

Lehto M. (2018). The modern strategies in the cyber warfare, in M. Lehto, P. Neittaanmäki (Edit.) Cyber Security: Cyber power and technology, Springer, Berlin, pages 3-20

Liggesmeyer P. (2009). Software-Qualität; Testen, Analysieren und Verifizieren von Software. Springer Verlag

Russel S. and Norvig P. (2003). (Edit.). Artificial Intelligence- a modern approach. 2nd edition. Prentice Hall Series

Ryan J. (2015). (Edit.) Leading issues in Cyber Warfare and Security. Vol.2. ACPI

Schmidt E. and Cohen J. (2014). The New Digital Age: Reshaping the Future of People, Nations and Business, Vintage Book

Seffers, G. (2018). A Quest for Answers on Army Expeditionary Cyber teams, Signal, November 2018

Stuckenberg D., Woolsey R. J., DeMaio D. (2018). Electromagnetic Defense Task Force, 2018 report, LeMay Center for Doctrine Development and Education, Air University, Montgomery, Alabama, November 2018

Tyugu E. (2015). Artificial Intelligence in Cyber Defence. Scenario 2040. Cyber Defence – NATO CANADA. 32nd International East/West Security Conference




View publication stats