Required Abilities for a Cyberwarfare Officer in an Air Flight Squadron: A Curricular Analysis

Maj. Tiago J. Diedrich, , Brazilian Air Force
Lt. Col. Luís E. P. C. Cordeiro, , Brazilian Air Force
Sgt. Felipe Coradesque, , Brazilian Air Force

Cyber Defense in Brazil

The Brazilian National Defense Strategy (BNDS), released in December 2008, addressed for the first time, at the political level, a concern about cyber-related issues. At it´s core, the BNDS defined that all branches of the military forces should guarantee the protection of the government's computer network systems, under the coordination of the Brazilian Army.[1]

On the document, it was also clear that the Brazilian Air Force (BAF) would be responsible to specify its own internal guidelines in order to provide for the defense of the military organizations under its responsibility.[2]

As defined in its own basic doctrine, the BAF considered cyberwarfare as the capability to monitor computer network communications of interest in the event of a military conflict. In other words, BAF personnel should be able to protect its own networks and explore/attack targeted networks using cyberspace as a battlefield,[3] since cyberspace is a virtual environment which contains computational devices used to process and store digital communications which may or may not be interconnected by public or private networks.[4]

Therefore, the BAF defined that cyberwarfare operations means activities in order to provide successful use of cyberspace in war operations at all command levels, since it maintains a direct relationship with the Command and Control (C^2) of the operation through the information safeguard.[5]

As an example of the importance of cyberwarfare operations, in April 2015 the United States National Intelligence Director prioritized the cybernetic threat as a top priority, ahead of the terrorist threat, which was the number one on the list since 9/11.[6]

Some previous occurrences may have triggered this warning. Back in 2010 a computer virus called Stuxnet was discovered, some would say it is the first cyber weapon ever delivered. Part of an attempt to delay Iran's nuclear program, this virus attacked the industrial data monitoring and acquisition system of the Iranian uranium enrichment plants in Natanz, developed by Siemens, speeding up the centrifugal spin causing damages to the system while the data on the monitor appeared to be normal, and it was capable of doing everything while preventing detection.[7]

In Brazil, during the Rio+20 in 2012, for the first time a report of a cyberattack was released when an attempt to invade a government agency responsible for the defense of critical computer network communications throughout Brazil came to the public.[8] In 2015, the Minister of Defense at the time, Mr. Celso Amorim, reported his concern about the lack of security in this area as well as the need to defend it during the 2016 Olympic Games.[9]

In a more recent context, Norton antivirus presented a statistic reporting the occurrence of various crimes in Brazil during 2017. These crimes generated a loss of US$22 billion, placing the country in second place in the world with regards to cybernetic losses.[10]

All of this has caught the attention of the BAF Air Operations General Command (AOGC), which started to invest its resources in order to become ready to fight in cyberspace. As an example, one of the authors participated in a Multinational Exercises called PANAMAX as a Cybernetic Planner. Through this military operation, promoted and executed annually by the United States, it was possible to learn about interoperability, training military personnel in planning tasks and executing activities integrating Cybernetic, Psychological and Electronic Warfare (EW) in a joint force with 17 nations.

One of the lessons learned was that cybernetic activities demand prepared personnel at the tactical level in the Air Flight Squadrons (AFS) of the BAF, as was already in place in other countries participating in the exercise. This holistic application of a Cyber Officer follows the example of other positions held in the AFS such as the Flight Safety Officer (FSO) and the Electronic Warfare Officer (EWO), because they are activities that require a certain degree of specialization that can only be achieved through specific courses. Since these functions (FSO and EWO) already exist in the BAF flight unit structure, we understand that it would be reasonable to propose the establishment of a Cyberwarfare Officer (CO) position. The problem lies in defining the gap in the abilities between the regular flight curriculum and the abilities needed for a CO, and that is the objective of this article.

For example, the BAF chose to use officers graduated from its Air Force Academy (AFA) as pilots to fulfill the position of FSO and EWO by providing additional specialized courses after graduation that could vary in length from eight to forty weeks, depending on the level of knowledge required. The reasons for using pilots for these functions include that they have the same background (what makes it easier to plan the content of the specialized courses to achieve the necessary abilities), their first post is usually a flying squadron in which they will be working for five to ten years and they have knowledge of the kind of mission their aircraft will perform. There is no formal rule demanding that this kind of position must be occupied by a pilot, but in actuality, this is how it happens.[11]

When it comes to Information Technology, each Air Force Base (AFB) has a group of designated Information Technology Officers (ITO), usually graduates from civilian universities and

responsible for managing routine duties such as server maintenance, network usage optimization, password control and so on. Although these officers could be use as COs, in our opinion there are three major disadvantages to do so: there is a shortage of these types of officers, they have a maximum time of eight years as enlisted due to Brazilian legislation, and they could only work as O-1 and O-2 officers, since 1st Lieutenant is the highest rank they can attain.

In contrast, although pilots have a lack of specialized abilities related to IT, they can be trained, and remain in the position for a longer period of time compared with the ITO, they have an operational view of the mission since they also perform squadron flight missions, they can be promoted up to O-10, and there is a relative abundance of pilots in the BAF.

Another factor is that no university in Brazil graduate personnel in cyber security; all personnel must accomplish post-graduate specializations on the subject. This means that anyone who occupies the position of CO would need specialized training, regardless of background. Of course a graduate in the area of IT would have a stronger background on cyber in general, but a graduate from the AFA would have a stronger background on leadership and warfare, specifically on the type of operations of his/her particular unit (fighter, SAR, ISR, mobility, bomber, etc.), giving him/her a more precise view of the cyber operations at a tactical level.

In our opinion, all of this makes it more advantageous to employ AFA graduate pilot officers as COs in a flying squadron.

This being the premise, we looked at the pilots' core curriculum, which is basically focused on leadership and flying, with some degree of administrative procedures, and other related courses (physics, math, psychology, management), aside from the military foundation.[12] Considering this, our first objective was to investigate the abilities related to cybernetics developed by the pilot while in the AFA (if there was any), and second, comparing them to the abilities (Knowledge, Skill and Attitude – KSA)[13] required to the AFO position.

With data in hand, we were not only able to determine what are the required abilities a CO in a flying squadron, but also the extent that the curriculum adopted in 2017 developed the essential abilities for a pilot to hold the position of a CO in a flight squadron right after graduation, thus allowing us to identify the gap between what is taught at AFA and what is needed to become a CO.

We chose to follow a Cartesian method by dividing our big problem (the gap of abilities) in two smaller problems, each one related to one Guiding Questions (GQ) listed below:

GQ1) What are the essential abilities that a CO must possess?

GQ2) What are the essential abilities developed at the AFA pilot curse that are related to the CO function?

In the end, by answering both questions we reach a conclusion to our problem and contribute to further research on cybernetic activities within the armed forces, especially in support of the Brazilian Air Force.

Knowledge, Skills and Attitudes

Educational institutions identify that training human resources is a hard and complex process. Thereby the motivation of the student is a core factor to achieve the required level at the end of the course. In the military career field it is no different, one must want to learn in order to learn well, and consequently develop the necessary abilities .[14]

In this article, we understand that ability is defined as:

> The set of knowledge, skills and attitudes required to perform a particular activity, [...] such as the performance expressed by the person in a given context, in terms of behaviors and achievements resulting from the mobilization and application of knowledge, skills and attitudes at work.[15]

Brandão specifies abilities based on these three dimensions (knowledge, skills and attitudes -KSA) and associates these characteristics with the cognitive, technical, social and affective aspects related to work.[16] This amplifies the considerations defined by Carbone et al. because it relates the personal competences to the professional activities exercised by the individual, as a way to improve the quality in the services.[17]

Therefore the following KSA considerations are adopted for this article:

> […] knowledge corresponds to information that, when recognized and integrated by the individual in their memory, has an impact on their judgment or behavior. It refers to the knowledge that the person accumulated throughout his life, something related to the memory of concepts, ideas or phenomena [...] skill is related to the productive ability of knowledge, that is, the capacity of the person to use stored knowledge. [...] attitude, in turn, refers to social and affective aspects related to work [...] and concerns the feeling or predisposition of the person, which influences their conduct towards others, to work or to situations.[18]

As a way of identifying the abilities to be developed by an individual to perform certain tasks, Santos suggests to apply the Delphi Method to gather the opinions of experts, that is, an intuitive and consensual judgment of a participant group, which must have experience in a given task. The information of this group should be collected anonymously through questionnaires and from this a statistical representation about the defined concepts should be generated in order to facilitate the understanding. The objective of this methodology is to achieve a consensus among the specialists about the list of competencies needed, since there is no previous study about what should be the KSAs needed for a CO.[19]

In this paper we will use the term "essential competence" to characterize a core ability that must be developed during the learning process (during his/her time as an Air Force Cadet) of a student so he/she could be able to execute specifics tasks in an organization (in this case, a CO at a BAF unit). On the order hand, a "desirable competence" is an ability that although would increase the KSAs of a student, doesn´t need to be learned in order to prepare the individual to execute the desired task. Since the learning processes must be continuous through time, the desirable competences can be offered as"on the job" training (during his/her time as a CO) in a continual process.[20]

A CO must be capable of responding to the expectations of the BAF regarding cyberwarfare requirements to the operational needs of the unit to which he/she is subordinate. For this, the grouping of essential competences of a CO must be part of the curriculum used during the learning process, and the officer designated as a CO must undergo continuing education to fulfill the needs of the organization.[21]

The type of education offered by an educational institution, with regards to academic planning, must be structured and organized in the school's curriculum. Therefore, the curriculum represents the discipline itself, that is, the curriculum of a course associated with a level of education expected to be achieved by the student at the end of the course. The curriculum's composition is associated with mandatory academic disciplines, including minimum credit hours, with the purpose of promoting the efficiency and legality of the learning process, and should be changed during through a continuous development process.[22] Therefore, we chose to restrict the study period to 2017, which is the latest program of study available.

A syllabus must prepare the apprentice to practice, and the KSAs developed must be an open door to the abilities that a professional acquires over time doing the same task, that is, the essential competences must prepare the learner to develop the desirable ones throughout the operational life of a CO. As defined by Sacristan:

> […] a curriculum, actually, perform different missions at different educational levels, according to their characteristics, as they reflect different purposes of these levels. This is a difficulty

in the pretense of obtaining a clear scheme [...]. At the same time, it is a warning against the pretensions of simplistic schemes of universalization of education.[23]

In the end, the curriculum refers to the professional abilities expected of a certain "class" of professionals, which will allow them not only to execute a determined task but also be capable of becoming an expert. These should be the foundations of any learning process: define what one must learn in the classroom that will give him/her the abilities necessary to, in practice, fulfill what is expected and also be capable of pursuing continuous learning in a roadmap thorough his/her career. It is not just about delivering a worker, but to plant the seed of a professional.[24]

Thus, in the case discussed in this article, we chose to use a group of specialists who are already involved in cyberwarfare since we understand that they have a more precise view of what KSAs should be taught at the beginning and which should be learned on the job, providing a training roadmap for the officer pilot to hold the CO position in a flying squadron, in order to answer our research question.

Methodology

This research used a descriptive research to identify what are the essential abilities that a CO must possess, since we used the data collected from the specialists in cyber through the Delphi's method questionnaires; and in parallel a documentary research by examining the regulations and the curriculum of the AFA.[25] It is important to clarify that those documentations do not receive an analytical treatment since they have a rich and stable data source.[26]

Following the proposed approach, initially we identified the competences that the CO must have to perform his/her role. For that, the first step was distribute a questionnaire to a specific audience of professionals in order to identify each one's experiences and therefore decide who could have the knowledge necessary to compose the group of experts.[27]

Once we narrowed the targeted audience, another questionnaire was used for the preliminary consolidation of the KSAs, based on the experts' opinions. To that end, the military group interviewed, without exchanging ideas, answered the following question: "What are the competencies needed for the Cyber Officer in a flying squadron?" All responses were collected, eliminating repetitions, and the interviewers were stimulated to justify their choices.

Next, a third questionnaire was sent to the interviewees with the following statement at the top of the page: "Do you agree that these characteristics correspond to the abilities required for a pilot to hold the role of Cyber Officer in a flying squadron?" followed by the knowledge, skills and attitudes (and the justifications for each one) defined by the experts in the previous round, so that we could establish which are the competencies needed for a CO.

Finally a fourth questionnaire was sent with the objective of differentiating which competences are essential and which are desirable. The survey started the question: "Do you agree that these characteristics correspond to an ability considered part of an "essential competence", which means a core Knowledge/Skill/Attitude that must be developed during his/her time as an Air Force Cadet so he/she could be able to become a Cyberwarfare Officer as soon as he/she gets to his unity?", followed by all the KSAs (and its linked justifications) found in the third questionnaire.

In both the third and fourth questionnaire an acceptance level (or a coefficient of concordance) was calculated to define which knowledge, skills and attitudes would be accepted using Santos' methodology with a defined threshold level of at least 60% of acceptance, using the following formula[28]:

$$Cc = \left(1 - \frac{Vn}{Vt}\right) * 100 \qquad (1)$$

Where:

Cc = Coefficient of concordance or acceptance level, expressed as percentage;
Vn = number of specialists in disagreement with the predominant criterion; and
Vt = total number of specialists.

With the results in hand, we were able to distinguish the essential competencies from the desirable ones (the answer to the GQ1) and we could search for the answer to the GQ2 by comparing the 2017 curriculum content with the KSAs found.

Information and data

We used two main criteria to gather the group of specialists: one should be a military instructor of cyberwarfare or have a career in cyberwarfare and be involved with the development of the cyberwarfare doctrine of the BAF. The justification of the first choice is related to the view of someone who has the knowledge of how cyberwarfare must be taught and the second choice to a view of how cyberwarfare should be used in an Air Force.

The questionnaires were sent and 27 military personnel were identified as potential experts: 15 of them being from the Air Force and consultants of the Basic Doctrine development group with regards to cyber and 12 being from the Army and instructors from the Cyber Defense Center, the organization responsible to educate and train all military personnel in matters of cyberwarfare. All 27 agreed to be part of the research, which made our sample equal to our universe and therefore there is no need for inferences or extrapolations in the results.

Once we had the expert group defined, the second questionnaire was sent to them and in response we obtained 74 competencies divided into 34 knowledge, 20 skills and 20 attitudes. A list with all of the answers and the respective justifications was made and then the third questionnaire was sent to all 27 military personnel. The results of their responses have allowed us to calculate the acceptance level of the each KSA, as shown on the following table:

Table 1 - Competencies listed by the specialists

Competence	Quantity	Cc ≥ 60%	Cc < 60%
Knowledge	34	32	2
Skills	20	18	2
Attitude	20	18	2

Source: The authors.

In the fourth and last round a new application of the Cc was made over the 68 competencies in the previous step, and as result we found 37 essential competencies for the pilot to hold the Cyber Officer position, as seen in table 2:

Table 2 – Essential Competencies listed by the specialists

Competence	Quantity	Cc ≥ 60%	Cc < 60%
Knowledge	32	16	16
Skills	18	9	9
Attitude	18	12	6

Source: The authors.

With the results in hand, we were able to respond to our first G1: which are the core abilities a CO must possess.

Going after our answer to the second GQ, we started a research on the official papers that regulate the officer pilot course curriculum at the AFA. Two documents were found: the Minimum Curriculum (MC) and the Didactic Unit Plan (DUP). The first contains the basic disciplines that one should attain in order to fulfill the minimum requirements to become an officer, in other words, a contingency plan that should be used in case a shorter and/or cheaper course is needed. On the other hand, the DUP is the guiding document which contains all the activities that must be done during the course, encompassing the MC. That´s why we choose the Didactic Unit Plan used in 2017 to compare it with the data collected.

That being said, our analysis revealed that the DUP prescribes the teaching of operational systems general theory, decision support systems, basic concepts of cyber physical components (types and storage); cyber logical components (operational systems and programming languages); telecommunications (computer networks, types of communications and internet/web environments) and information security (concepts).[29]

Once we had all this data in hand, we were able to compare the KSAs found with the disciplines present in the 2017 course.

Data Analysis

In order to facilitate the understanding of the results, we chose to first show individually each one of the 37 essential competences (divided in groups of Knowledge, Skills and Attitude) along with the specific discipline.

On the left side of the following tables are the essential KSA defined by the specialists and on the right side which discipline from the Didactic Unit Plan covers that specific ability. The ones we found no correlation will be written "nonexistent".

Table 3 - Relationship between Knowledge and the DUP

Knowledge Essential Competencies	Competences Developed by the DUP
01 - Basic cybernetic course	nonexistent
02 – BAF's Basic Doctrine	Discipline: Military Doctrine
03 - Cyber Defense Military Doctrine	nonexistent
04 – Hardware functionality	Discipline: Information Technology
05 - Cybernetic threats identification	nonexistent
06 - English	Discipline: English 1, 2, 3 and 4.
07 - Basic notions about protocol	nonexistent
08 - Basics notions about configuring computer networks	Discipline: Information Technology
09 - Basic notions about servers	nonexistent
10 - Cybernetic technological innovation	nonexistent
11 - Recognize Information Systems and Information Technology vulnerabilities	Discipline: Information Technology
12 - Information security rules	Discipline: Information Technology
13 - Operational systems	Discipline: Information Technology
14 – Cyber attacks types	nonexistent

15 – Cyber exploitation types	nonexistent
16 – Cyber protections types	Discipline: Information Technology

Source: The Authors.

It is noted that only half of the competencies developed by the AFA may in fact support the pilot to hold a Cyber Officer position. When it comes to Skills, a correspondence of four in nine is observed, as seen in Table 4:

Table 4 -Relationship between Skill and the DUP.

Skill Essential Competencies	Competences Developed by the DUP
01 – Oral communication about cybernetic issues	nonexistent
02 – Written communication about cybernetic issues	nonexistent
03 - Develop a security incident management plan	nonexistent
04 - Develop cyber protection plans	nonexistent
05 – Identify computer network vulnerabilities	Discipline: Information Technology
06 – Identify information Security threat events	Discipline: Information Technology
07 - Plan cybernetic doctrinal activities	nonexistent
08 - Plan malicious computational models analysis	Discipline: Information Technology
09 – Teamwork and leadership	Discipline: Organizational Psychology

Source: The Authors.

Finally we have the worst scenario when it comes to Attitude, with only four of twelve essential competencies observed:

Table 5 -Relationship between Attitude and the DUP.

Attitude Essential Competencies	Competences Developed by the DUP
01 - Self-educated in cyber	nonexistent
02 – Cogent of the importance of cyber issues among his peers	nonexistent
03 – Accountable when defining users access levels and functionality	nonexistent
04 – Confident when talking to authorities about the importance of cyber	nonexistent
05 - Encourage the subordinates to develop theirs cyber competencies	nonexistent
06 – Updated on cyber doctrine	nonexistent
07 - Promotes training in cyber	nonexistent
08 - Promotes protection actions for computerized environments	Discipline: Information Technology
09 - Promotes improvements for integrated information management systems	Discipline: Information Technology
10 - Promotes network contingency plans	Discipline: Information Technology
11 - Promotes information security procedures	Discipline: Information Technology
12 – Take the lead on cyber incidents	nonexistent

Source: The Authors.

Based on the information generated through the data collection, the total results are described below.

Table 6 – Essential Competencies relationship

Competence	Covered by the curriculum	Total essential competencies
Knowledge	8	16
Skills	4	09
Attitude	4	12
Total	16	37

Source: The Authors.

With the final data gathered, it was possible to answer the GQ2by identifying what are the essential abilities developed by the AFA pilot course that are related to the CO function.

By doing that, we could answer our research question concluding that the curriculum adopted by the AFA in 2017 had developed 16 of the 37 essential competencies necessary for a pilot officer to hold the position of CO in a flying squadron right after graduation from the AFA, identifying a gap of 21 abilities.

It is important to emphasize that our study was a snapshot of a certain group of people during a certain scope of time. A change in the curriculum or in the group of experts would probably lead to different conclusions, but we understand that it could not be used to refute our conclusion since we focus on the development of a method, not on the results. With a group of experts more heterogeneous and a 2018 or 2019 curriculum, we would still be able to identify the gap in abilities, and answer our question.

Conclusion

The motivation for this research was first due to the National Defense Strategy's decisions, which required the protection of computer network systems in the national territory. Inside this, the BAF basic doctrine made clear that cybernetic operations are directly linked to enemy and friendly C2 operations, at all command levels.

The importance of cyber was highlighted trough domestic and foreign examples, and the experience at PANAMAX aroused an idea: the creation of a position similar to the one related to flight safety and electronic warfare in the air units of BAF with focus on cyber operations at a tactical level being conducted by pilot officers.

With that in mind, our problem became to define the gap in abilities between what pilot officer possesses and the ones needed for the cyberwarfare officer at an air unit. We chose to approach the issue by dividing the central problem in two minor guiding questions in a Cartesian way. We also divided the abilities into "essential competence" and "desirable competence", the first meaning an ability that must be learned during his/her course before the end of graduation and the second one could be learned on the job, and we also divided the competencies into Knowledge, Skills and Attitudes.

In order to answer the first guiding question "What are the essential abilities that a CO must possess?" we used the Delphi method in a group of experts and we found 37 essential abilities that a CO in an air unit must possess. To answer the second guiding question "What are the essential abilities developed at the AFA pilot course that are related to the CO function?", we sear-

ched through the officer pilots' 2017 curriculum and we compared them to the 37 essential abilities found.

Our final conclusion is that 16 of the 37 essential abilities needed for a CO in an air unity are taught at the AFA pilot officer course, and with that we were able to identify a gap of 21 abilities.

As recommendation for future work, it is suggested the verification of the gap of desirable competences for pilot officers and the research of the same gap between IT personnel. This will allow a more precise comparison between both careers and a development of a more holistic approach to cyber operations, since a commander would be able to identify the KSAs of both branches, which would provide more data to decide specific duties in a cyberwarfare environment. ❑

Notes

1. Ministério da Defesa, Estratégia Nacional de Defesa (END) (Brasília, DF: Ministério da Defesa, 18 December, 2008), http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm.
2. Ministério de Planejamento Orçamento e Gestão, Implantação do Sistema de Defesa Cibernética: Ações Orçamentárias Integrantes da Lei Orçamentária para 2013. (Brasília, DF: Ministério de Planejamento Orçamento e Gestão, May 2013), http://www.orcamentofederal.gov.br/orcamentos-anuais/orcamento-2013-1/arquivos-cadastro-de-acoes/2058.pdf.
3. Comando da Aeronáutica, Doutrina Básica da Força Aérea Brasileira (DCA 1-1), April 2012.
4. Ministério da Defesa, Doutrina de Operações Conjuntas (MD30-M-01), May 2011.
5. Ministério da Defesa, Doutrina Militar de Defesa Cibernética (MD31-M-07), August 2014.
6. Department of Defense, The Department of Defense Cyber Strategy, (Washington, DC: Department of Defense, 17 April 2015), http://weaponsman.com/wp-content/uploads/2015/04/U-DoD-Cyber-Strategy-2015-17Apr15.pdf.
7. Jhon Markoff and David E. Sanger, "In a computer worm, a possible biblical clue," The New York Times, 29 September 2010, http://www.nytimes.com/2010/09/30/world/middleeast/30worm.html.
8. Humberto Trezzi, "País cria sistema de defesa cibernética", Defesanet, 09 January 2013, http://www.defesanet.com.br/cyberwar/noticia/9228/pais-cria-sistema-de-defesa-cibernetica.
9. Ibid.
10. "Brasil é o segundo país em perdas com crimes cibernéticos", Istoé dinheiro, 22 February 2018, https://www.istoedinheiro.com.br/brasil-e-o-segundo-pais-em-perdas-com-crimes-ciberneticos/.
11. Comando da Aeronáutica, Currículo Mínimo do Curso de Formação de Oficiais Aviadores (ICA 37-113), June 2014.
12. Ibid.
13. Philippe Perrenoud, Construir competências desde a escola, (Porto Alegre: Artmed, 1999), 17.
14. Elliot Cohen, "Technology and warfare" in: Baylis et al., Strategy in the contemporary world, (New York: Oxford Univrsity Press, 2002), 141-160.
15. Pedro Paulo Carbone et al., Gestão por competências e gestão do conhecimento, 3rd ed. (Rio de Janeiro: Fundação Getúlio Vargas, 2009) 75.
16. Hugo Pena Brandão, "Gestão baseada nas competências: um estudo sobre competências profissionais na indústria bancária" (master thesis, Universidade de Brasilia, 1999), 20.
17. Pedro Paulo Carbone et al., Gestão por competências e gestão do conhecimento. (Rio de Janeiro: Fundação Getúlio Vargas, 2009) 60-61.
18. Ibid., 14
19. ,Armando Cuesta Santos, "O uso do método Delphi na criação de um modelo de competências", Revista de Administração da Universidade de São Paulo 36, no. 2 (April-June, 2001) 25-32, www.rausp.usp.br/download.asp?file=v36n2p25a32.pdf.
20. Afonso C. C. Fleury and Maria Tereza L. Fleury, "Estratégias competitivas e competências essencias: perspectivas para a internacionalização da indústria no Brasil", Gestão e Produção 10, no. 2, (August, 2003), 135.
21. Philippe Perrenoud, Construir competências desde a escola, (Porto Alegre: Artmed, 1999), 25.
22. Arieh Lewy, Avaliação de currículo, (São Paulo: EPU, 1979) 36-38.
23. José Gimeno Sacristán, O currículo: uma reflexão sobre a prática, 3rd ed. (Porto Alegre: Artmed, 2000), 19.
24. Ibid., 25.
25. Willian H. Schubert, Curriculum: Perspective, paradigm and possibility, (New York: Macmillan Publishing Company., 1986).
26. Antonio Carlos GIL, Como elaborar projetos de pesquisa, 4th ed. (São Paulo: Atlas, 2002).

27. Comando da Aeronáutica. Plano de Unidades Didáticas do Curso de Formação de Oficiais Aviadores (MCA 37-42), October 2015.

28. Armando Cuesta Santos, "O uso do método Delphi na criação de um modelo de competências", Revista de Administração da Universidade de São Paulo 36, no. 2 (April-June, 2001), 27, www.rausp.usp.br/download.asp?file=v36n2p25a32.pdf.

29. Comando da Aeronáutica, Plano de Unidades Didáticas do Curso de Formação de Oficiais Aviadores (MCA 37-42), February 2017.

Maj. Tiago J. Diedrich, Brazilian Air Force, graduated from the Brazilian Air Force Academy -class of 2003. Specialist in Remote Sensing and Geographic Information Systems by the Regional Education Centre for Space Science and Technology to Latin America and the Caribbean (2011); MSc in Electronics and Computer Engineering in the Information Area from the Aeronautics Technological Institute (2014); Postgraduate in Public Management and Air Force Employment from the Brazilian Air Force Squadron Officer School (2015). Major Diedrich has experience in the defense area and is interested in to the following topics: Intelligence (Images); Semantic Web; Ontology; Data Fusion; Image Processing and Interpretation; Command and Control, Communications, Computer, Surveillance, Target Acquisition, Recognition, Data Link and Cyberspace

Lt. Col. Luís E. P. C. Cordeiro, Brazilian Air Force, graduated from the Brazilian Air Force Academy - class of 1999. Currently he is the chief of the training division at the Aeronautical Accidents Investigation and Prevention Center (CENIPA), and before that he was an instructor at the Squadron Officer College (Rio de Janeiro, Brazil) for four years as an instructor of Air Force Basic Doctrine, Law of Armed Conflict and Joint Operations. Lt Col Celles has a M.Sc. (Political Science and International Relations) from the Brazilian Air University, also located in Rio de Janeiro. His areas of interest are: Cyber Warfare, Joint Operations, International Law of Armed Conflict, Airpower Doctrine, Flight Safety and Logistics.

Sgt. Felipe Coradesque, Brazilian Air Force, Coredesque -Graduated from the Brazilian Air Force Specialists School –class 2004. Currently he is a student at the São Paulo's Federal University (São José dos Campos, Brazil) and has been an instructor at the Brazilian Air Force Specialists School (Guaratinguetá, Brazil) for four years in remote sensing, image interpretation and digital image processing. Sgt Coredesque has a degree in Math from Santa Maria's Federal University (Santa Maria, Brazil) and a lato sensu post-graduate degree in Remote Sensing and Geographic Information Systems from the National Institute of Spatial Research (Santa Maria, Brazil). His areas of interest are remote sensing, digital image processing, image interpretation and Geographic Information Systems.