Integrity of a Common Operating Picture in Military Situational Awareness

Jaco Robertson
Council for Scientific and Industrial Research
South Africa
jrobertson@csir.co.za

***Abstract*—The lack of qualification of a common operating picture (COP) directly impacts the situational awareness of military Command and Control (C2). Since a commander is reliant on situational awareness information in order to make decisions regarding military operations, the COP needs to be trustworthy and provide accurate information for the commander to base decisions on the resultant information. If the COP's integrity is questioned, there is no definite way of defining its integrity. This paper looks into the integrity of the COP and how it can impact situational awareness. It discusses a potential solution to this problem on which future research can be based.**

Keywords-Command and Control, Common Operating Picture, Integrity, Situational Awareness

I. INTRODUCTION

The lack of qualification of a common operating picture (COP) can have a potential negative impact on the situational awareness of a military operation. Military commanders have to rely on situational reports based on situational awareness. These reports are compiled by the commander's line staff, based on their interpretation of available information. Therefore, the possibility exists that this information may be incorrect or subjective. As a result, the integrity of the resultant COP may be questioned. If the COP cannot be trusted, there is no guarantee that the commander will make the appropriate decisions, and this can have an impact on warfare and the safeguarding of peace within the country.

It is the author's experience that a commander either decides to trust the COP or totally disregard it. It may happen that a single element of the COP may not be 100% accurate, but since this affects the integrity of the COP, the commander may regard the entire COP as suspect. As a result, other accurate contributions from the COP may be unnecessarily disregarded.

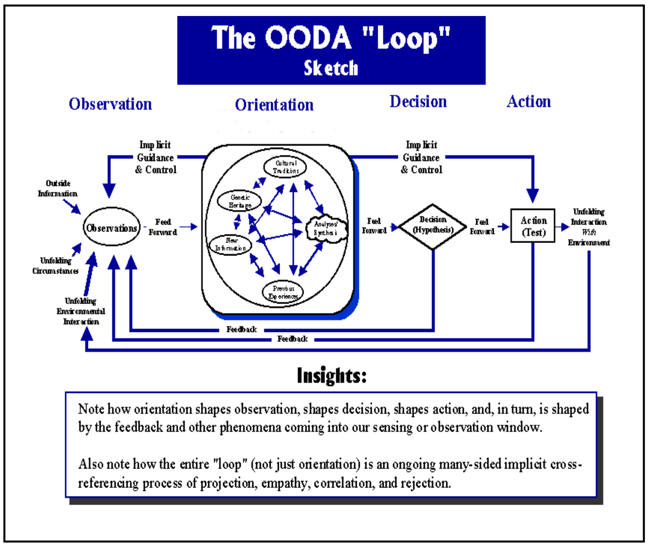
If a commander loses his trust in the COP (due to irrelevant data, wrongfully displayed data etc.), the commander tends to ignore all the information portrayed by the COP and needs to rely on other methods to keep informed of the situation within the battlefield. This is potentially detrimental to the situational awareness (SA). This paper aims to describe the problem of COP integrity and the lack of appropriate qualification, and aims to define a possible solution that could lead to future research.

This paper introduces a theoretical approach to determining the integrity of a COP. Further research and experimentation is required to evaluate the feasibility of the approach. Relevant terms are first discussed as background, then the concept of a COPs integrity. Five information security principles are introduced and then proposed as a way of evaluating the integrity of a COP. The paper does not cover the processes involved in achieving situational awareness nor the information required to create a COP.

II. BACKGROUND

Within the military environment, the commander in charge of an operation is responsible for all aspects of the operation and is accountable for the safety of the soldiers that are partaking in the operation. As an aid to make appropriate decisions regarding the operation, the commander relies on SA and situational reports to guide him in terms of the various operational parameters. This is necessary in order for the commander to make informed, timely decisions in advancing the operation's C2.

The U.S. Department of Defense Dictionary of Military and Associated Terms defines C2 as: "The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission" [1]. This authority is exercised towards the accomplishment of a common goal, whether defensive or offensive. C2 can be considered to consist of SA, planning, tasking and control. The goal of strategic and tactical C2 systems design is to present a situation selectively in a way that uses the commander's abilities to grasp and act in the best possible way [2].



Note how orientation shapes observation, shapes decision, shapes action, and, in turn, is shaped by the feedback and other phenomena coming into our sensing or observation window.

Also note how the entire "loop" (not just orientation) is an ongoing many-sided implicit cross-referencing process of projection, empathy, correlation, and rejection.

Figure 1. Boyd's OODA Loop

A commander typically operates on the principles of Boyd's OODA loop [3]. That is observe, orient, decide and act (see Figure 1). In the world's ever increasing digitised battlespace the commander is under pressure to speed up the OODA loop. To accomplish this, the COP becomes more and more integral to the commander's process. Therefore the trust in the COP is all the more pivotal. And then integrity of the COP is at the heart of the trust. Thus for the commander to command the operation successfully, the integrity of the COP is paramount to the commander. After all, as Brehmer stated "C2 is a human activity that aims at solving (military) problems" [4].

The commander achieves SA via the information presented to him via the operation's COP. The COP is generally a single display of relevant information shared by more than one command team. A command team being responsible for their operating picture. For example the airforce command team would be responsible for the air picture. The information is collected from various information sources and other pictures (see Figure 2). These sources tend to be different systems, located in different places.

These systems are not always under the control of the commander, but merely serve as a source of information, upon which a COP is built. If the systems provide the information remotely the integrity of the data link becomes crucial to having SA.

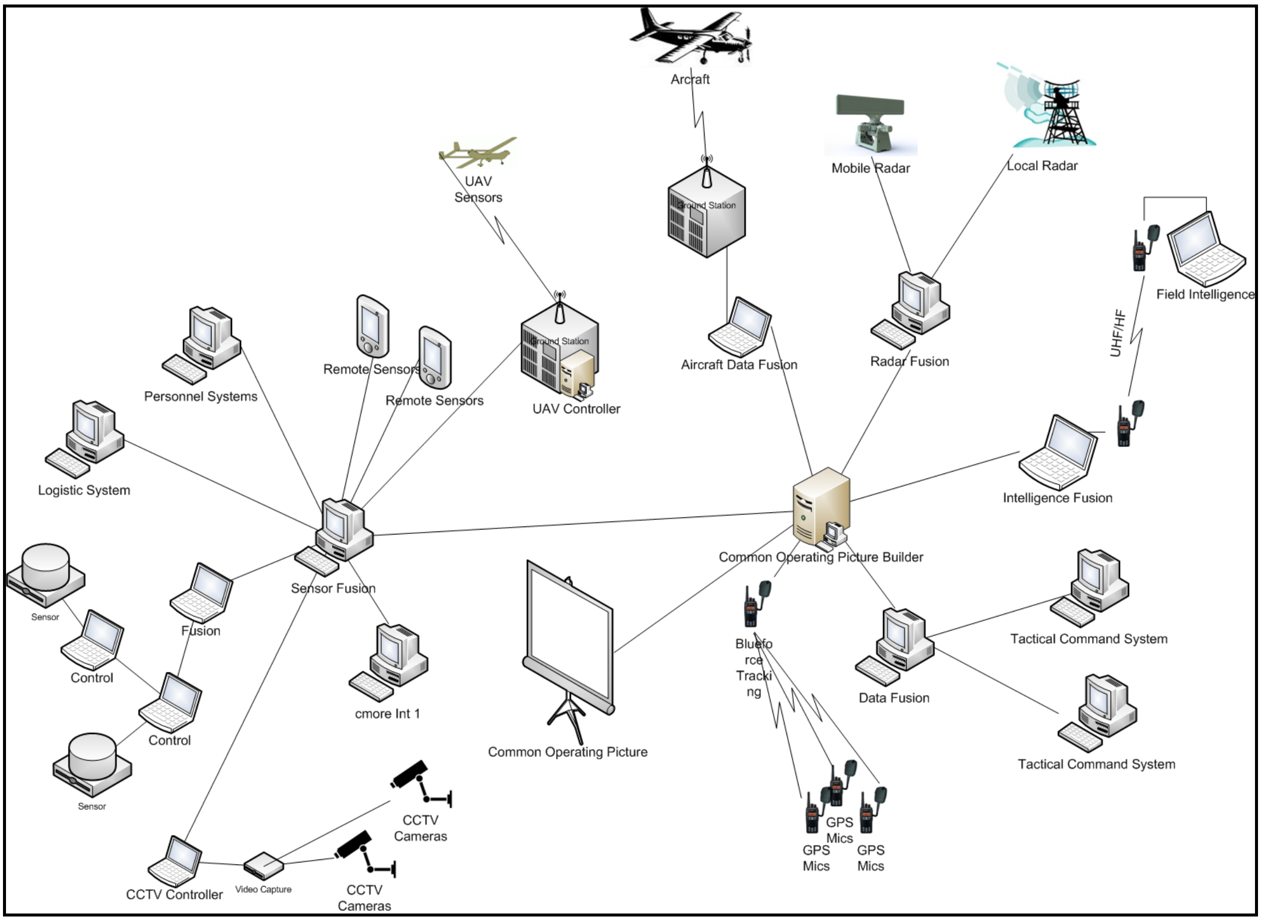


Figure 2. Information sources

A COP facilitates collaborative planning and assists all echelons to achieve SA. A COP can be tailored to a specific commander's interest in what level of detail he regards as important to the operation, based on common data and information shared by more than one command. The availability of a COP facilitates mission command by allowing all participants to see the overall operation and their contributions to it as the operation progresses. The COP incorporates as much information from running estimates as possible [5]. Figure 3 shows an example of a COP. This example was taken from Cmore System developed by the CSIR [6]. In this example the main view is a map display with a satellite image overlay. It shows the location of several resources, targets and blue forces. The left pane is a list of available information resources. These information resources can be viewed or enabled as overlays on the map display. The right pane is used for team communication purposes, similar to instant messaging and for logging of incidents. The top pane is media related to incidents.

Should the COP be inaccurate or incomplete, the commander's confidence in the COP may waiver. This then will have a detrimental effect on the commander's SA. The commander may then not completely focus on the C2 of the operation, since he may be focusing on which part of the COP may be trusted and which may not be trusted.

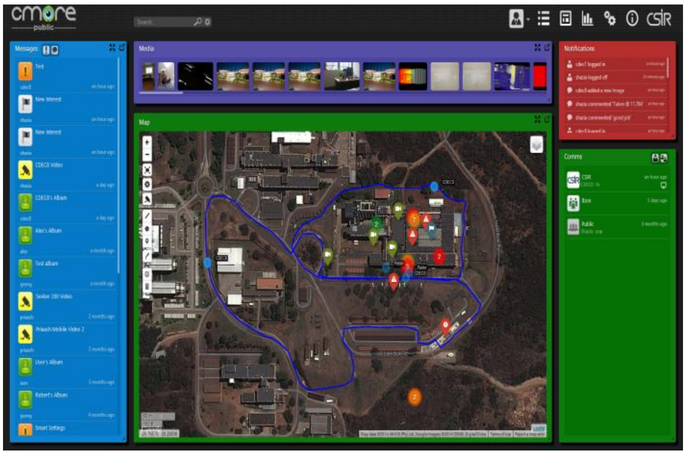


Figure 3. Example COP

SA can be regarded as "… the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future"[7]. According to Endsley [8], it can be defined in three levels.

- Level 1 is the perception of the critical factors in the environment.
- Level 2 is the understanding of those factors and how they relate to the goals to be achieved.
- Level 3 is the understanding of what will happen in the near future.

All three levels of SA are required for a commander to make adequate decisions regarding an operation.

III. Integrity of a COP

For a COP to be considered as having integrity and being qualified, there needs to be a level of consistency in terms of the values, methods and measures used within the COP.

For example, during an operation information from various systems, including blue force tracking, geographic information system, etc., are collated to form a single COP. One of the source systems may be a system that provides aircraft positions and flight paths. Should the link to that system go down, the COP display will be affected, and thus will have an impact on the commander‘s view of the current operation.

- If the COP continues to display the last available aircraft positions and flight paths, the picture will no longer be accurate, yet the commander will know that there are aircraft that may impact the operation. If the commander did not realize that the system link is down, he may continue to trust the displayed COP as real time information.
- If the COP removes the last available aircraft positions and flight paths from the display, the picture will also no longer be accurate since there would be no aircraft or flight path indicators. In this case, the commander may not be sure whether there are actually no aircraft flying through the area of interest or no aircraft displayed in the COP because the link is down.

Some of the questions that the commander may face are:

- Is the link down because it has been sabotaged, interfered with, or because of a benign failure?
- If the link was sabotaged, which enemy force is responsible and why?
- If the link comes back up should the data now be trusted?
- Will the commander be informed that that link is down?

In this example, the commander might now start focusing on the broken link rather than focusing on the operation at hand. Regardless of the physical impact that the link may have on the operation, the commander may become pre-occupied with the fact that the COP display is not accurate. The commander's concern over the status of the link and the reason for it being down might distract him from his immediate task. His attention is then not where it should be, and this does not make for good C2.

Information sources have measures of precision, quality and usability[9] but this is not a fine enough measure to qualify the integrity of a COP. To address the problem, the next section will look at the information security principles that can assist in qualifying the integrity of the COP display.

IV. Information Security Principles

Since the presentation of a COP is largely reliant on technology to transmit the original information from remote locations and to merge the collated information into a single display, it is crucial to secure these information telecommunications technology (ICT) links.

There are five principles that guide information security. These principles will be introduced briefly before being applied to determine the integrity of a COP.

The five information security five principles are:

1. **Confidentiality**: Confidentiality pertains to having the trust of someone with regard to private matters [10]. Only the intended people have access to the information. The information should only be accessible, retrievable or otherwise consumable by the parties that are privy to the information. This is typically achieved by encryption and access control.

2. **Integrity**: Integrity pertains to the state of being whole and correct [10]. Securing the data should not mean that the data is altered, degraded or destroyed. The data that was transmitted or stored is equal to the data that was received or retrieved. This is typically achieved by error correction and checksums.

3. **Availability**: Availability pertains to the suitability or readiness for use [10]. In essence, the data is available when needed. If the data is secured, it should not be unavailable due to the system securing the data not being accessible or responsive etc. This means the system securing the data should have complete availability.

4. **Authenticity**: Authenticity pertains to the quality of being genuine [10]. The origin of the information is clearly known and trusted. The data should not have been altered or changed by anyone other than the authorized parties. The authorized parties will be indisputably identifiable. The user shall be able to absolutely trust that the other parties are who they claim to be. This is typically achieved with encryption and private public key infrastructure.

5. **Non-repudiation**: Non-repudiation pertains to state of non-refusal [10]. It is trusted that the information comes from the source it is reported and that the source cannot deny the information. This is achieved with signing the data by use of a digital certificate.

These 5 principles are considered best practices and should as a matter of course be applied on the ICT links providing the data for the SA system. Taking these principles into consideration, the integrity of the COP can be evaluated based on them.

V. Evaluating the Integrity of the COP

The SA system responsible for building the COP should be able to apply the information security principles (refer to Section IV) to not only the ICT links but the information sources as well. If the compliance to the principles can be measured and quantified, combined with measures of precision, quality and usability, these can be used to calculate an integrity value for the COP.

1. **Confidentiality**: The commander should be able to trust that other parties (read opposing forces) which should not be privy to the information of the operation, does not have access to the information. This can be measured in what manner the information was received. Was it received over unsecure public networking infrastructure? Private encrypted networks? Via word of mouth? Through intelligence agencies? Putting values towards these as a measure of their relative confidentiality will allow them to be used in the calculation of the integrity.
2. **Integrity**: Integrity of the information source refers to how intact or complete the information is. If information was transmitted via voice over a HF link, that degraded, the integrity can be regarded as low. If the information was received via a digital medium that included error checking, the integrity is higher. The source of the information is also a consideration. The commander must have confidence that the information that makes up the COP is beyond reproach.
3. **Availability**: How reliable is the information source? If the information is received over a wireless technology that keeps failing, it will score low. If the information is received at the required rate, as and when expected, over a robust link, it will score much higher. If the information is unreliable, the commander shall be less inclined to give it undue attention and will focus more on the reliable information.
4. **Authenticity**: Can the information sources be trusted? If the air picture that makes up part of the COP is received from a qualified system, built by an qualified operator and received over a secure, robust digital link it will score high. However if the air picture is determined by experimental systems, new technology or unknown sources, it will score low. The commander needs to know that the information he receives is authentic, or at least to what degree it can be determined to be authentic.
5. **Non-repudiation**: Non-repudiation seems like the odd one out. But it can have real implications, especially in life or death situations. The commander needs to know that the decisions he is making is based on real substantiated information. To this affect he needs to know that the information source will stand by that information and that they used due diligence in preparing it. For example, should the commander be given the target coordinates for an airstrike with the assurance there are no friendly forces in the strike zone. He must have the confidence that if he gives the go ahead for the strike, that the information sources will not and can not deny that they supplied the information.

Evaluating the integrity of the COP can be done by implementing a weighted system, which can give different weights to the different principles for every source, depending on the source's relative importance or impact on the operation.

Different types of operations place varying importance on different information sources. For instance, in a land based operation that does not include any aircraft as part of the operation, not too much value needs to be placed on the air picture. An air picture might not even be used. An operation that includes aircraft will put a lot of importance on the air picture, not only to ensure the safety of the airspace, but also to have an understanding of what is happening in the airspace. Thus the weight assigned to the air picture source will differ between these operations and will consequently have a different impact on the integrity of the COP. Should the air picture during the land based operation be unreliable or inconsistent, it will have minimal impact on the integrity of the COP. But during an air based operation, the integrity of the air picture will have tremendous impact on the integrity of the COP.

A measure of granularity can then be applied, based on a weighted system to measure the information against these principles. Thereafter, the COP can be rated to quantitatively determine the integrity of the COP. A commander can then use this measure to determine his trust level of the COP. Presenting the commander with a value of the integrity of the COP, gives him the opportunity to decide if he wants to trust the COP or not. An experienced commander can then set this value as his preferred minimum value for the operation at hand. Information sources that do not meet this minimum value can be discarded from the COP, ensuring the integrity of the COP is not compromised.

At the end of the paper are examples of tables that can be used for such calculations. Keep in mind that these values are for illustrative purposes and not based on any real data. In addition the information sources are higher level order. These can be broken down even further into their own sources and calculations applied to those sources. The first table (TABLE I. is an example of a normalised weighting table. The weightings can be used to indicate the relative importance of the various information sources. The weighting is based on a value between 0 and 1. It indicates the relative importance of the measured principal of that information source to the current operation, 0 meaning not important at all and 1 meaning it is of extreme importance. In this example then, to that operation, the air picture's integrity is of utmost importance and is weighted at a normalised value of 0.13. The precision of the intelligence sources is not of that much concern and is therefore only weighted at 0.08. TABLE II. is the score of the information sources as it relates to the five principles and the information quality measurements. The scores range from 1 to 10 where 1 is poor and 10 is excellent. From the example it can be seen that the air picture information's integrity was scored at 10, meaning the integrity was excellent. This is good since the weighting given to it is 0.13. The information received from the intelligence sources was spot on with a precision score of 10, but the precision was not of that great importance as it is only weighted at 0.08, therefore it will not contribute much to the final integrity measure. TABLE III. is an example of the weighting that can be applied to the different information sources based on a per operation basis. From the table it can be seen that for Operation Alpha, the air picture, blue force tracking and intelligence sources are important, but that the ground picture, maritime picture and opforce tracking is not of great importance.

By combining the measurements with the weights it is possible to put a value on the integrity of the COP. Such a formula should be the focus of scientific research, but a simplistic formula can be as simple as multiplying the weight with the measurement score and adding all the values. So to calculate the measure of integrity for Operation Alpha, given the values in the tables, would appear as in TABLE IV. Multiplying the weighted scores with the weights for Operation Alpha gives the weighted measures. Adding up the weighted measures gives us a integrity value out of 10. In this example it is 8.18. These values are not an indication of what the values should be, but merely an example for illustration only.

Presenting an actual weighting system is beyond the scope of the paper. It requires in depth research as to what information is critical for which type of operations and how the five principles relate to those information sources. Not to mention what every commander believes they require to successfully command a operation. A set of experiments will have to be defined to test and evaluate the commanders performance with and integrity measure and without a integrity measure. Designing such experiments are undertaking in and of themselves as the same experimental operation can't be used twice since the commander will know the outcome. Experiment will most likely have to rely on participant feedback to determine if the integrity measure provided value.

VI. Impact of Required Integrity Measure on Situational Awareness

If a quantitative measure of integrity can be applied to the COP, it can also be used to discard information if it does not meet the required level. Thus the COP can have a Required Integrity Measure (RIM). For example, if certain information sources fall below a certain value of integrity, the information sources can be omitted from the COP. This will increase the integrity of the COP since the displayed information is qualified and not adversely affected by the omitted data. With this weighting system in place, a commander can therefore always trust in the integrity of the COP, even if data is omitted.

The RIM could be predetermined and standardized by the commander based on specific inputs and rated weighting of these inputs, or predefined dependent on the operation (for instance, in an air operation the air picture will be of critical importance, whilst it may only serve as anecdotal information in a land based operation with no air component). Furthermore, a commander (or the builder of the COP) could also choose to change the RIM in real time, as certain changes in the SA necessitates. For example, depending on the commander's risk assessment he could increase the RIM, causing information not meeting this requirement to be discarded from the COP. Or alternatively the RIM could be lowered, showing more information, with the associated risk that the extra information could be of questionable integrity. This concept is not new in the military as it is similar to the Constant False Alarm Rate (CFAR) used by radar operators.

CFAR detection refers to a common form of adaptive algorithm used in radar systems to detect target returns against a background of noise, clutter and interference [11]. It allows the radar operator to lower the CFAR, this will clear up the radar picture and show only definite targets. However, smaller or targets further away, will be discarded as they would be indistinguishable from noise. Increasing the CFAR will show a lot more targets, but it could be that these are not in fact real targets, but noise, signals bouncing of clutter, waves at sea etc. Choosing the correct CFAR is thus a fine line.

The false alarm probability depends on the noise variance. Therefore, to calculate the false alarm probability, the noise variance must be estimated. If the noise variance changes, the threshold must be adjusted to maintain a constant false alarm rate [12]. Therefore, as the integrity of the information feeds changes (analogous the noise variance), the commander may choose to adjust the RIM of the COP to maintain the best possible COP for the operation.

VII. CALCULATING THE REQUIRED INTEGRITY MEASURE

As with the weighting system discussed in section V, determining the RIM falls outside the scope of this paper. It is however an interesting topic for future research. Although the previous section described how a commander might change the RIM based on his needs, there should still be some guidance.

Not all commanders will have the experience to know under what circumstance and in what operations a good RIM would be. To the uninitiated it might end up being a useless sliding value that's only purpose seems to change how much information is displayed on the COP. With research and case studies it should be possible to capture the knowledge of experienced commanders. Determining indicative RIM values and making it part of the training of future commanders will help ensure that they are more effective commanders sooner.

VIII. CONCLUSION

Commanders tend to completely disregard the contributions of a COP if there is any discrepancy in the data, or they find a reason not to trust the COP. This research has shown that by assigning a measure of integrity to the COP, a commander can use a COP for SA, even if the picture is less than perfect. By giving the COP a qualified integrity measure, the commander can use the COP in his risk assessment, instead of disregarding the whole picture.

To calculate the measure of integrity it is necessary to measure the information sources used to build the COP. By applying the five principles to the information sources, their integrity can be determined. This, in turn, contributes to the calculation of the integrity of the COP.

Once the integrity of a COP can be measured, a required value can be set, the Required Integrity Measure. Setting the RIM allows a commander to determine the integrity that needs to be met by the information sources, disregarding the data that does not.

It is believed that this paper describes a new concept to be applied to a common operating picture as it is used for situational awareness in command and control. The concept remains theoretical and as such there further research required to determine the information lacking in this paper. Further research should include the possibility of applying the five principles to the various information sources, determine the impact an integrity measure will have on a commander's ability and what would constitute the weighting system.

TABLE I. EXAMPLE OF A RELATIVE IMPORTANCE WEIGHTING TABLE

	Confidentiality	**Integrity**	**Availability**	**Authenticity**	**Non Repudiation**	**Precision**	**Quality**	**Usability**
Air Picture	0.09	0.13	0.13	0.13	0.13	0.13	0.13	0.13
Ground Picture	0.14	0.15	0.12	0.15	0.08	0.12	0.12	0.12
Maritime Picture	0.13	0.19	0.1	0.19	0.08	0.1	0.12	0.09
Blueforce Tracking	0.18	0.17	0.08	0.12	0.08	0.17	0.08	0.12
Opforce Tracking	0.07	0.17	0.07	0.10	0.17	0.24	0.10	0.08
Intelligence	0.11	0.11	0.13	0.15	0.18	0.08	0.16	0.08

TABLE II. EXAMPLE OF MEASSUREMENT SCORES

	Confidentiality	**Integrity**	**Availability**	**Authenticity**	**Non Repudiation**	**Precision**	**Quality**	**Usability**
Air Picture	10	10	10	10	10	8	10	8
Ground Picture	10	8	10	10	10	5	6	8
Maritime Picture	10	10	10	10	10	10	10	10
Blueforce Tracking	6	10	7	9	10	10	10	10
Opforce Tracking	3	4	1	9	3	6	3	4

Intelligence	10	4	4	5	1	10	10	10

TABLE III. EXAMPLE OF RELTAVIE IMPORTANCE PER OPERATION

	Operation Alpha	**Operation Bravo**	**Operation Tango**	**Operation Shield**
Air Picture	0.33	0.04	0.19	0.17
Ground Picture	0.03	0.35	0.12	0.17
Maritime Picture	0.00	0.00	0.23	0.17
Blueforce Tracking	0.33	0.28	0.00	0.17
Opforce Tracking	0.00	0.18	0.23	0.17
Intelligence	0.30	0.16	0.23	0.17

TABLE IV. EXAMPLE CALCULATION

	Weighted Score	**Operation Weighting**	**Measurement**
Air Picture	9.48	0.33	3.13
Ground Picture	8.38	0.03	0.25
Maritime Picture	10	0.00	0.00
Blueforce Tracking	8.92	0.33	2.94
Opforce Tracking	4.43	0.00	0.00
Inteligence	6.19	0.30	1.86

REFERENCES

[1] DOD Dictionary of Military and Associated Terms, Available from: http://www.dtic.mil/doctrine/dod_dictionary/ (Accessed 7 April 2014)

[2] Brynielsson, J; Artman, H; Wallenius, K.; Arnborg, S. Information awareness in command and control: precision, quality, utility. Institute of Technology, Stockholm, 2000.

[3] Boyd, J R. The Essence of Winning and Losing, 28 June 1995 a five slide set by Boyd. Available from: http://www.danford.net/boyd/essence.htm (Accessed 7 April 2014).

[4] Brehmer, B. Command and control as design. 15th ICCRTS “The Evolution of C2”, Santa Monica, California, 2010.

[5] United States Army Combined Arms Center. 2008. Common Operational Picture. Available from: http://usacac.army.mil/cac2/call/thesaurus/toc.asp?id=8113 (Accessed 2 April 2014).

[6] Terlunen A., Botha P., Ramadeen P. & Vawda S. Facilitating Collaboration in an Integrated Command and Control Environment, MICSA, 2014.

[7] Endsley, M. R. Design and evaluation for situation awareness enhancement. Proceedings of the Human Factors and Ergonomics Society Annual Meeting October 1988 vol. 32 no. 2, Santa Monica, CA, 1988.

[8] Endsley, M. R; Bolt B. and Jones D. G, Designing for Situation Awareness: An Approach to User-Centered Design, CRC Press, Taylor & Francis Group, 2003.

[9] Ivanov, K. "Quality-control of information: On the concept of accuracy of information in data banks and in management information systems", 1972. Available from: http://www.informatik.umu.se/~kivanov/diss-avh.html (Accessed 7 April 2014).

[10] Wang, C; Wulf, W, A. Towards a Framework for Security Measurement. 20th NISSC Proceedings October 1997. Available from: http://csrc.nist.gov/nissc/1997/proceedings/522.pdf (Accessed 6 July 2014).

[11] Scharf, LL. Statistical Signal Processing: Detection, Estimation, and Time Series Analysis. Addison Wesley, NY,1991.

[12] MathWorks. 2014. Constant False-Alarm Rate (CFAR) Detectors. Available from: http://www.mathworks.com/help/phased/ug/constant-false-alarm-rate-cfar-detectors.html (Accessed 2 April 2014).

[13] Bau, N., Gerz, M. & Glauer, M. 2008. Ensuring Interoperability of Command and Control Information Systems – New Ways to Test Conformance to the MIP Solution. Journal of Telecommunications and Information Technology. Volume 2. P 5 – 13.