Peacekeeping: The Relationship Between Information Systems & Peacekeeper Security

Benjamin Wright

2020 Laurea

Laurea University of Applied Sciences

Peacekeeping: The Relationship Between Information Systems & Peacekeeper Security

Benjamin Wright
Security Management
Bachelor’s Thesis
June

Laurea University of Applied Sciences **Abstract**
Bachelor of Business Administration, degree program of
Security Management

The Relationship Between Information Systems and Peacekeeper Security

Year 2020 Pages 739

Currently, while there is much research and literature dedicated to the topics of peacekeeping security and information systems, there is almost no research or literature that discusses the relationship between the two. The aim of this thesis is to clarify and elucidate information surrounding the scarcely researched topic of information systems in the context of peacekeeping. In elucidating this information, this paper can serve as a research tool, contributing towards the development of education of this topic, for example, in universities and academies. In doing so, this paper aims to help students who may enter the fields of Information Security, Information Systems or Peacekeeping. So that they can better contribute towards a future that ensures the best people are employed to develop and operate these information systems.

The purpose of this thesis, therefore, is to obtain and amalgamate findings from the research and literature surrounding the topics of information systems and peacekeeping organizations. Primarily, the United Nations (UN), North Atlantic Treaty Organization (NATO), and the British Army. The sub-topic of information security, and the importance it plays between peacekeeper security and information systems, will be used to contribute to the analysis of the relationship between information systems and peacekeeper security.

To achieve this aim, the primary objective of this thesis, is to analyze the topics of peacekeeping, peacekeeper security, information systems and information security, followed by three real information systems, currently used in UN, NATO and British Army peacekeeping operations. The systems are Deployable Communication Information Systems (DCIS) type information systems, namely the UN Modular Command Centre (UN MCC), NATO DCIS, BAE FALCON. In analyzing these systems, the relationship between each system and peacekeeper security will be shown. More specifically, it will be determined which system aspects contribute towards peacekeeper security, and how it is achieved in the context of peacekeeping threats. And therefore, the information system requirements, too.

Keywords: Information System, Information Security, Peacekeeping, Command & Control, Situational Awareness, Interoperability.

Table of Contents

List of Abbreviations

C2	Command & Control
CAVNET	Communications Against Violence Network
CIA	Confidentiality, Integrity, Availability
CS	Central Service
DCIS	Deployable Communications Information System
EW	Electronic Warfare
HQ	Headquarters
HVAC	Heating, Ventilation and Airconditioning
IED	Improvised Explosive Device
IP	Internet Protocol
LAN	Local Area Network
MINURSO	United Nations Mission for the Referendum in West Sahara
MINUSCA	United Nations Multidimensional Integrated Stabilization Mission in the Central African Republic
MONUSCO	The United Nations Organization Stabilization Mission in the Democratic Republic of the Congo
NATO	North Atlantic Treaty Organization
NEC	Network Enabled Capability
NGO	Non-Government Organization
OODA	Observe, Orient, Decide, Act
SATCOM	Satellite Communications
SCS	Supply Chain Service

SGITT	Service for Geospatial, Information and Telecommunications Technologies
UAV	Unmanned Air Vehicle
UN	United Nations
UN MCC	United Nations Modular Command Centre
UNFICYP	United Nations Peacekeeping Force in Cyprus
UNGSC	United Nations Global Service Centre
UNITAR	United Nations Institute of Training and Research
UNOSAT	United Nations Operational Satellite Applications Programme
WAN	Wide Area Network
WASP	Wide Area Service Provision
UNFICYP	The United Nations Peacekeeping Force in Cyprus
SFOR	Stabilisation Force in Bosnia and Herzegovina
IFOR	Implementation Force in Bosnia and Herzegovina

1 Introduction

This paper comprises six chapters: ‘Introduction’, ‘Peacekeeping’, ‘Information Security’, ‘Information Systems’, ‘Deployable Communication Information System Analysis’ and ‘Conclusions’. In the first chapter, the aim and purpose of peacekeeping, its history, and its modern environment today, will be discussed, including threats and operational types, which will later be linked to the research question of this thesis: ‘what is the relationship between information systems and peacekeeper security?’ In the second chapter, will be introduced the information security threats present in the modern peacekeeping environment, leading on to why information security protective measures must be used by peacekeeping organizations. Chapter 3 will introduce the information system functions, as well as two key concepts which will be used as a theoretical framework to determine the purpose of an information system in the context of peacekeeping operations – Lawson’s Model of Command & Control, and the OODA Loop. Elements of the concepts will be referenced to and their importance in peacekeeper security will be made more apparent in the next, and second focus chapter of this thesis, ‘Deployable Communication Information System Analysis’.

The different types of peacekeeping mission and the methods used to conduct them vary greatly, and each will be discussed. Peacekeeping threats, information system fundamentals, the role they play during peacekeeping operations, and their relationship with peacekeeper security will also be discussed. ‘Peacekeeper security’, will be defined as a state in which peacekeepers are protected and kept safe from threats which may cause them harm or put their lives in danger. The concepts of situational awareness and operational intelligence and the relationships they have between information systems and peacekeeper security will also be discussed to determine how situational awareness is critical to ensuring peacekeeper security.

After determining the roles information systems play in peacekeeping operations and how they are used to provide security to peacekeepers during operations, a relationship between information systems and a different type of security, directly related to the security of the information systems themselves, will be discussed – information security. In this discussion, it will be introduced how information security is connected to the continuity of the overall functionality of an information system, and therefore how information security is also crucial to peacekeeper security. After the discussions of peacekeeping, information systems, information security and the relationships they have with one another, the concept of Deployable Communications Information Systems (DCIS) will be introduced. Followed by an analysis of three real DCIS systems currently in use in peacekeeping operations. DCISs are a type of information system with the core purpose of communication. Of which, information (data) continually flows between an operational environment and other system users, through the DCIS.

While each of these three topics and their relationships with each other are important, it must be noted that the focus of this paper is the relationship between information systems used by peacekeeping organizations and peacekeeper security. In chapter four, ‘Command & Control Concepts’, two key concepts about communication and transmission of information between an operational environment, an organization ’s forces, and other parts of an organization will be discussed, namely Lawson’s Model of Command & Control and The OODA Loop.

1.1 Research Questions

The research questions are as follows:

- How do information systems used in peacekeeping operations contribute to peacekeeper security?
- How does information security, information Confidentiality Integrity Availability (CIA), and its relationship with information systems affect peacekeeper security?

1.2 Literature Review

There has been much work and literature related to the independent fields of peacekeeping, peacekeeper security, situational awareness, information systems and information security, which form the framework of this paper in answering the main research question: ‘what is the relationship between information systems and peacekeeper security?’ However, there is little literature that assess these different field collectively, or the relationships they have with one another. Or, they present a different viewpoint which this paper challenges. For example, Culture and Interoperability in Integrated Missions (2008), presents the viewpoint that interoperability in missions is achieved almost exclusively through the human component, specifically cultural understanding, and effective interactions between different parties. In this paper, however, that viewpoint is challenged, in addressing the technical aspect of interoperability. Which is that information systems need to be connected with one another and organizations need to have common information sharing platforms. While this paper and the literature disagree on the method of interoperability, the outcome, however, as with other literature is agreed upon in that it strengthens cooperation between parties to accomplish operational goals. And, in doing so, matching the context of this paper, enhances peacekeeper security.

1.2.1 Peacekeeping Literature

While both the UN and NATO can be considered peacekeeping organizations (though NATO conducts other activities too (including crisis management and civil emergency missions) who both conduct peacekeeping operations, the United Nations (UN) is the world’s leading peacekeeping organization, both in terms of scale and operational history. For example, in reflecting the UN’s scale, they “keep peace with 102,482 peacekeepers in 14 operations around the world” (the UN has 13 global peacekeeping operations as of 2020), as well as assisting and protecting “71.4 million people fleeing famine, war, and persecution” as listed on the regularly updated UN Card which highlights ten quantifiable actions of the UN in their global work. Regarding operational history, the UN has conducted peacekeeping operations since the early nineties in the Balkans alongside NATO. And they continue to conduct joint operations around the globe working with nations around the world who attach their solders from their Armed Forces as part of a joint force in UN peacekeeping operations, as is the case in with the UN's current 13 operations, as visible on their website. These are the key reasons why the UN is regarded as the world's leading peacekeeping organization. Therefore, throughout this thesis, the UN will be used as the backbone of this paper in terms of referencing, definitions, and operational examples.

Historical literature and electronic publications have been used to obtain qualitative data in providing a brief history of modern UN and NATO peacekeeping operations. With the first globally recognized peacekeeping operations beginning in the Balkans during the early nineties, the Balkans became "Europe's security policy testing ground" (1999, 7), as former U.S. Secretary General Javier Solana said in the NATO Review, 'NATO Steps Boldly into the 21st Century'. Beginning in Croatia in 1992 with the deployment of the United Nations Protection Force (UNPROFOR), followed by supporting NATO's 'Operation Maritime Monitor' (16 July to 22 November 1992). Information relating to Balkans peacekeeping has been obtained from the mission profile of UNPROFOR on the 'Past Operations' section of the UN official website, as well as the 'Terminated Missions' section of the official NATO website.

Regarding current UN operations, such as the United Nations Mission for the Referendum in Western Sahara (MINURSO) and the United Nations Peacekeeping Force in Cyprus (UNFICYP) the data and references used in this thesis, has been collected largely from the current operations section of the UN official website. The United Kingdom is an example of a UN member nation who attaches members of its Armed Forces to UN forces in peacekeeping operations and will be referred to throughout this thesis. As of 2020, the UK is ranked the 47th biggest troop contributor, with "279" troops currently contributed to UN peacekeeping operations, as according to official statistics on the 'Troop and Police Contributions' section of their website.

Figure 1 below, demonstrates the top troop contributions from UN member countries including the United Kingdom, for one of the UNs biggest current operations, the United Nations Mission for the Referendum in Western Sahara (MINURSO). While Figure 2 shows the top troop contributors of the United Nations Peacekeeping Force in Cyprus (UNFICYP), the latter of which primarily involves United Kingdom troops from the British Army, exemplify the wide array of nationalities that send attachment forces to UN peacekeeping missions.

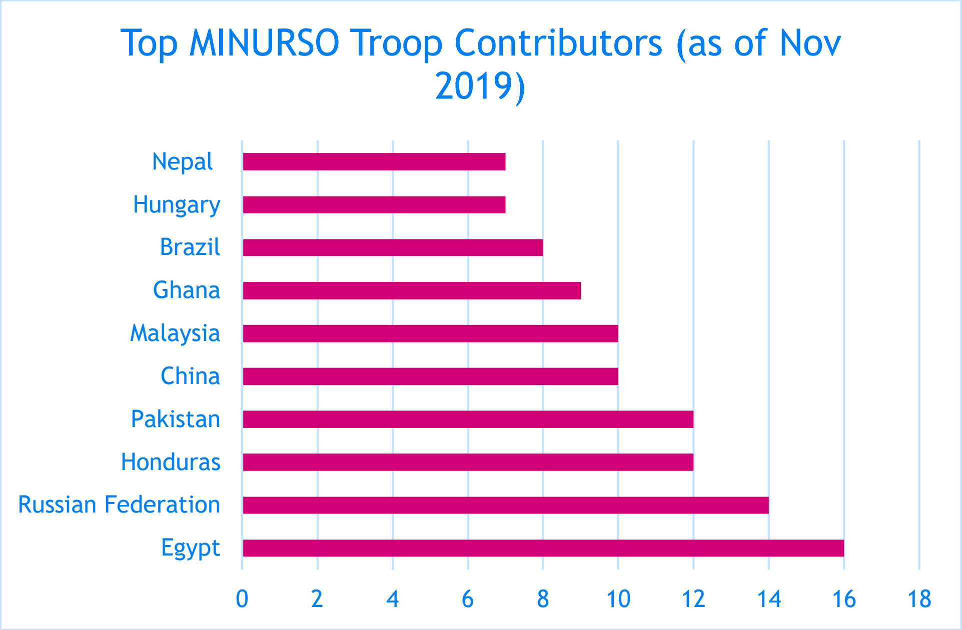


Figure 1: Top MINURSO Troop Contributors (United Nations 2019)

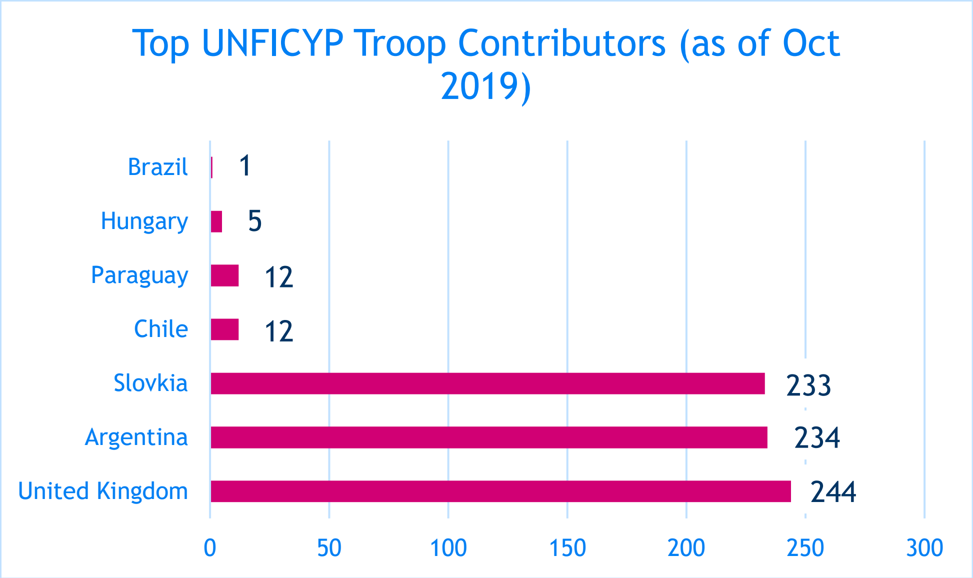


Figure 2: Top UNFICYP Troop Contributors (United Nations 2019)

Regarding the interoperability aspect of information systems used by the UN and NATO, both internally and externally, including with armed forces of other UN member nations like the British Army, it is crucial to operational success. So, literature from various printed and electronic publications has been used to collect data and references. The United Kingdom, as one of the original and founding UN members since 1945, alongside 50 other founding members, such as the Republic of China, United States of America, and the Unions of Soviet Socialist Republics, as according to the official ‘Growth in United Nations Membership, 1945-Present’ section of their website.

And the United Kingdom's Armed Forces, as one of the world's most technologically advanced and powerful militaries, will be used in tandem with one of their biggest information systems - the BAE FALCON, to demonstrate the importance of interoperable information systems in peacekeeping. Interoperability is a key concept which will be discussed later in this thesis. The United Nations Modular Command Centre (UN MCC), and the NATO Deployable Communication and Information System (DCIS), will also be used to prove the importance of interoperability in peacekeeping, as well as in answering the research questions of this paper. The importance of interoperability will be demonstrated by analyzing the different capabilities of these information systems and it will be determined what each system offers in contributing towards peacekeeper security during operations.

It is not only what the differing capabilities of different information systems can offer to operations, however. It is also the ability to communicate between different forces which is crucial for situational awareness and peacekeeper security, which is where the biggest significance in the concept of interoperability will be found and discussed in this paper. The significance of interoperability will contribute towards answering the research question 'what is the relationship between information systems used by peacekeeping organizations and peacekeeper security?

1.2.2 Research Gaps in Literature This Paper Expands On

To understand why the literature that has been chosen to research the fields and concepts in this paper, and what research gaps in literature this paper expands on, the definitions of these fields and concepts must first be understood. The fields of which this paper discusses and refers to literature of, have quite universal definitions. The exception, however, is the core topic of Information Systems. Because the term 'Information System' is a very broad term because Information Systems are used in various forms, for different purposes, in almost every industry and profession. Therefore, there is no universal definition, and it is harder to pinpoint the appropriate literature to reference to in this thesis. Furthermore, there is no literature niche for Information Systems used in Peacekeeping.

To avert any problems this research gap in literature could cause, only general literature relating to the basics of Information Systems, answering fundamental questions like 'what is an information system?', 'what is the purpose of an information system' and 'how does an information system work?', have been used as the literature foundation of this thesis. Some of the specific literature of which will be mentioned, shortly. The information and key concepts of Information Systems, obtained from this literature, will be applied and used in the context of Peacekeeping and the environments in which peacekeeping organizations operate, in tandem with Peacekeeping literature and literature related to the specific Information Systems which will be analyzed in this paper. This is how this paper will expand on the research gap in literature relating to the Information Systems in the context of Peacekeeping. Rather than using literature that addresses Information Systems in a specific context, largely the field of Business. Such as: Business Driven Information Systems (2006), Essentials of Business Information Systems (1994), Business Information Systems (1999).

There is much work and literature dedicated and related to the fields of Peacekeeping, Information Systems, and Information Security, independently, the primary fields comprising the content of this paper. Acclaimed publications in these fields which have been used to research these fields for this paper include: The Oxford Handbook of United Nations Peacekeeping Operations (Koops, J., MacQueen, N., Tardy, T., Williams, P. 2015), 'Does Peacekeeping Work?' (Fortna, P. 2008), Principles of Information Systems (Stair, R., Reynolds, G. 2012), Fundamentals of Information Systems (Stair, R., Reynolds, G. 2012) Information Systems for Business and Beyond (Bourgeois, D.T. 2014), and Computer and Information Security Handbook (Vacca, J.R. 2009). The two key concepts that will be discussed significantly throughout this paper in relation to these fields, as two of the main arguments of how information systems contribute towards peacekeeper security, are Interoperability, and Command & Control (C2). There is also much literature surrounding these two concepts, including: Information Systems Interoperability (Krämer, B., Papazoglou, M., Schmidt, H.1998), Intelligent Integration of Information (Wiederhold, G. 1996) Command Concepts (Builder, C.H., Bankes, S.C, Nordin, R. 1999), and Modelling Command and Control (Baber, C., Harris, D., Stanton, N. 2008).

However, while there is a substantial amount of literature surrounding these fields and concepts independently, there is little literature that addresses the relationship between these fields, of which the main research question of this thesis is based. There is some literature addressing the relationship between two or more of these fields and concepts, for example, Information Systems Interoperability (1998) addresses the field of Information Systems and the concept of Interoperability, as does Intelligent Integration of Information (1996). But there seems to be no literature which amalgamate each of these fields and concepts into a single piece of literature. This paper achieves the amalgamation of these fields and concepts and addresses the relationships between them as the framework of this thesis. Thus, addressing the overall relationship between information systems and peacekeeper security and answer the research question 'what is the relationship between Information Systems and Peacekeeper Security?'. This is the research gap in literature this paper expands on.

1.2.3 Terminology and Concepts Definitions

- **CIA Triad:** The CIA Triad, as visible by Figure 3 below from F5 Labs Application Threat Intelligence, a cyber security educational website, encompasses three core components: Confidentiality, Integrity, and Availability (CIA). These three components, when protected by information security measures such as information security controls, ensure data is protected. The CIA triad will be used extensively in this thesis to discuss the reasons why security controls of information systems are in place to protect the data that is managed by information systems during peacekeeping operations, which in turn protects peacekeeper security. Security controls that ensure the Confidentiality, Integrity and Availability of information will be discussed particularly in Chapter 5, Deployable Communications Information System Analysis.

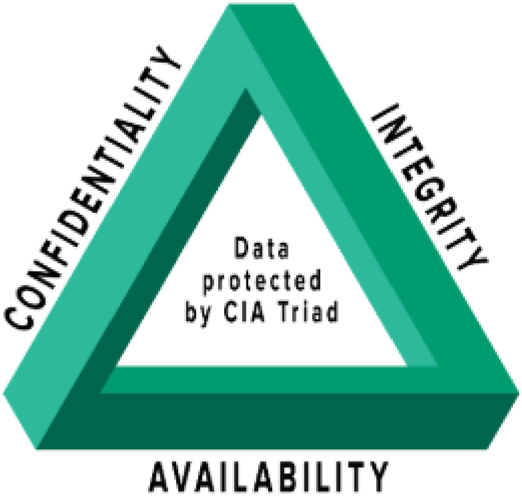


Figure 3: Confidentiality, Integrity, Availability Triad (Walkowski, 2019)

- **Command & Control (C2):** As defined in C2 Re-envisioned: The Future of the Enterprise (Alberts, Agre, Vassiliou, 2014), C2 is “the set of organizational and technical attributes and processes by which an enterprise marshals and employs human, physical, and information resources to solve problems and accomplish missions” C2 will be used in this paper as a key attribute of which peacekeeper security and the key information resource that will be discussed in unison with C2, is situational awareness, to enhance it. In this paper, C2 will encompass the human aspects, primarily focused on how commanders in the command and control elements of an information system enact decisions, as well as the physical and technical aspects by which information can be shared and received. Using C2 as a means of issuing orders and making decisions is the key C2 method in this paper of contribution to peacekeeper security. Cruz, Cusimano, and Phillips explain the importance of C2 to protect the security of peacekeepers in the United Nations report, ‘Improving Security of United Nations Peacekeepers’ (2017). Saying that “the quality of leadership at the sector level, battalion level and below is essential to the maintenance of security of peacekeepers” because it is at the C2 level of peacekeeping organizations, that “the majority of operations are planned and executed” (2017, 19).

- **Deployable Communications Information System:** An information system which can be deployed in any environment which a peacekeeping organization is likely to operate, which can operate with a command and control function, and can provide situational awareness. Deployable Communication Information Systems (DCIS) will be analyzed in Chapter 5 of this paper to provide real examples of the determined aspects of information systems that contribute to peacekeeper security, as well as of information security controls. The United Nations Modular Command Centre (UN MCC), North Atlantic Treaty Organization Deployable Communication & Information System (NATO DCIS) and BAE FALCON will be used in the analysis.

- **Interoperability:** As defined in the NATO document "Interoperability for Joint Operations" (2006), "Interoperability refers to the ability of different military organizations to conduct joint operations. These organizations can be of different nationalities or different armed services (ground, naval and air forces) or both. Interoperability allows forces, units, or systems to operate together. In this paper, while no in-depth analysis is conducted of the technical measures of information systems which allow for interoperability, the focus of interoperability in this paper will be of information systems. Specifically, the ability for organizations to share information throughout their organization, as well as with other organizations. Interoperability will be discussed from a theoretical perspective, determining the benefits and methods of interoperability in relation to peacekeeper security.

- **Peacekeeping:** activities which "provide security and the political and peacebuilding support to help countries make the transition from conflict to peace" (UN)

- **Peacekeeper Security**: In this paper, the term peacekeeper security, will be defined as a state in which peacekeepers are able to successfully conduct their operation while being situationally aware of present threats, and absent from immediate danger threats in an operational environment may cause to peacekeepers.

- **Situational Awareness**: "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" (Endsley 1988). Situational Awareness, will be the primary type of information to be analyzed and discussed in this paper as a means of providing an awareness of an operational environment and the threats it contains to stakeholders and Command & Control elements of an organization.

- **Situational Understanding:** is the product of receiving, analyzing, and interpreting situational awareness. And as defined in the paper 'How Are Situation Picture, Situation Awareness, and Situation Understanding Discussed in Recent Scholarly Literature?' (Ruoslahti, Tikanmaki, 2019) it is "how the situation is or can be formed and how the different activities affect the developing situation". Situational understanding will be primarily be discussed in this paper from the perspective of Command & Control elements as a means of enabling them to enact orders and decision which contribute towards peacekeeper security.

1.3 Methodology

To use different sources of information to increase the validity and reliability of finding in this thesis, the triangulation method of research has been used in this paper. Sources include, United Nations peacekeeping mission reports, in which graphs, statistics, and opinions have been gathered as well as implemented using the triangulation method. Additional sources include This multi-method approach for obtaining and implementing qualitative research, using qualitative research, includes, comparative research, historical research, case studies and theoretical research. The primary category of research used to answer the research questions in this thesis is primarily qualitative; focusing on the definitions and published literature surrounding the concepts that are discussed in this paper, to give an accurate, relevant and balanced discussion of the topics in this thesis as well as analysis of the three Deployable Communication Information Systems in the Deployable Communication Information System Analysis, Chapter 5.

Chapter 5 obtains the tangible findings and examples from the largely theoretical perspective that will be discussed throughout the other chapters, where the finding are obtained through conducting an analysis of the three systems through both assessing the systems individually, as well as comparing the facts and data found on the three systems to make connections between the facts and data to find out what the common themes of the systems are in answering the research questions of ‘what is the relationship between information systems and peacekeeper security?’ and ‘how do deployable information systems contribute to peacekeeper security?’. The methods of finding the data used for the findings of these questions are reviews, articles, info-graphics sheets, and educational videos.

Some quantitative research has also been used to support the primary method of research which is qualitative research. This research includes facts and dates about background and historical information surrounding peacekeeping, beginning with being included in a brief introduction to the first modern peacekeeping operations which were commenced by the UN and NATO in the Balkans during the early nineties in the “Peacekeeping” chapter, as well as statistics that support the need for the research question of this thesis, including peacekeeper casualty statistics and attack statistics on peacekeeping bases, as mentioned in the report UN report Improving Security of United Nations Peacekeepers (2017) by Cusimano, Phillips, and Lt General (Retired) Carlos Alberto dos Santos Cruz, who was Force Commander of United Nations Stabilisation Mission in Haiti (MINUSTAH) United Nations Organization Stabilization Mission in the Democratic Republic of the Congo (MONUSCO). Quantitative research has also been obtained and implemented throughout the three analyses of the United Nations Modular Command Centre, NATO Deployable Communication Information System, and the BAE FALCON in the “Deployable Communications Information Systems Analysis” chapter, in providing statistical data that that support how the technical and physical security controls of the DCIS systems, the primary contributors in answering the research question: “How do deployable communication and information systems contribute towards peacekeeper security?”.

For example, statistics have been used relating to the operating temperature regarding physical controls. This data has been collected from a variety of electronic literature sources, mainly tertiary research in the form of educational videos. In the case of the sources for the BAE FALCON analysis, documents from the BAE Systems official website have been used as the primary source of information, namely the BAE FALCON Brochure (BAE Systems 2011), Fact Sheet (BAE Systems) and Infographic (BAE Systems). Other statistical information has come from UN peacekeeping mission reports, again including from Lieutenant General (Retired) Carlos Alberto dos Santos Cruz’ report Improving Security of United Nations Peacekeepers (2017), as well as NATO Reviews, including The Washington Summit: NATO Steps Boldly Into the 21st Century written by former US Secretary General Javier Solana. While the administrative controls, however, by nature have been implemented with the qualitative research method, as the measures of administrative controls relate to the practices and personnel of an organization, which generally are not quantifiable.

2 Peacekeeping

To begin answering the research questions of this paper, the nature and background of the /modern peacekeeping environment must first be understood. So that the role information systems have in the modern peacekeeping environment can also understood, allowing the information systems which will be discussed in this paper to be analyzed accurately and effectively to answer the research questions of this paper. One key point to begin understanding the modern peacekeeping environment is that while the organizations around the world that conduct peacekeeping activities can differ in nature, as well as in mandates and objectives, by and large, the purpose and definition of peacekeeping is generally the same. Which, as how the UN describes the roles of UN peacekeepers on the peacekeeping section of their official website, peacekeeping is defined as activities that help countries emerging from a conflict, make the “transition from conflict to peace”, achieved through providing “security and the political and peacebuilding support”.

Peacekeeping missions are only conducted after all attempts of the peaceful settlement of disputes between belligerent forces have failed, as mentioned in Chapter VI of the UN Charter. Methods of peaceful settlement of disputes, as mentioned in Article 33, Chapter VI of the UN Charter, which requires countries with disputes that could lead to war must first the methods: “negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their choice”. If the methods of dispute resolution fail and conflict becomes unavoidable, Chapter VII of the UN Charter sets the parameters of the UN’s powers to restore international peace and security, be it through military or non-military action.

Since its formation at the end of the Second World War, the UN, enacted, alongside NATO, the first official peacekeeping operations in the Balkans, and particularly in Kosovo, during the breakup of Yugoslavia, in 1994. After the UN, they are recognized as the second largest peacekeeping organization in the world. The Balkans became known as "Europe's security-policy testing ground" (Salana 1999) and peacekeeping began with the deployment of the original UN protection force to Croatia in 1992, followed by Bosnia and then Macedonia. “What was originally envisaged as a six-month deployment lasted for four years”, says Salana (1999, 7).

This is where the first real lessons of effective peacekeeping were realised, reflecting the complications of peacekeeping in the complex and volatile fourth generation warfare environment, where "frequently, the situation is complicated by the presence of warlords and conflict entrepreneurs, prepared to exploit myths and instigate violence to help seize or retain power", says Espen Barth Eide, State Secretary in the Royal Norwegian Ministry of Foreign Affairs, in the NATO Review Article, Peacekeeping Past & Present (2001). The unpredictable and volatile nature of these relatively new and modern environments peacekeepers operate, have created a crucial need for deployable information systems which can be rapidly deployed at any location, able to provide a Command & Control function. This is where the new concept of Deployable Communication Information Systems (DCIS) has emerged, as most effective information system of its kind and the most effective information management asset available in the field to peacekeepers.

2.1 Peacekeeping Organizations

In terms of length of operational history, organizational size and scale, the UN is the world's most prevalent peacekeeping organization. With a budget of "$6.51 billion for 13 peacekeeping operations in 2019 and 2020", as stated on the 'Meetings coverage and Press Releases' section of the UN official website, from a UN General Assembly meeting on 3 July 2019. According to the 'How We Are Funded' section of the UN official website, "this amount finances 12 of the 13 United Nations peacekeeping operations, supports logistics for the African Union Mission in Somalia (AMISOM), and provides support, technology and logistics to all peace operations through global service centres in Brindisi (Italy) and a regional service centre in Entebbe (Uganda)". The amount includes paying for the just over 100,000 active peacekeeping personnel for the 13 current UN peacekeeping operations as of 2020.

Because of the UN's large size and scale, as well as the reputation the UN has gained through their lengthy history organizational history since being formed in 1945, the UN and their peacekeepers, easily recognisable by the distinctive blue 'UN' marked helmets, are widely regarded to be the main actors of global peacekeeping operations. The other key organizations, in terms of global peacekeeping presence, is NATO. Conducting both independent and joint peacekeeping operations, with other organizations or military forces. But more often, alongside the UN in joint peacekeeping operations or missions. A new peacekeeping concept and term of 'hybrid' peacekeeping missions is emerging, however, as a new and more appropriate way of describing joint peacekeeping missions, to reflect the changes of the modern peacekeeping environment and the more collaborative and diplomatic approach organizations are applying in their missions. The United Nations African Union Mission in Darfur (UNAMID) is the first example of a 'hybrid' peacekeeping mission, although the UN has worked with other organizations countless times throughout the history of peacekeeping.

In addition to the UN, the other organizations that will be discussed and referenced in this paper for their peacekeeping activities and whose information systems will be analyzed, is NATO and the British Army. The UN, NATO and the British Army have been chosen for discussion, comparison, and analysis of their information systems in the context of peacekeeping in this paper, is largely for one reason. Because, while the nature and mandates of these organizations have some significant differences, the peacekeeping operations they conduct, and the information systems that are used to support their operations, have many similarities. Providing the opportunity for a rich, more accurate and reliable information system comparison in this paper.

The comparison and analysis of the information systems used by these organization in Chapter 5 of this paper is what will primarily contribute towards the purpose and aim of this thesis, which is to amalgamate information about information systems used by peacekeeping organizations to further the development of teaching and learning in the fields of information systems, peacekeeping, and information security. In doing so, answering the research questions of this paper.

2.1.1 North Atlantic Treaty Organization (NATO)

NATO is another organization highly prominent in global peacekeeping activities, following closely behind the UN in supporting the global peacekeeping cause. NATO shares a commonality with the UN in that it also began its peacekeeping activities in the Balkans in 1992, during the break-up of Yugoslavia. Leading the military offensives against Serbia in Bosnia and Herzegovina. NATO is a political and military alliance with the purpose to "guarantee the freedom and security of its members through political and military means", according to the ‘What Is NATO?’ section of their official website. NATO operates globally in every kind of environment and terrain to meet this objective. In terms of power, with 29 member countries from the U.S. and Europe, as well as 40 partner countries, NATO has greater offensive and military capabilities than the UN.

Regarding NATO’s large organizational size and scale, as is the case with the UN, there is an imperative need for native and fully interoperable information systems that every member countries’ forces can use, especially when conducting joint peacekeeping operations. NATO achieves this with the UN MCC (United Nations Modular Command Centre), of which its interoperability will be analyzed later in this paper, in relation to the research questions of this paper. Regarding organizational structure, NATO's diverse and often large-scale international peacekeeping activities, as is also the case with the UN, mean that a clear chain of command is vital for the use of an information system to conduct peacekeeping operations.

NATO often operates in extremely hostile and dangerous environments, as do the British Army and UN. Depending on the type of peacekeeping mission, and mandate under which a NATO operation is authorised, NATO’s strong-point - military force, is often required. Which is particularly useful in peace-enforcement missions, for example. NATO operations could be in an active conflict or warzone, or a zone which is recently emerging from a war or conflict – the first NATO military operations in Bosnia, during and after the break-up of Yugoslavia, from 1992 – 2004 testify to this. The Yugoslav Wars period, and the Bosnian War (1992-1995) which NATO was heavily involved in alongside the UN, testifies to the level of danger peacekeepers can face. The Yugoslav Wars, ending with the Kosovo War (1998 – 1999) were the last of the twentieth century, and arguably of the twenty-first century. Involving NATO and other Western peacekeeping forces, including the UN and British Army, in which there occurred armed conflicts against an official army – primarily Serbia’s Army, ‘Republika Srpska’.

2.1.2 United Nations (UN)

Similarly, to the North Atlantic Treaty Organization, the UN constantly pursues a core mission of “the maintenance of international peace and security”. This includes, protecting human rights, delivers humanitarian aid, promotes sustainable development, and helps uphold international law. Comprising of 193-member states (every country in the world apart from the Holy See and the State of Palestine), the UN not only the largest peacekeeping organization in the world, but also the largest international governmental body in the world, too.

Unlike NATO which is a military alliance, the UN is defined simply as an “international organization ”, their activities aiming to avoid military force whenever possible, as guided by the “non-use of force except in self-defence and defence of the mandate” principle, one of three principles which is the backbone in guiding the mandates of their peacekeeping operations and the methods of their peacekeeping activities. The other principles are: “consent of the parties” and “impartiality”. These principles govern the five activities of the UN: “maintain international peace and security”, “protect human rights”, “deliver humanitarian aid”, “promote sustainable development” and “uphold international law”. These activities reflect their peacekeeping objectives and greatly influence the mandates of their peacekeeping operations.

Deriving from the large and global scale of the UN, the organizational structure comprises of "organs", as opposed to structures and divisions in NATO. The six organs of the UN are the: General Assembly, Security Council, Economic and Social Council, Trusteeship Council, International Court of Justice, and the Secretariat. Similarly, to NATO, the six UN organs are part of one overall structure. At the top of this structure is the General Assembly. With all 193 states represented, it is the biggest and most important organ of the UN, as the "main deliberative, policy making and representative organ of the UN. Following a hierarchical organizational structure, the Secretariat organ is at the bottom of the organ structure, with tens of thousands of international UN staff members. Also relating to UN’s large size and global nature, the UN also divides itself into agencies, each conducting different activities to contribute to the UN’s overall objectives and can play key roles in supporting UN peacekeeping operations. This depends on what the UN agency is and what its purpose is, however.

Perhaps the most crucial agencies in terms of supporting the information systems used on peacekeeping operations, such as the UN Modular Command Centre, is the United Nations Global Service Centre (UN GSC). The UN GSC, headquartered in Valencia, Spain, and Brindisi, Italy, supports UN peacekeeping operations by providing three core services, Supply Chain Service (SCS), Service for Geospatial, Information and Telecommunications Technologies services (SGITT), and lastly Central Service (CS). It is the first two of these services which “represent the core of UNGSC's service provision to peace operations”.

2.1.3 British Army

The British Army, as one of the three services that form the British Armed Forces, alongside the Royal Navy and Royal Airforce, is not a global, international organization like NATO and the UN. And is therefore a lot smaller in scale, with “112,000 regular and reserve personnel”, according to the homepage of the British Army’s official website. This is not to say the British Army does not operate globally and internationally, which they do, with “43,390 soldiers deployed on tasks in over 40 countries across the globe in 2017”. But that the British Army is based and run only from within the UK. Baring this in mind, the British Army will be referred to as a ‘military service’ or ‘armed force’, for the remainder of this paper, as opposed to an organization. The reason an Armed Forces has been selected among the UN and NATO as a frame of reference is to add an element of variation to the analyses conducted in this paper, enhancing the academic quality and reliability of this paper. The information system employed by the British Army which will be discussed and analyzed in Chapter 5 of this paper, is the BAE FALCON.

The British Army has the core purpose to “protect the United Kingdom’s interests at home and abroad, providing a safe and secure environment in which all British citizens can live and prosper”. While this is the core purpose of the British Army, peacekeeping is an important part of the British Army’s activities. On the ‘What We Do’ section of the ‘Army’ section of the British MOD official website, there are four key activities that the British Army conducts: “Protect The UK”, “Prevent Conflict”, “Deal With Disaster”, and “Fight The Nation’s Enemies”. It is the “Prevent Conflict” activity which refers to the British Army’s peacekeeping activities. Of this activity on the same section of the British Army’s website, it says: “it is in the UK’s interest to tackle causes of instability, fragility and conflict, and to respond rapidly to prevent them – or deal with the instability and conflict that does emerge”.

The UK and the British Army has proved this by preventing and engaging in many conflicts throughout the 20th and 21st centuries when military intervention was necessary. Such involvements include: The Gulf War (1990-91), Bosnian War (1992-96), Operation Desert Fox (1998), Kosovo War (1999), Sierra Leone Civil War (2000), Libyan Civil War (2011), Syrian Civil War (2018), and the ongoing ‘War On Terror’. In addition to these military engagements, interventions and other such peacekeeping activities mentioned above, the UK, according to official UN data, is among 120 UN member nations who contribute troops to UN peacekeeping missions, as an attachment to a UN force. Most of which are from the British Army. For example, on the current UNFICYP mission in Cyprus the UK has attached “244” British troops.

Regarding the British Army’s position in the overall structure of the British Armed Forces, which is part of the overall Ministry of Defence (MOD) structure, the British Army, alongside the Royal Navy and the Royal Air Force, are the three services that comprise the British Armed Forces, which is controlled by Strategic Command (UKStratCom). The British Armed Forces is headed by the Chief of Defence Staff (CDS), the most senior uniformed military adviser, which currently is “General Sir Nick Carter”, as according to the ‘Ministry of Defence’ section of the UK Government official website. The CDS reports to and advises the Secretary of State for Defence, who heads the MOD, which is currently “Ben Wallace MP” (Member of Parliament). So to summarise the British Army’s position in the MOD organizational structure, as the British Army is part of the British Armed Forces, which is headed by the Chief of Defence Staff, the British Army is on the second to highest level of hierarchy. Because General Sir Nick Carter is the head senior military official, and the senior military officials is the second level of hierarchy in the MOD, after the Ministers, who are ultimately in charge of the MOD.

2.2 Peacekeeping Operations

Peacekeeping operations have been conducted on every continent of the globe, with current UN missions including MINURSO in the Western Sahara, UNFICYP in Cyprus, UNTSO in the Middle East and UNMOGIP in India and Pakistan. The methods of which peacekeeping operations are conducted is dependent on the nature of the conflicted environment in which an organization operates. In the most simplistic sense, peacekeeping methods can be defined as military and non-military. It is the mandates of peacekeeping operations that define the authority and powers, and therefore the methods of which an organization conducts a peacekeeping operation.

In the context of UN peacekeeping operations, the UN Security Council authorises missions. The methods of which an operation is conducted can be defined into four categories: observational missions, inter-positional missions, multidimensional missions, and peace enforcement missions. These types of mission, among other factors can present various dangers to peacekeepers, in turn affecting the capabilities of information systems to provide security largely achieved through situational awareness.

2.2.1 Peacekeeping Threats

There are often many and various dangers present to peacekeepers during peacekeeping missions and operations. The risky, unpredictable, and unstable environments in which peacekeepers operate is largely the reason why. Examples of types of political and governmental situations which precipitate conflict in a given country, and therefore dangerous operational environments for peacekeepers, include: “failed governance, conflict spill over, vulnerabilities in ungoverned strategic spaces and resource rich territories, border disputes, extremism and uncontrolled migration”, according to Kalle Kallio in the paper Peace Operations: Supporting Organization by Efficiency (2017, 30).

The following steps from Figure 4, from the educational United Nations video, Security & Rule of Law in the Field (2011) are a typical process during a country’s transition from conflict to peace, in which there are many threats still present to peacekeepers – such as IEDs (Step 1 below).Each step below are also typical mission objective which must executed sequentially in order to safely remove threats and re-build law and order correctly. During these missions in which UN forces directly help with this transition process, they do so with the purpose of re-establishing and maintaining security and rule of law – the lack of which are another one of the main reasons why there are often many and varying dangers present to peacekeepers.

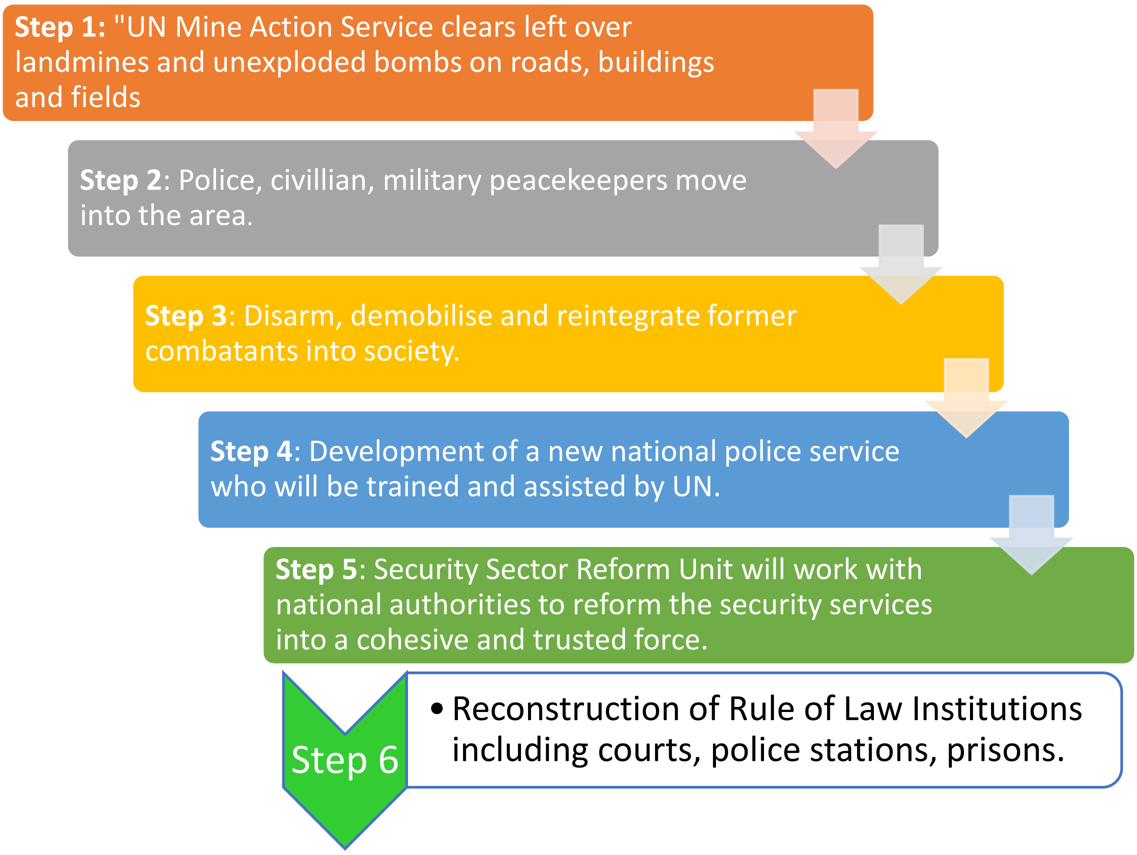

Step 1: "UN Mine Action Service clears left over landmines and unexploded bombs on roads, buildings and fields
Step 2: Police, civillian, military peacekeepers move into the area.
Step 3: Disarm, demobilise and reintegrate former combatants into society.
Step 4: Development of a new national police service who will be trained and assisted by UN.
Step 5: Security Sector Reform Unit will work with national authorities to reform the security services into a cohesive and trusted force.
Step 6
• Reconstruction of Rule of Law Institutions including courts, police stations, prisons.

Figure 4: Re-establishment of Security & Rule of Law Process (United Nations 2011)

After the re-establishment of law and order and security, as accomplished in step 6, the dangers which were present not only to peacekeepers, but to civilians, too, have mostly been removed. Aside general factors related to the country in which a peacekeeping mission is being conducted, and that country's governmental and political situation, the dangers which may be present to peacekeepers are also highly related to the type of peacekeeping mission which is being conducted. In reference to Page Fortna's 'Does Peacekeeping Work?' (2008, Chapter 7) there are four types of peacekeeping operations, of which the methods in which they are conducted are heavily influenced by the mandate of which they are authorised. The four missions are as follows:

- Observational Missions

In these missions, peacekeepers, typically unarmed, comprise small contingents of military or civilian personnel, who must observe and oversee cease-fires, troop withdrawals, or other conditions outlined in a ceasefire agreement. Because observation missions occur after a peace agreement has already been signed, and the transition of conflict is already in the process of being fully implemented, these types of missions are generally present a far lower risk and far less danger to peacekeepers. As opposed to a mission in which peacekeepers entered an active conflict zone, for example.

- Inter-positional Missions

Inter-positional peacekeeping missions can be interpreted as 'traditional' peacekeeping missions. Whereby, lightly armed peacekeepers, which comprise medium to large scale contingents of troops, act as a buffer between belligerent factions in the aftermath of a conflict. This is the stage where a conflict zone is still settling down before implementations for the transition of conflict to peace are made. Therefore, dangers such as hostile local militia, insurgents, or remnants of the offensive strategies such hostile forces employed, may still be present, such as IEDs, which poses a particularly dangerous threat to peacekeepers in the United Nations Multidimensional Integrated Stabilization Mission in Mali (MINUSMA).

- Multidimensional Missions

Multidimensional peacekeeping missions are conducted by military and police personnel and are somewhat of a hybrid between observational and inter-positional type peacekeeping missions. As well as the tasks of observational and inter-positional peacekeeping missions, military and police personnel also conduct more 'multi-dimensional' tasks, which include "electoral supervision, police and security forces reformations, institution building – such as courts or police stations. Examples of such missions include UNTAG in Namibia and ONUSAL in El Salvador.

- Peace-Enforcement Missions

Peace enforcement missions comprise both civilian and military personnel to comprise a large and well-equipped military force. The mandates of these missions authorise peacekeepers to use offensive force. Offensive force is authorised because these types of missions are the most dangerous – whereby peace is enforced largely through offensive means. The NATO operations in Bosnia during the break-up of Yugoslavia conducted by the NATO Implementation Force (IFOR) and Stabilization Force (SFOR) are examples of peace enforcement missions in which force is required. These types of missions are different from UN peacekeeping missions, but the threats present to peacekeepers, such as small arms fire which still remains the single biggest killer of UN peacekeepers, although perhaps to a lesser extent in UN peacekeeping missions, remain the same.

In the United Nations report Improving Security of United Nations Peacekeepers (2017), Cusimano, Phillips and Lieutenant General (Retired) Carlos Alberto dos Santos Cruz, provide insight into the level of threats and consequential casualties in modern UN peacekeeping operations. They say, “since 1948, more than 3,500 personnel have lost their lives serving in United Nations peace operations with 943 due to acts of violence” (2017), as written in the executive summary of the report. There are lots of potential dangers present in peacekeeping missions, though more so in type four peace enforcement missions. Dangers arise mostly due to the threat of violence from hostile forces in operation areas. For example, the bases of peacekeeping organizations deployed in an operational area can be attacked – as recently was the case in the UN MONUSCO mission, for example, when, “at the end of 2017 militants attacked a UN base in the Eastern Democratic Republic of Congo” – killing fifteen peacekeepers, “the highest single death toll from an attack on a UN peacekeeping mission since Somalia in 1993”, writes Lisa Sharland of the Australian Strategic Policy Institute in the 2018 article, Security of UN Peacekeepers: the Minefield of Politics, People and Principles. Sharland also writes in the article that “small arms and improvised explosive devices being used in the vast majority of fatal attacks in recent years”, supporting that terrorists and other such violent extremists now present in the modern peacekeeping environment now launch attacks against peacekeepers.

Although, while terrorists and extremists can choose peacekeepers specifically as a target and attack them directly, as was the case when a UN base in the Democratic Republic of Congo was attacked in 2017, casualties are often civilians too. It often appears in dangerous environments in which peacekeepers operate, such as in the UNAMA mission in Afghanistan, that both peacekeeper or civilian casualties occur as a result of a ‘crossfire’ of attacks or threats against either one of these parties, although often leading to casualties both peacekeeper and civilian. In the case of suicide IEDs, detonated using a vehicle or vest, for example, the explosion of which does not discriminate against civilian or peacekeeper.

This is particularly evident in the United Nations Multidimensional Integrated Stabilization Mission in Mali (MINUSMA), the UN peacekeeping mission with the “highest fatality numbers due to IEDs, with the majority occurring during convoy operations”, according to Cruz, Cusimano and Phillips in “Issue 11 – Improvised Explosive Device (IED) Threat Mitigation” in the report ‘Improving Security of United Nations Peacekeepers (2017, 26). They also say, “the frequency of attacks and quantity of explosives used in IEDs have increased and emplacement methods have increased” and that “these trends will likely worsen in the future” (2017, 26). There have been extremely high levels of UN casualties and fatalities in Mali since MINUSMA commenced in 2013, now at a total of “208” as of 31 December 2019 as mentioned on the UN’s official “total fatalities since 1948” list on their website. MINUSMA, as the current peacekeeping mission with the highest number of IED casualties, many fatalities of the 208 recorded fatalities were from IEDs. In fact, according to the UN Secretary General's report of the situation in Mali, (2018), in the three-month reporting period between October and December 2018 alone, "48 incidents involving the use of improvised explosive devices were recorded" (2018, 6), point 27 of the Secretary's General's attack reports.

For the total, however, since January 2018, the Secretary General in the report says this: "The number of improvised explosive device incidents since January 2018 continued to increase, with 192 incidents having occurred, compared to 124 incidents during the same period in 2017". Regarding an attack on a MINUSMA base in Ber, Timbuktu region on 27 October, he says this "two vehicles filled with explosives entered the camp, where one of them exploded. The attack resulted in two peacekeepers killed in action and eleven injured". Figure 5 below, from the report Improving Security of United Nations Peacekeepers (2017) illustrates the high threat of base attacks between 2013 and 2013, at a total of 65 UN fatalities due to attacks on camp or positions.

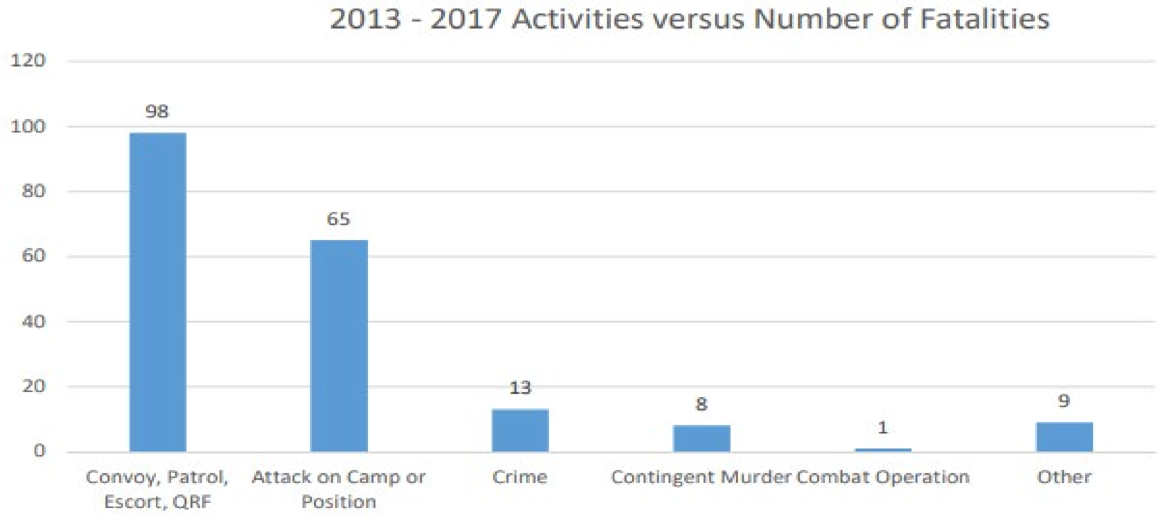


Figure 5: 2013 – 2013 Activities versus Number of Fatalities (Cruz, Phillips, Cusimano 2017, 7)

As Figure 6 below illustrates, also from the report Improving Security of United Nations Peacekeepers (2017), while small arms fire is still the single biggest killer of UN peacekeepers, IEDs are nevertheless, the second biggest contributor to peacekeeper fatalities, causing a total of 43 peacekeeper deaths between the years 2013 and 2017. While in the MINUSMA mission, IEDs are becoming an even greater threat. As the UN Secretary General reports on the MINUSMA mission, on the same day as the base attack, "a MINUSMA vehicle (was) struck (by) an improvised explosive device or mine, followed by an armed confrontation with an alleged violent extremist group. The attack resulted in the wounding of six peacekeepers". The Secretary General continues to list a number of IED related attacks in the report, emphasising how the increased in today's peacekeeping environment there is an increased level of danger to peacekeepers on operations from evolved threats – increasing the need of advanced technology in information systems used on operations to mitigate these threats through situational awareness.

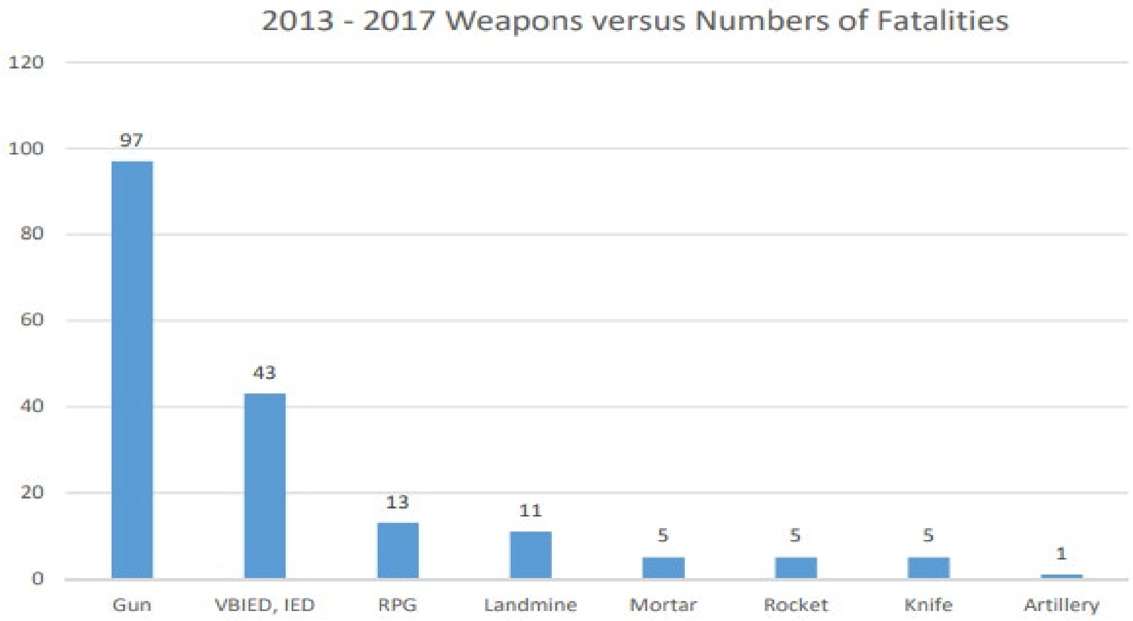


Figure 6: 2013 – 2017 Weapons versus Numbers of Fatalities (Cruz, Phillips, Cusimano 2017, 7)

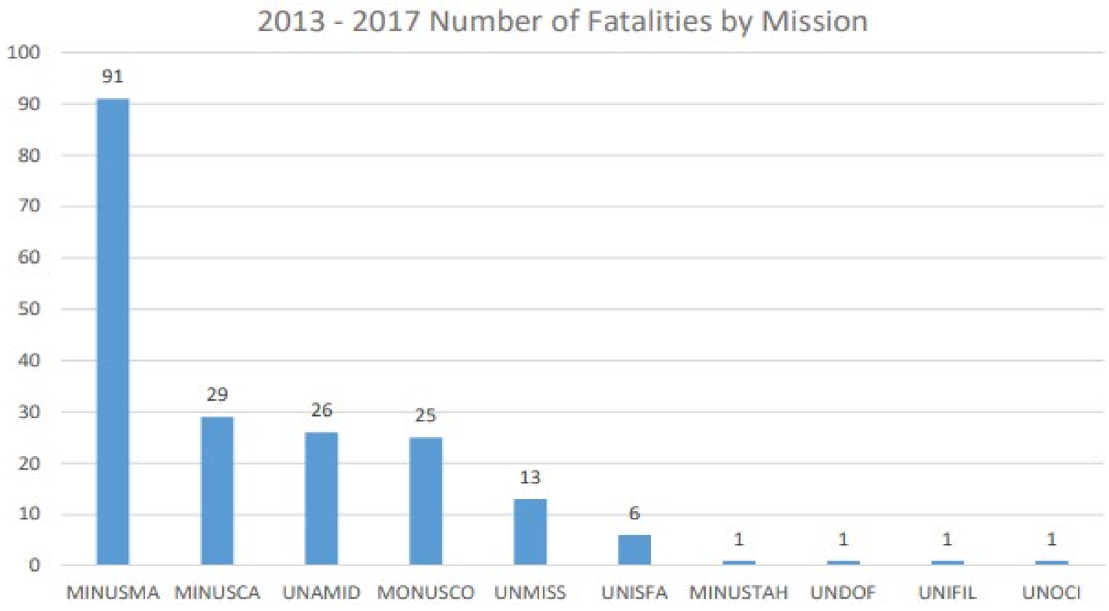


Figure 7: 2013 – 2017 Number of Fatalities by Mission (Cruz, Phillips, Cusimano 2017, 8)

2.2.1 How Peacekeeping Information Systems Mitigate Peacekeeper Threats and Contributes Towards Peacekeeper Security

In looking at Figure 7 above, representing the total number of deaths between the yeas 2013 and 2017 by mission type, it is evident due to the fact that the MINUSMA mission has the highest number of peacekeeper fatalities than any other mission, at 91, that the high level of IED related casualties in the MINUSMA mission is the main contributor to this statistic. The modern peacekeeping environment poses many new threats to peacekeepers, which were not present in the past peacekeeping operations since until the end of the twentieth century. Consequentially, the need for information systems to provide security to peacekeepers, largely achieved through delivering situational awareness, has never been higher. The increased level of threat to peacekeepers and the increased need for information systems to deliver security, is reflected through the significant increases of peacekeeper casualties since 2013. Evident by how Lieutenant General (Retired) Carlos Alberto dos Santos Cruz, a former force commander of the UN Organization Stabilization Mission in the Democratic Republic of Congo (MONUSCO) as well as the UN Stabilization Mission in Haiti (MINUSTAH), says "casualties have spiked" (2017.)

In fact, emphasising the increased level of danger to peacekeepers and how threats have evolved in the modern peacekeeping environment, Cusimano, Cruz and Phillips (2017) also say that during the five-year period between 2013 and 2017, "195 personnel in United Nations peacekeeping missions have been killed by acts of violence", which they also say, is "more than during any five-year period in history". Examples of threats which have contributed to the rise in peacekeeper casualties include "armed groups, terrorists, organised crime, street gangs, criminal and political exploitation, and other threats" (2017). Unpredictable and highly dangerous threats to peacekeepers such as these, reflect the importance and need for information systems to be able to provide situational awareness, for example, from SATCOM. As well as the ability for information systems to receive situational awareness, obtained from peacekeeper patrols in operational environments. For strategies and orders from Command & Control to be issued, enabling for the mitigation of threats in an operational environment. Threat mitigation could mean, for example, advising a patrol of UN peacekeepers to stay clear of an area known for hostile activity. In utilising the five basic information system functions of: input, storage, processing, output, and feedback loop, there are various ways information systems mitigate threats and deliver situational awareness and security to protect peacekeepers.

2.2.2 Threat Identification

Arguably the most effective security benefit that information systems can provide, is Threat Identification. There are various ways in which an information system can detect threats, such as satellite imagery and other such forms of monitoring and surveillance technology, or security cameras and other such devices connected to an information system. As is mentioned by Lieutenant General (Retired) Carlos Alberto dos Santos Cruz, one of his recommendations for the report of Improving Security of United Nations Peacekeepers (2017), under the heading; “defensive posture”, he mentions that threat identification is crucial and necessary to “neutralise or eliminate threats”. The ways in which threat identification as well as the means of doing so, including through satellite and UAV (Unmanned Air Vehicles), will be discussed throughout this paper as well as in the Deployable Communications Analysis as not only a basic requirement of information systems in the modern peacekeeping environment, but also as one of the most crucial and effective means an information system, in combination with the human component of the system, has in contributing towards peacekeeper security.

2.2.3 Advanced technology

Advanced technology refers in this thesis to both the technological infrastructure of an information system, as well as the devices and equipment connected to an information system. Advanced technology is fundamental in enabling peacekeeping organizations to obtain situational awareness and intelligence. Without advanced information system technology, however, to deliver situational awareness and intelligence, such as satellite communications (SATCOM) (which is also heavily relied upon for threat identification) these critical types of information could be unobtainable and peacekeeping operations would be much riskier for peacekeepers.

In addition to enhanced situational awareness and intelligence capabilities, advanced technology enables command and control elements in peacekeeping organizations to enact military strategies and enhance their overall offensive and defensive capabilities against enemy forces and threats. An example of this, can again be seen in the report “Improving Security of United Nations Peacekeepers”, also under the recommendation of “defensive posture”, where Lt General Carlos Alberto says UN peacekeepers should “push combat to the night, to take advantage of their superior technology” (2017) (in peacekeeping missions where use of force is required, such as peace enforcement missions). Because, when advanced technology (most of which is connected to the information system of a peacekeeping organization, such as the UN Modular Command Centre) enables use of tactics and strategies such as night combat and operations, which enemy forces do not possess the technological capacity to effectively conduct, peacekeepers have the advantage over their adversaries. Whereby, active and offensive strategies such as this, prevent “freedom to hostile forces to decide when, where and how to attack” (Cruz, Phillips, Cusimano 2017) peacekeeping forces.

2.2.4 Interoperability

In today’s computer-driven world that produces “2.5 quintillion bytes of data everyday”, according to Bernard Marr of Forbes Magazine in the 2018 article, ‘How Much Data Do We Create Every Day?’. And it is because of the fact that today’s world is so computer driven that the term ‘interoperability’ is such a widely applicable concept in today’s computer driven world. Because of this, there is no singular and universally agreed upon definition. A basic definition, however, as defined by Merriam-Webster, is the "ability of a system to work with or use the parts of another system", which in the context of peacekeeping information systems, means the ability of parts of an information to exchange data with either a different part of the same information systems, or with another information system. This can be classified as internal interoperability and external interoperability. Interoperability can be achieved through various communication methods, including Wide Area Networks (WAN) and Local Area (LAN) Internet Protocol (IP) networks, as will later be seen in the case analysis of the NATO DCIS. There are various benefits to interoperability of information systems during a peacekeeping operation which will be discussed below.

External Interoperability of an organization 's information system with the information systems of other organizations, and vice versa can be crucial on operations, and can greatly contribute towards peacekeeper security. Particularly as current peacekeeping operations include multiple different UN member nations. If a system is interoperable with other systems during operations, organizations can have one shared common operational picture displayed on their information system. And there is a common platform which organizations can use to share and receive the same information with each-other, in the same format. This enhanced accuracy of shared information through a common system and format, leads onto the benefit of enhanced situational awareness and situational understanding. The relationship between interoperability, Situational Awareness (SA) and Situational Understanding (SU) will later be discussed in this chapter. Preceding how SA and SU contribute to peacekeeper security in the next chapter.

Depending on the type of information peacekeepers of an organization such as NATO is sharing with another organization such as the UN, there is the potential to enhance SA and SU through interoperability. Whereby, if NATO peacekeepers, for example, send real-time information from an operational environment to a universal and interoperable platform between NATO and the UN, whereby the UN can receive and analyze the information instantaneously, without the information having to pass through other systems before reaching them. Because not only is time saved which increases the chance of the information received being more up to date, accurate, and reliable, which therefore enhances the quality of the SA being received, but it also guarantees that the UN peacekeepers and UN Command & Control elements will receive exactly the same information as was sent by the NATO peacekeepers in the field.

The ability for organizations on joint peacekeeping operations to share and receive accurate and direct information from the same reliable sources, in the same place is crucially beneficial also in speeding up the process of completing mission objectives. Because, as is the case by how in crises, "there is a lot of information available from different sources" (Kallio 2017). And, as often happens in these situations, "communication systems are not able to provide this information (from different sources) in an organised way" (Kallio 2017). Creating a delay in not only the receiving of information, but also the processing and understanding of information which hinders the ability to plan and enact peacekeeping operations. Which again, provides far more accurate situational understanding and situational awareness, which will now be discussed why situational awareness and understanding contributes to peacekeeper security in the following chapter.

Another benefit of external interoperability through a common information sharing platform, is that all peacekeeping organizations and stakeholders in an operational area, such as NGOs, have access to the same information. As opposed to having different access privileges to certain information, which could occur because data in one organization 's information system could have been given a different security classification than in another organization 's system, or because of differing access controls to shared information. In preventing this obstacle to creating an accurate and cohesive common operational picture and understanding, through interoperability and enhanced cooperation, a greater Situational Understanding, collectively speaking in terms of all friendly forces in an operational area. Which is crucial to mission success.

Because, as Kallio agrees, in the paper 'Peace Operations: Supporting Efficiency by Organization', "access to information is an essential factor in reaching the strategic objectives" (Kallio 2017) and information that is shared and received "can be utilized only if it is accessible" (Kallio 2017). Therefore, as previously stated and as Kallio also agrees when he says "the stakeholders should form an information network enabling the information to reach the end-users" (Kallio 2017), interoperability should be achieved through an interoperable and common information sharing network or platform between organizations on joint peacekeeping operations. Because in doing so, there is a stronger and more effective joint ability to "contribute(s) to a situational understanding and to reaching the objectives" (Kallio 2017), because "when stakeholders are within an information sharing community, they have access to contributing to the operation as well as sharing their information and resources" (Kallio 2017).

This benefit of enhanced cooperation and mission planning through interoperability includes the additional benefit of a stronger ability for Command and Control elements to have the necessary information to act upon in making decisions to avert threats and enhance peacekeeper security. Of which the information sharing of the/ decisions themselves can also be achieved more efficiently through an interoperable system, as will shortly be discussed in the benefits Regarding internal interoperability. Additionally, when peacekeeping objectives are being met, such as objective 1 of Figure 4, Chapter 2.2.1 Peacekeeping Threats, of the UN Mine Action Service to clear left over landmines and unexploded bombs, it means the mission is progressing towards the overall objective of all peacekeeping missions. Which is, as stated by the UN on the 'Peacekeeping' section of their website, the "transition from conflict to peace", whereby after this transition is complete, there is less danger not only to the civilians and local population, but also of the peacekeepers. Because, again referring to Figure 4, Chapter 2.2.1

Peacekeeping Threats, as seen in step six in which rule of law and law establishments and security services have been re-created, threats previously present to civilians and peacekeepers, such as terrorists and the consequent IEDs they lay, as was the case in Afghanistan, can now be apprehended and removed. As has been the case in Afghanistan when the British Army as other British Armed Forces ceased all combat operations in Afghanistan leaving in 2014, handing over control to the Afghan police and allowing the sub sequential United Nations Assistance Mission in Afghanistan (UNAMA) to take effect.

In achieving external interoperability by having two or more parties which can communicate with each-other through a shared information system, there is another joint cooperation benefit in which the peacekeeping organizations working together on a peacekeeping operation can more effectively work with each-other and cooperate to meet mission objectives. Which is another reason why interoperability in joint peacekeeping operations and between UN attachment forces is imperative in allowing them to plan, cooperate and conduct operations more effectively through using the same information systems and communicating with the same technology and information sharing networks and platforms. “Joint planning, as well as implementing and evaluating actions, will enhance the level of understanding of strategic objectives. Therefore, information is needed to reach a holistic approach and more efficiently perform as one” (Kallio 2017). Because cooperation and shared communication platforms not only allow an increased ability to complete mission objectives, but also to share situational awareness, crucial for peacekeeper security.

Regarding Internal Interoperability, it is when the parts and components of an information system of one organization ’s information system are connected so that data can be shared, received, and stored throughout an information. Internal interoperability of an organization ’s information system, as will be discussed later in the Deployable Communications Analysis, Chapter five of this thesis, particularly in analyzing the WAN and LAN IP networks of the interconnected Wide Area Service Provision (WASP) vehicles of the British Army’s BAE FALCON information system, is crucial in allowing information to effectively flow between the peacekeepers in an operational environment and the C2 element of an information system. As seen in Lawson’s Model of Command and Control, allowing situational awareness to be received by a commander to provide situational understanding, which further allows for the commander to issue orders back down the chain of command and through the information system before reaching peacekeepers in the field. These orders and information provided by commanders can enable them to avert from any potential threats in an operational environment. And the decisions made from situational understanding of a commander may not only have come directly from the situational awareness of peacekeepers themselves, but from other means in an information system achieved through advanced technology, such as monitoring and surveillance technology such as satellites or UAVs, capable of taking extremely high zoom and resolution images which can provide intelligence and awareness to threats present to peacekeepers in an operational environment, such as the locations of enemy forces.

2.2.5 Situational Awareness

Situational Awareness (SA), as defined by Endsley in Design & Evaluation for Situation Awareness Enhancement (1988), defines situation awareness 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”. It is a state in which the human factor of an organization has an accurate, up to date, and often real time perception of the events unfolding in an operational environment, and around one’s forces. The importance of SA in providing peacekeeper security lies in the fact that without it, C2 elements who rely on information systems to obtain SA of their forces and of the state of an environment (of which they can enact Lawsons’ Model of Command & Control if the environmental state is not as is desired) as well real-time SA transmitted by ground forces to an information system, which acts as a medium between forces and C2 elements, commanders would not have accurate information. Without accurate information about an environmental state and the situation of his/her forces, loss of life can occur, especially when considering the previously mentioned and extremely dangerous threats which are now rife in the modern peacekeeping environment.

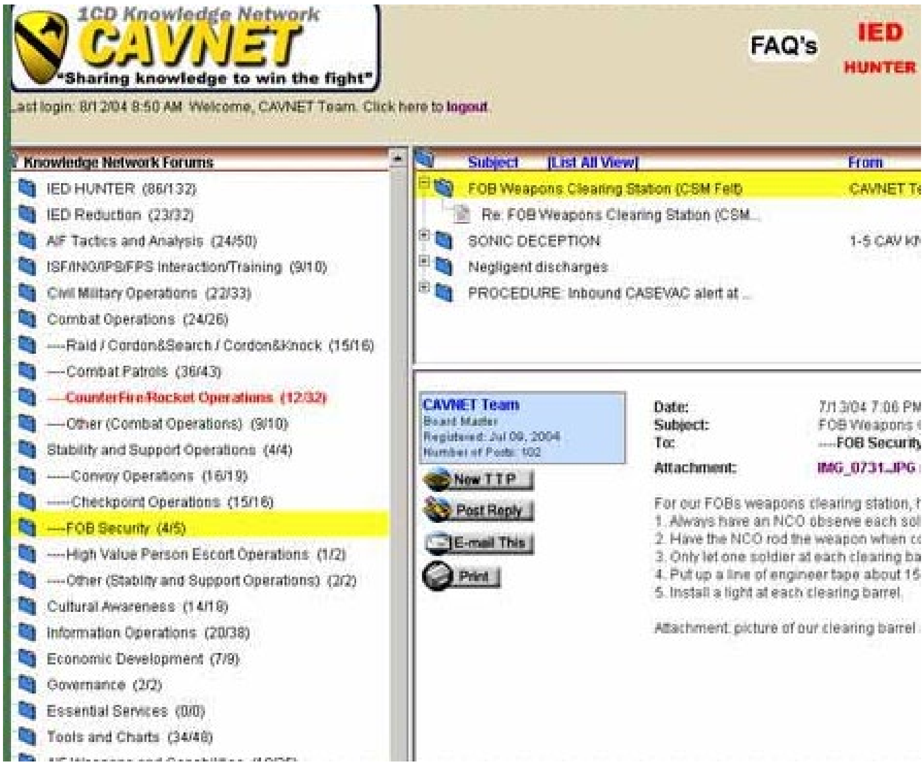
Situational awareness is a form of tactical intelligence, which Cruz, Cusimano and Phillips (2017) emphasize the crucial need for in peacekeeping operations, to improve peacekeeper security. Under “Issue 13- Intelligence for The Security of Peacekeeping Personnel” (issues in the report referring to current problems in the way UN peacekeeping missions are being conducted, which are causes of peacekeeper casualties and fatalities), they say that “A lack of tactical intelligence prevents leadership and personnel from detecting, avoiding, and countering threats” (2017, 28). The best example to demonstrate the importance of Situational Awareness, and the effectiveness it can have in providing peacekeeper security, when effectively delivered, are communication networks. While communications networks are not strictly information systems themselves, in the sense of the information systems used to support operations with an attached C2 element, examples of real communication networks that have been used by peacekeeping forces on operations will be used to demonstrate exactly how SA is important, and why the information systems that are used by peacekeeping organizations as their primary information management assets on operations, must be capable of delivering SA.

Interoperability is crucial for SA to be shared on communications networks and received by other organizations. Because interoperability between peacekeeping organizations in an operational area allows for all friendly forces to communicate and constantly be connected with each other, sharing SA over one single network. Because interoperability means that the real time information inputted into an information system, can also be shared simultaneously to other organizations, alerting all branches of a single organization, as well as other organizations of threats in an environment.

In Afghanistan, the particular threat that demanded such an SA capability to counter it and protect peacekeepers, was IEDs, laid on roads by insurgents. For this particular threat, according to Henry S. Kenyon in Chapter 2 “NATO Deploys Command and Control Tool in Afghanistan” of the Multinational Operations Newsletter (2009) TIDE featured a "planning and deconfliction capability that permits convoys to plan around traffic jams", whereby convoys could alert other convoys in the area of potential threats in the local area, and advise which roads not to travel on when there was traffic. Because high traffic is risky in that it increases the chance of ambush or being attacked, or for insurgents to lay an IED. But TIDE therefore decreased the threat of being attacked by insurgents, therefore contributing towards peacekeeper security.

The network, CAVNET (Communications Against Violence Network), enabled users to "enter situational data into the network to alert other groups operating in the area" (Kenyon 2009), enabling them to plan around a situation before entering it unknowingly. Thus, preventing casualties that would result from threats present in an operational environment, which would otherwise be much harder to avoid without the constant communication flow between coalition forces, achieved by CAVNET. Again, demonstrating the importance of interoperability in an information system. It can also be noted that CAVNET, was also a form of monitoring technology, where instead of having monitoring technology to alert of imminent threats, it was the soldiers themselves alerting of imminent threats by inputting data into the network to keep other friendly forces in area safe.

The screenshot from CAVNET below, Figure 8, is obtained from a PBS FRONTLINE article called Innovating and Improvising (2005), which featured a Q & A with the founder of CAVNET Maj. Patrick Michaelis. It illustrates how an interoperable network is not only a crucial part of an individual organization 's information system, but how in connecting multiple organizations, it can form one giant, interoperable collaborative information for joint peacekeeping operations. The various capabilities of the network to increase Situational Awareness, interoperability, and operational safety and security to peacekeepers in the field are listed on the left column, such as "IED HUNTER", "IED REDUCTION" and "FOB Security" (Forward Operating Base).



Last login: 8/12/04 8:50 AM Welcome, CAVNET Team. Click here to logout.

Knowledge Network Forums

- IED HUNTER (86/132)
- IED Reduction (23/32)
- AIF Tactics and Analysis (24/50)
- ISF/ING/IPS/FPS Interaction/Training (9/10)
- Civil Military Operations (22/33)
- Combat Operations (24/26)
- ----Raid / Cordon&Search / Cordon&Knock (15/16)
- ----Combat Patrols (36/43)
- ----CounterFire/Rocket Operations (12/32)
- ----Other (Combat Operations) (9/10)
- Stability and Support Operations (4/4)
- -----Convoy Operations (16/19)
- -----Checkpoint Operations (15/16)
- ----FOB Security (4/5)
- ----High Value Person Escort Operations (1/2)
- ----Other (Stability and Support Operations) (2/2)
- Cultural Awareness (14/19)
- Information Operations (20/38)
- Economic Development (7/9)
- Governance (2/2)
- Essential Services (0/0)
- Tools and Charts (34/48)

Subject [List All View]	From
FOB Weapons Clearing Station (CSM Felb	CAVNET Te
Re: FOB Weapons Clearing Station (CSM...	
SONIC DECEPTION	1-5 CAV KN
Negligent discharges	
PROCEDURE: Inbound CASEVAC alert at ...	

CAVNET Team
Board Master
Registered: Jul 09, 2004
Number of Posts: 102

Date: 7/13/04 7:06 PM
Subject: FOB Weapons
To: ----FOB Security
Attachment: IMG_0731.JPG

For our FOBs weapons clearing station, t
1. Always have an NCO observe each sol
2. Have the NCO rod the weapon when c
3. Only let one soldier at each clearing ba
4. Put up a line of engineer tape about 15
5. Install a light at each clearing barrel.

Attachment: picture of our clearing barrel

Figure 8: CAVNET Screenshot (PBS, 2005)

The following are examples of how the situational awareness capabilities of CAVNET have been used in Iraq to enhance security, according to the founder of CAVNET Maj. Patrick Michaelis. They testify to the importance of shared, interoperable communication networks in contributing to security through providing enhanced situational awareness and situational understanding. This importance is demonstrated by actively averting threats and danger.

- “A scout platoon leader -- in this case the scout platoon leader from 1-8 Cav. -- was given the mission to conduct sniper operations. He had never really executed a mission like it before. He looked on the CAVNET, where a commander from 1-9 Cav, in another part of the city, had posted notes and TTPs from employment of snipers over the past months. The Scout Platoon Leader from 1-8 was able to integrate what he had read from the CAVNET into his planning, preparation, and execution cycle.

- “A leader posts a report that his unit experienced an IED that was cloaked by a poster of Moqtada al-Sadr. On the other side of the city, a commander taps into the CAVNET and reads the post. Though he is in another part of the city, he has been involved in operations that require removing posters posted on IIG (Iraqi interim government) projects. He briefs up his leaders before they execute a normal combat patrol. One sees a poster that mirrors the description given by the original post. Instead of ripping it down, he calls EOD [Explosive Ordinance Disposal], who discovers that it is rigged as an IED”

2.2.6 Situational Awareness Collection Methods: Field Assessments

Field assessments, is something particularly the UN, will conduct before arrival to an operational environment. Field assessments, more commonly referred to as 'baseline assessments' in the UN, provide information about an operational environment, including demographics, weather, and geography. This geographical and demographical information can be collected, stored, and shared in an information system. The BAE FALCON, being an excellent example of an information system that achieves this process via satellite photography, transmitting data and photographs to ground connected ground stations. Field assessments are critical in providing Situational Intelligence that not only allows peacekeepers to be appropriately equipped and prepared to conduct their mission, but also creates security and protection. Because if peacekeepers are adequately equipped and prepared and aware of potential threats, they can more effectively counter them.

2.2.7 Situational Awareness Collection Methods: Sampling

Sampling, a practice conducted primarily by the UN to gather information about an operational environment, contributes towards operational security because it enables peacekeepers to logistically prepare before deploying in an environment. Therefore, minimising the chances of peacekeepers not being properly equipped or prepared to deal with threats which may be present on the ground. Intelligence about an operational area allows an organization to be logistically prepared, which is particularly relevant, given how, again referring to Lieutenant General Carlos Alberto Santos Cruz' report "Improving Security of United Nations Peacekeepers", under the recommendation of "Operational Behaviour", "each mission is unique, and even within each country, different situations require different actions given the threat that prevails in an area" (Cruz, Phillips, Cusimano 2017). Therefore, sampling, largely achieved through collection, storage and sharing capabilities of information systems, is a critical activity for threat mitigation - enhancing the security and safety of peacekeepers

UNITAR, exemplifies how information systems are used to conduct field assessments, with their Operational Satellite Applications Programme – UNOSAT. Demonstrating similar imagery and data collection as is present in the British Army's BAE FALCON information system, which will later be discussed, UNOSAT's "Humanitarian Rapid Mapping Service", according to UN-SPIDER (United Nations Platform for Space-based Information for Disaster Management and Emergency Response), delivers "imagery analysis and satellite solutions" which is an effective method of conducting geographical and landscape assessments to better help peacekeepers understand the environment they will be operating in, which is crucial for logistical preparedness and providing peacekeepers with the correct equipment to conduct their operation and enhance peacekeeper security. And to quote Lieutenant General (Retired) Carlos Alberto dos Santos Cruz, former commander of MINUSTAH in Haiti and MONUSCO in the Democratic Republic of Congo, "Nobody attacks a stronger opponent", as said in the 2017 report, Improving Security of United Nations Peacekeepers (2017). And in the same report, one of the most important recommendations for improving peacekeeper security is that “troops should not be deployed without the necessary and appropriate equipment in the threat environment. Inadequate or missing equipment facilitates and increases the number of casualties”. Again, emphasizing that gathering intelligence about an operational environment is a crucial activity.

Furthermore, UNOSAT provides such solutions to "relief and development organizations within and outside of the UN system" (UN SPIDER), demonstrating the importance of interoperability between stakeholders involved in peacekeeping operations. Especially regarding those such as Non-Government Organizations (NGOs), who may not have the IS technological capabilities for obtaining such data themselves. Therefore, exemplifying how activities like field assessments, achieved through information systems, can enhance not only the security and safety a single organizations’ peacekeepers, but of many.

3 Information Security

While modern information systems used by peacekeeping organizations must be capable of protecting peacekeepers against the dangers and threats in today's peacekeeping environments, there must also be measures to deal with the cyber threats against the information systems themselves. Because if the information systems used by peacekeeping organizations are compromised, the security created by information systems during peacekeeping operations, and therefore the safety of peacekeepers, may also be compromised. To deter and protect against the various threats posed to information systems, an information system must have robust information security measures in place.

There are various definitions of the term information security', also known as 'InfoSec'. However, it is generally agreed upon by information security experts, to be the practice of protecting information - by mitigating information risks, through a set of practices and tools deployed by an organization, to protect sensitive information. Information, particularly in the context of information systems, is referred to more commonly as 'data', however. In an information system, the set of practices that protect an organization 's information, are largely in the form of access controls, which prevent unauthorised personnel from entering or accessing a system. Access controls, although a critical form of information security, are only, however, a category of the larger information security practice of information security controls, which are the overall crucial enablers for the detection and remediation of security breaches. In addition to information security controls, information assurance is another one of the most integral information security practices. Information assurance is the practice of ensuring the continuity of information confidentiality, integrity, and availability (CIA).

3.1 Information Security Threats

There are many different forms of threats to information security. Including software attacks, theft of intellectual property, theft of equipment or information, sabotage, and information extortion. Regarding software attacks, today there are countless forms of software attacks, though some of the most common ones are viruses, worms, phishing attacks and trojan horses.

Data Integrity is another form of information security, in that integrity of the data can ensure the data or information security. The Electronic Discovery Reference Model (EDRM) is one of the biggest standardization, education and resource platforms dedicated to the fields of data and information security. According to them, Data Integrity "refers to the validity of data". Data Integrity can be compromised for various reasons. Which, as EDRM says, include: "human errors when data is entered, errors that occur when data is transmitted from one computer to another, software bugs or viruses, hardware malfunctions such as disk crashes, and natural disasters such as fires and floods". These threats to information security can be managed and mitigated through security controls, which will be discussed in more detail later. There are different types of information security controls which are designed to mitigate specific threats. For example, physical controls mitigate the risk of data assets succumbing to natural disasters such as fires and floods.

One of the biggest reasons why data can be compromised and its integrity undermined, as in some of these ways listed by EDRM, is because the devices used to store data (data storage devices), are tangible, physical assets. Or are formed by an infrastructure of physical devices. For instance, 'the cloud', which relies upon vast databases comprising of large amounts of servers. Regarding the ways the above causes can compromise Data Integrity, they include "modification, disruption, destruction, and inspection" – the things Information Security practices are designed to prevent, according to CISCO, one of North America's biggest technology conglomerates. For example, if a virus infected a computer, its data could be subject to any one of these methods of data being compromised.

3.2 Protective Measures

To ensure operational security is not compromised, every component in the technological infrastructure of an information system, must have information security measures in place to ensure the overall information security of an information system is secure and protected against threats. The information shared in information systems used by peacekeeping organizations can be extremely sensitive, for example, information relating to operational intelligence, situational awareness, or mission objectives during peacekeeping operations. If such information was to be compromised, operational security, and therefore the safety of the peacekeepers is also put at risk of being compromised. Therefore, it is imperative that peacekeeping organizations have robust information security measures employed in their information systems.

3.2.1 Security Controls

Security controls are measures deployed by an organization to "reduce or mitigate risk" (Walkowski 2019). Risk mitigation in the context of security controls, refers to risk mitigation of an organization 's assets. The most crucial asset to an organization in the context of information systems, is the data itself, managed by an organization 's assets. There are various ways security controls can be implemented, including any type of "policy, procedure, technique, method, solution, plan, action, or device" (Walkowski 2019) designed to achieve the objective of security controls – reducing or mitigating risk to an organization 's assets.

There are three types of security controls: physical, technical, administrative. These control types can have three control functions: preventing, detecting, and correcting. Preventive controls are arguably the most important of the control functions, as their purpose is to prevent security incidents from happening – thus preventing any form of asset damage or loss, as well as financial loss. Detective controls and corrective controls on the other hand, have the purpose of managing incidents while they are in the process of happening, or after they have happened, to try and prevent any imminent or further asset damage or loss.

Regarding the other two control functions, detective controls refer to measures taken to “detect and alert to unwanted or unauthorised activity in progress or after it has occurred” (Walkowski 2019) allowing for a counteractive response to be made and measures for recovery to be implemented at the soonest possible time. On the other hand, corrective controls function after a security incident has happened and are intended to “repair damage or restore resources and capabilities to their prior state following an unauthorised or unwanted activity” (Walkowski 2019), thus remedying the incident. And in the context of peacekeeping, corrective controls would ensure the CIA of information in an information system, as well as the continuity of any information system functions which may have been impaired or compromised as a result of a security incident or breach. Therefore, after the successful implementation of corrective controls, full functionality, and the ability of an information system to contribute towards peacekeeper security would be fully restored.

Concerning the types of security controls themselves, administrative controls are intended to control or change the behaviour of personnel or employees in an organization to lessen the chance of any security breaches or information security incidents occurring through human error. They are “policies, procedures or guidelines that define personnel or business practices in accordance with the organizations’ security goals” (Walkowski 2019). These policies and procedures can apply to many things, including “equipment and internet usage, physical access to facilities, separation of duties, data classification and auditing” (Walkowski 2019). Administrative controls are important because they shape the behaviour of an organization ’s employees or personnel in a way that makes them more aware and knowledgeable of information security. Thus, making information security incidents or breaches from the internal perspective of an organization, less likely to happen.

With respect to technical controls, they are the measures enacted by the network infrastructure and technological components of an organization ’s information system, including “hardware or software mechanisms” (Walkowski 2019). Measures include “authentication solutions, firewalls, antivirus software, intrusion detections systems (IDSs), intrusion protections systems (IPSs), constrained interfaces, as well as access control lists (ACLs) and encryption measures” (Walkowski 2019). Also included as technical controls, as written in the 2012 IGI Global book “Grid and Cloud Computing: Concepts, Methodologies, Tools and Applications” (2012), are “implementing and maintaining access control mechanisms”, “password and resource management”, and “security devices”. Technical controls are important because they strengthen the security of an organization ’s technological and network infrastructure, thus lessening the chance of an external security incident or breach.

Regarding physical controls, according to YAU HK (2014) in the open access article Information Security Controls. Adv Robot Autom 3: e118, from the University of Hong Kong, they are measures to “control physical access to sensitive information and to protect the availability of information”. They include things such as “fences, gates, biometrics access controls, security lighting, CCTVs” (Walkowski 2019). as well as “motion sensors” (Walkowski 2019). and “environmental controls like HVAC and humidity controls” (Walkowski 2019). Physical controls are also a fundamental security control to ensure information security because physical security and information security are interconnected whereby if physical security is compromised, information security can be compromised to. For example, if an information storage facility such as a data centre, is not physically secure, unauthorised personnel may be able to gain access to that facility, thus causing a security breach and potentially an information security breach, with data or data assets being compromised. Physical security controls include controlling facility access, system locking (for example, by password), facility perimeter protection, intrusion monitoring and environmental controls.

It must be noted that physical controls do not only extend to perimeter protection and entry controls, notably with the example of HVAC (Heating, Ventilation, Air Conditioning). Whereby, HVAC controls ensure physical protection of data assets as well as other assets concerning the data assets themselves, against environmental or climate related threats to information security, such as extreme temperatures or humidity. The housing of an information system, which will be discussed later, particularly in the analysis of the UN MCC, is a prime example of where HVAC controls are applied.

4 Command & Control Concepts

An information system is an organised network or structure designed for the collection, organization, storage, and communication of information. There are five functions of an information system: input, storage, processing, output, and feedback loop. Two of the most acclaimed theoretical Command & Control models; Lawson's Model of Command and Control, created by "Dr Joel S. Lawson Sr." of the "Naval Electronic Systems Command", as mentioned in George Orr's 'Combat Operations C3I' (1983, 32), and U.S military strategist John Boyd's OODA (Observe, Orient, Decide, Act) Loop, demonstrate these five functions. Specifically, how they can be executed in an information system.

4.1 Lawson's Model of Command & Control

Figure 9, below, from the article 'Test Design Using the OODA Loop' (Krishnanand 2018), depicts Lawson's model of Command and Control. Which in the most basic interpretation, demonstrates how information is obtained from an environment and then processed and acted upon within a command centre. As is visible by the sequential chain of analyses that occur in the process of interpreting received information, the information or data begins by being sensed, before proceeding through the other analyses before finally being acted upon. Another way of interpreting the information flow of transmission and analyses depicted in this model, is that the information is transmitted and processed hierarchically, flowing from bottom of a command chain or organizational hierarchy in an operational environment, to the top of a command chain or organizational hierarchy to the commander in a Command and Control centre.

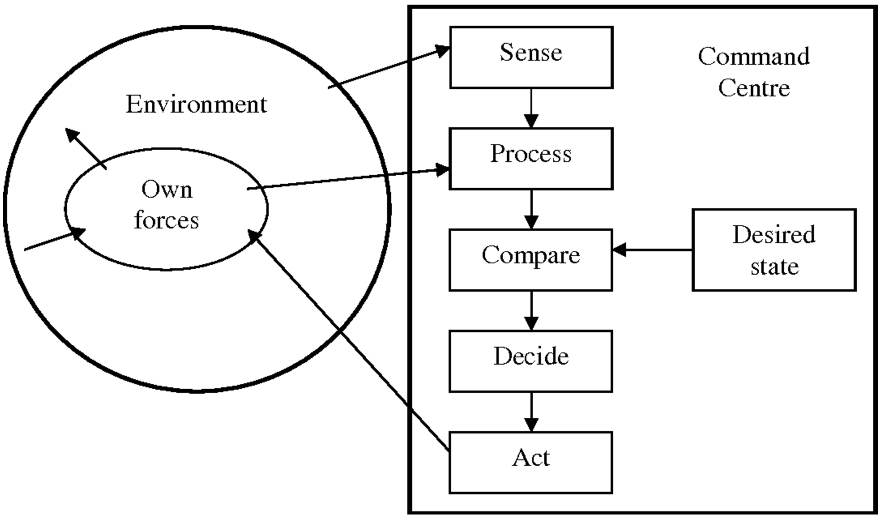


Figure 9: Lawson's Model of Command & Control (Stanton, Baber, Walker, 2008, 209 – 220)

Comparing the current environment state (Situational Awareness) with the desired environmental state, is how Lawson's model theoretically depicts how the information system commander is able to deem whether action needs to be taken, based on the information he or she receives.

If the current environmental state is not the same as the desired state, a decision will be made by the commander in the command centre, and orders will be issued which will lead to a change in the environmental state to make it as desired. In the context of peacekeeping, this would mean Command & Control issuing orders to peacekeepers in an operational area.

4.2 The OODA Loop

Another important command and control concept, which reflects the way peacekeeping organizations process information, using their information systems as a vehicle to do so, comes from US Airforce Colonel and military strategist, John Boyd. He developed a concept known as the OODA loop, of “observation-orientation-decision-action”, as Baber, Harris & Stanton note in Modelling Command and Control – Event Analysis of Systematic Teamwork (2012, 16). The OODA loop can be regarded as a simplified version of Lawson's C2 model processes of sensing, processing, comparing, deciding, acting, and “provides a tactical-level perspective on Command and Control as a Process” (2012,16). Figure 10 below illustrates the individual but sequential ‘Observe’, ‘Orient’, ‘Decide’ and ‘Act’ processes working in sync with each other, the ideal order and state of decision making which represents the Command & Control (C2) process.

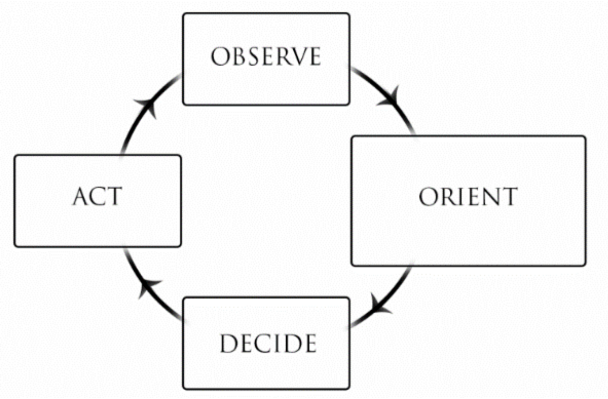


Figure 10: John Boyd’s OODA Loop (Krishnanand, 2018)

4.3 Deployable Communications Information Systems

Highly diverse with many operational capabilities is the concept of deployable communications and information systems (DCIS). They are robust, rapidly deployable information systems, designed significantly around the element of Command & Control, and can be deployed in any environment in which a peacekeeping organization may operate. This is why they are such an effective asset in peacekeeping operations in which command and control as well as communications capabilities may need operational readiness and to be fully effective within a short period of time, to meet operational needs anywhere in the world. Such technology is currently being used by the UN through the Modular Command Centre, and NATO through Airbus's Deployable Communications Information System (DCIS).

Deployable Communications Information Systems have the core purpose of communicating information. The British Armed Forces' BAE's FALCON system exemplifies this, providing a "secure internet for the battlespace linking service personnel at all levels of command" (BAE Systems). Communication is the core purpose of all DCISs. Because in the context of peacekeeping operations, the role of the information system is to support peacekeeping missions and operations through managing and communicating information. Between peacekeepers in the field, headquarters, and ground stations deployed in the operational environment, and other domains of the peacekeeping organization of which are connected to the same information system network and where command and control elements are present.

The three deployable communications information systems which will be analyzed in this paper are: the UN Modular Command Centre (UN MCC), the NATO Deployable Communications Information System (DCIS), and the British Armed Force's BAE FALCON. By and large, the three information systems are extremely similar, all functioning with a command and control component, largely achieved through WAN (Wide Area Network) and LAN (Local Area Network) connectivity. WAN and LAN capabilities are achieved in the systems primarily through standard internet protocol (IP) networks, which is particularly apparent in the BAE FALCON which almost exclusively relies upon this method of communication. Because during peacekeeping operations, internet access is perhaps the most integral part of the communications elements of an information system. As will be discussed, internet-based communications networks allow for real time information, also known as situational awareness, to be transmitted and received instantaneously between peacekeepers on the field, HQs stationed on the ground, and command and control elements within the organization at a remote location, such as the UNGSC, headquartered in Brindisi, Italy.

5 Deployable Communications Information Systems Analysis

With information security in consideration, this chapter will analyze three Deployable Communication & Information Systems (DCIS), namely the NATO Deployable Communication & Information System (DCIS), the United Nations Modular Command Centre (UN MCC) and the British Army's BAE FALCON. It will be determined how and what aspects of the DCISs contribute towards peacekeeper security, and whether they support Lawson's Model of Command and Control as well as John Boyd's OODA Loop. More so, however, the focus of the analyses will be of the administrative, technical, and physical information security controls of the three systems to ensure the Confidentiality, Integrity, Availability (CIA) of the information managed in the systems. The CIA triad analysis sections of the three individual DCIS analyses will determine how the information shared in these systems is protected, and therefore how the operational security that the systems contribute towards is maintained and not compromised.

5.1 UN Modular Command Centre

The UN Modular Command Centre (UN MCC) developed by the United Nations Global Service Centre (UNGSC), is the perfect embodiment of a Command and Control centre with C4 capabilities, demonstrating how the two work in accordance with each other. A 20ft converted sea container, its purpose is rapid deployment, to any location, allowing to support UN peacekeeping operations in hostile and remote locations, able to be fully installed and deployed within 5 hours. Its connectivity and communications come in the form of Data Voice, VTC, standard ICT configuration DFS 75 (connects up to 75 users).

Such communications technology enables clear and concise information sharing between commanders and peacekeepers in the field. Data Voice, VTC and DFS 75 are examples of how it is the communications technology aspect of an information system that is mainly responsible for achieving interoperability of a system, too. The technology allows commanders to instantly and seamlessly share real time information and logistics with each other and throughout the organization as well as connecting military, UN and civil communications systems, part of their larger information systems. The information and communications technologies provided by the UN GSC to support UN peacekeeping operations, is utilised by information systems such as the UN Modular Command Centre. The UN GSC is ISO14001 and ISO9001 certified, which is therefore an administrative control to the people who operate the UN MCC. This is an administrative control or the UN to ensure information security vulnerabilities are minimal.

5.1.1 Administrative Controls

The UN GSC trains all operators of UN MCCs to be proficient and knowledgeable in information security and cyber security practices. And overall information security awareness. Thus, decreasing the chances of information security incidents occurring due to human error and strengthening the overall information security of the UN MCC information system when it is being operated. However, a lot of the information relating to the specifics of how the UN and UN agencies like the UN GSC train their personnel in the field of information security, as well as using systems like the UN MCC, are classified and not publicly available. It is therefore hard to give a more in-depth analysis of this control category.

5.1.2 Technical Controls

Though the UN MCC is a fully functional DCIS, due its small scale and limited technological capacity in comparison to other systems such as the NATO DCIS, and its heavy reliance on UN GSC for communication support and resources, the information security measures of the UN GSC will be also be analyzed. These security measures are applicable to the UN MCC, too however, because a lot of the data that is transmitted from the UN MCC to the UN GSC headquarters, is operational information that may concern peacekeeper security. One of UN GSC's technical information controls is its firewall solution, achieved through Fortinet FortiGate 100D Firewall. A firewall is a network security device that monitors incoming and outgoing network traffic. In analyzing network traffic, a firewall can detect information security threats. This security feature contributes towards operational by ensuring the preventing any harmful threats from passing through the network and damaging information CIA, which could, in turn, deteriorate UN GSC service provision to UN MCCs, which affect peacekeeper security by directly affecting the ability of MCCs to monitor missions.

This information security measures of the UN GSC which processes information received from UN MCCs, contributes towards operational security of peacekeepers 'on the ground', because analysis of network traffic through a firewall enables the UN transmit information and support to connected MCC users, of which 75 can be connected at a given time, and "counter cyber security threats", as said in the educational video "UN GSC 2018" (2019), by the UN GSC. Countering cyber security threats helps to ensure mission critical support and information reaches UN stations in an operational environment.

5.1.3 Physical Controls

Regarding physical controls, the Modular Command Centre, although not the largest in terms of size, being fitted in a twenty square foot metal sea container, is perhaps the most physically and environmentally durable deployable communication information system, currently available. An environmental control is a form of physical control. The UN MCC's main environmental control is in the form of its hard and almost impenetrable steel exterior, ensuring the information system technology and assets housed inside are entirely protected from environmental threats. This tough UN MCC housing allows the UN to conduct peacekeeping operations all over the world, in some of the most extreme conditions, without information technology and information security being compromised.

The current MINURSO mission in the Western Sahara, for example, is one of such environments that has extreme conditions whereby extreme heat and dust poses a threat to information system technology and assets. Figure 11 below, depicts typical air conditioning systems that keep UN MCCs ventilated. All UN MCCs are equipped with air conditioning systems to ensure they do not overheat and the functionality of information technology and their ability to execute tasks which ensure security during UN peacekeeping operations, is maintained.

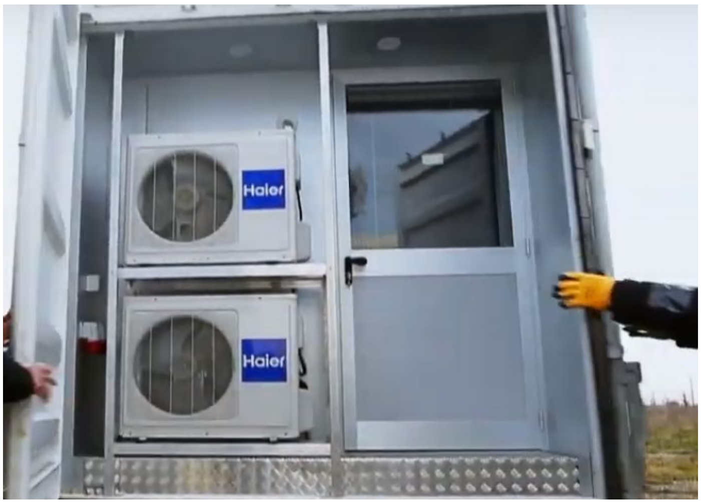


Figure 11: United Nations Modular Command Centre Air Conditioning Unit (United Nations Global Service Centre, 2017)

5.2 NATO Deployable Communications Information System

The NATO DCIS is an information system for "providing managed information and communication services within and between deployed command and control elements, reach back to strategic networks", as said in the educational video “Deployable Communication Information System (DCIS)” (2014) by Airbus Defence and Space. The system can achieve connectivity between HQ can “using multiple SATCOM, radio, fibre, or locally available public telecoms bearers"(DCIS 2014). Methods of these types of connectivity include “telephony, video and data application services over a common IP network.”(DCIS 2014) The system provides "operational intelligence, situational awareness, operational planning and analysis, reporting and tasking, logistics, geographic information, modelling and simulation and collaboration tools"(DCIS 2014), all of which, especially OPINTEL and SA, are useful in providing creating an accurate picture about an operational environment and the threats it may contain, which can be used to plan and navigate operations in a way that mitigates the chance of peacekeeper safety being compromised by threats.

One of the ways this can be achieved through compiling the different types of information listed above, is by creating a Common Operational Picture (COP). A COP is “a single identical display of relevant information shared by more than one command (that) facilitates collaborative planning and assists all echelons to achieve situational awareness", as defined in the Department of Defence Dictionary of Military and Associated Terms (2001). Figure 12 below illustrates the outer structure of the easily and quickly deployable tents used to house the DCIS, while Figure 13 illustrates an inside operating area of NATO DCIS.

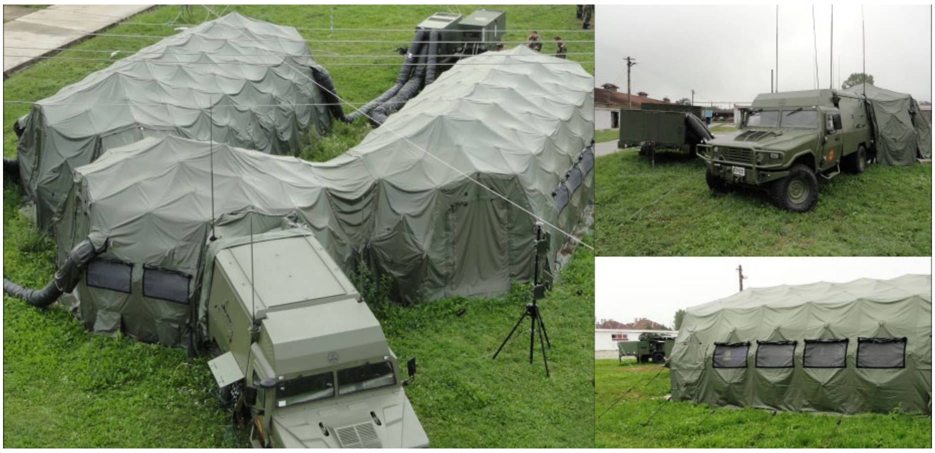


Figure 12: North Atlantic Treaty Organization Deployable Communication & Information System (Interactive Systems & Business Consulting)

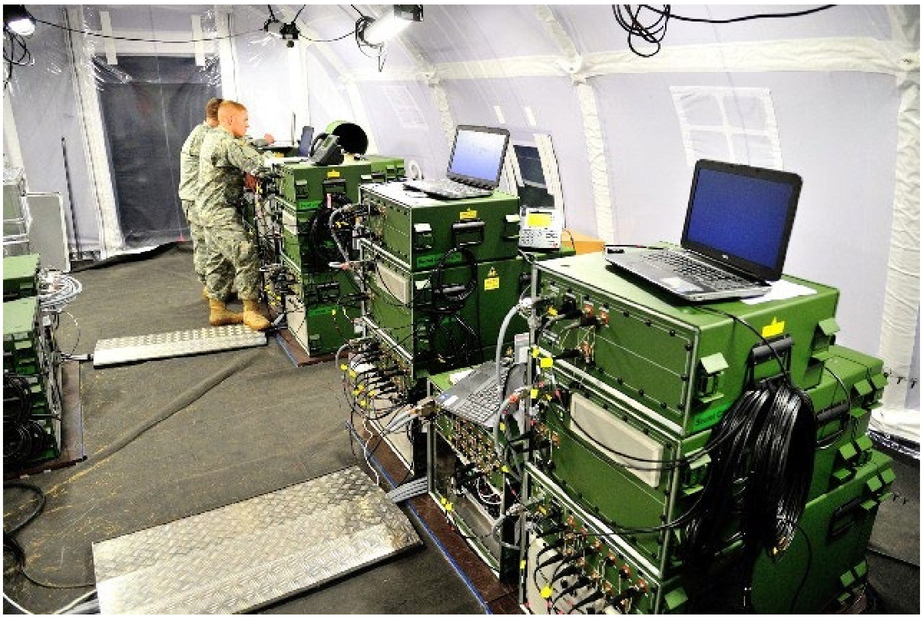


Figure 13: Operating Equipment Inside North Atlantic Treaty Organization Deployable Communication & Information System (Defense News, 2014)

The ability to decide upon and alternate the fastest networks at a given time in a given location, greatly enhances operational and personnel security, because the speed of which data can be received and transmitted between the DCIS and other HQs or peacekeepers in the field, greatly affects the quality of the information that is received by the user of whom the information has been transmitted. In the context of a peacekeeping operation, high quality and useful information is information that can be defined as ‘real time’ or situational awareness. This type of information allows commanders to make decisions while situations unfold, which are therefore more accurate decisions which can better protect the safety and security of the soldiers.

5.2.1 Information Security Measures & Controls

Regarding the information security measures of NATO’s DCIS, it has robust administrative, technical, and physical information security controls which help ensure the DCIS manages, is secure and protected against information security threats and vulnerabilities. The information security controls of the NATO DCIS which will be discussed below, are an integral part of the system to ensure information is not compromised, as well as continuity of the information system’s functions, and therefore maintenance of the operational security these functions create, too.

5.2.2 Administrative Controls

A key theme of deployable information systems, much like NATO’s DCIS, is that they require minimal training on behalf of the personnel who operate them. In accordance with the nature and purpose of administrative information security controls, minimal training, and ease of use of an information system lessens the chances of information security incidents occurring due to human error. When a system like the NATO DCIS is easy to use by NATO personnel, it means the chances of human error caused by mistakes when using one of the five components of an information system, as a consequence of having sufficient knowledge of how to use it, are significantly reduced.

This is a crucial benefit, because if personnel do not have a sufficient understanding of how to use one of the five components of the DCIS, such as the computer software component of the system, which can often be the most difficult component of the system to fully understand and correctly learn how to use, the consequential increased likelihood of human error, can cause negative consequences to both the information security of the information system, and therefore also jeopardise the operational security that the NATO DCIS creates for the NATO peacekeepers who are dependent on it for their operational security and safety.

One of the key reasons as to why information security incidents caused by human error can negatively affect information security and operational security, is because, depending on the type and severity of the information security incident that has occurred, the entire efficiency of the information system can be affected. Because, when information security incidents occur through incorrect use of one of the five information system components, due to human error, the five functions of the system which are interconnected to the five components the information system are also negatively affected.

And if the efficiency of a system to execute its functions, such as data output, is not as efficient as it is supposed to be, the roles of the information system, such as the communication of information – one of the most crucial elements of an information system in creating operational security during peacekeeping operations, could be jeopardised. In this event, situational awareness data may not be able to be transmitted from peacekeepers to HQ in a volatile situation, or vice versa. And the command and control elements of the system would not possess the required information to make decisions which affect the lives and safety of peacekeepers – which is detrimental to the security of the peacekeepers in the field. Another example is if a skill-based error occurred because a user made small but consistent mistakes in using software of the system, an information security incident could occur through sensitive information unintentionally being sent to unintended recipients. This same scenario could also occur because of a decision based-error – which is also more likely to occur when a system is more complex.

To conclude the NATO DCIS information security control of ease of use of the system, the administrative control of minimal training required to operate the system, significantly reduces the likelihood of information security incidents occurring because of human error. And therefore, the overall information security of the information system is enhanced, in turn enhancing the operational and personnel security of the peacekeepers who are dependent on the DCIS to share and receive mission critical information, by ensuring continuity and efficiency of the DCIS in executing its functions that enable users to share and receive information.

5.2.3 Technical Controls

A technical control of the NATO DCIS that affects operational and personnel security rather than information security, is the DCIS's throughput interface and monitoring system. Basically defined, throughput, in the context of the communications networks of the DCIS, as written in the article Bandwidth Vs Throughput (2014) by Jartinez Boston, published on AvaLAN Wireless, is the "rate of successful message delivery over a communication channel". Throughput is usually measured in bits per second (bit/s) or bps. A throughput interface allows NATO personnel to monitor the performance and speed of their communications networks within the DCIS. This feature enables DCIS users to decide which network or data transmission method to be used as the fastest and most effective way of transmitting and receiving date to the different HQs and to peacekeepers in the field. If the throughput interface of the DCIS showed a communications network is slow, an alternative means of communication could be found.

Another technical control of the NATO DCIS that enhances information security, is network layer cryptography. Network cryptography is the "conversion of data into a secret code for transmission over a public network", as defined in the encyclopaedia section of the PC MAG website. Cryptography when referring to presence of third parties in the context of peacekeeping, can be referred to as adversaries. This means that information being transmitted by the DCIS over a public network is encrypted and more difficult to be intercepted by unintended recipients who also may be on the network, which one of the information securities threats of sending information over a public network.

In the event situational awareness data was being inputted into the DCIS for transmission during a peacekeeping operation, for example, on the CAVNET network which was an IED situational awareness network used by peacekeeping organizations in Afghanistan, network layer cryptography would minimise the risk of the sensitive information that is shared on the network being intercepted by the Taliban or other hostile forces. Sensitive information could include the location of a friendly patrol, and if this information was intercepted by enemy forces, the operational security of the peacekeepers would be jeopardised because they would be vulnerable to an ambush, among many other possible security threats.

5.2.4 Physical Controls

The following physical controls of the NATO DCIS are not strictly information security controls, rather information technology controls. Because they relate to physical security measures that directly protect the IT equipment of the NATO DCIS, unlike traditional physical information security controls which mainly revolve around facility protection and security, such as facility protection and intrusion monitoring. Because of the relatively small and portable natures of deployable communications information systems, however, these physical information security controls are not entirely relevant for the NATO DCIS.

Therefore, the following physical controls which will be referred to in the NATO DCIS analysis, as well as for the other information systems to be analyzed in this paper, will relate to IT security, rather than directly to information security. It could be argued, however, that IT security, is in-fact in interconnected to information security, because of the information security practice of information assurance comprising of three components – confidentiality, integrity, availability. Both the integrity and availability aspects of the information security practice of information assurance could be compromised if IT security is compromised, which is why it can be argued there is an interconnected dependency of functionality between IT security and information security. Because, if the physical security of IT equipment is compromised, the functionality of that IT equipment, and therefore the integrity of the data it may be storing could be compromised, for example, by being corrupted.

And the availability of information of which a given piece of IT equipment may be responsible for managing, could also be compromised. Therefore, throughout the following information systems analyses, physical IT security controls, while not officially being defined in information security literature as information security controls, will be used interchangeably as information security controls, too. Regarding the physical controls of the NATO DCIS which ensure the integrity of DCIS IT equipment, and therefore information security, is the ruggedness and toughness design of the equipment. Deployable communications information systems like the DCIS must be capable of operating in any terrain and in extremely harsh environments which is why the IT equipment of such information systems, and the various information system components, particularly the system hardware, must durable enough to be transported in such environments without being physical compromised by physical or environmental conditions.

To ensure this, the NATO DCIS has an operating range of between "-30 and +49 degrees Celsius" (DCIS 2014), meaning the systems can function at almost any environment in which humans are likely to operate, and continuity of information will not be compromised. Additionally, as the standard external structure that all DCIS systems are packaged with, the DCIS uses a biological and chemical proof" (DCIS 2014) tented environment, which forms the external and protectoral structure of the system. A "building of opportunity" (DCIS 2014) can also be used to house the DCIS, if for some reason during an operation, was to become more desirable to house the DCIS, providing further opportunities for physical protection. The equipment that forms the DCIS, is transported in portable, ruggedized cases "to ensure survivability of equipment in the most extreme environmental conditions" (DCIS 2014).

5.3 BAE FALCON

The BAE FALCON, used by the British Armed Forces, by and large, is very similar to the NATO DCIS, also providing "operational intelligence, situational awareness, operational planning and analysis, reporting and tasking, logistics, geographic information, modelling and simulation and collaboration tools" (DCIS 2014). While also similar the UN MCC, too, though differing in scale and layout. Regardless of the degree of similarity between the FAALCON and the previous to DCISs, the FALCON continues the notion shared by all three of the systems, that the communications aspect of information systems, in the form of situational awareness and command and control, is the main way information systems contribute to peacekeeper security. As is evident by the fact that the first key point on the BAE FALCON Fact Sheet is that the system "provides a secure internet for the battlespace, linking service personnel at all levels of command" (BAE Systems).

Because of the hierarchical structure of the British Army, and the strong reliance on a hierarchical organizational command and control structure, as with all Armed Forces, FALCON's interoperability is achieved through the ability to serve as a "communication hub, linking nearly a hundred separate headquarters together"(BAE Systems). Figure 14 illustrates how this is achieved through creating both a Wide Area Network (WAN) and Local Area Network (LAN) "Falcon provides both a local area system, within the Command Post for example, and wide area systems which can, if required provide a secure link back to the UK", as mentioned on the BAE FALCON Infographic (BAE Systems).

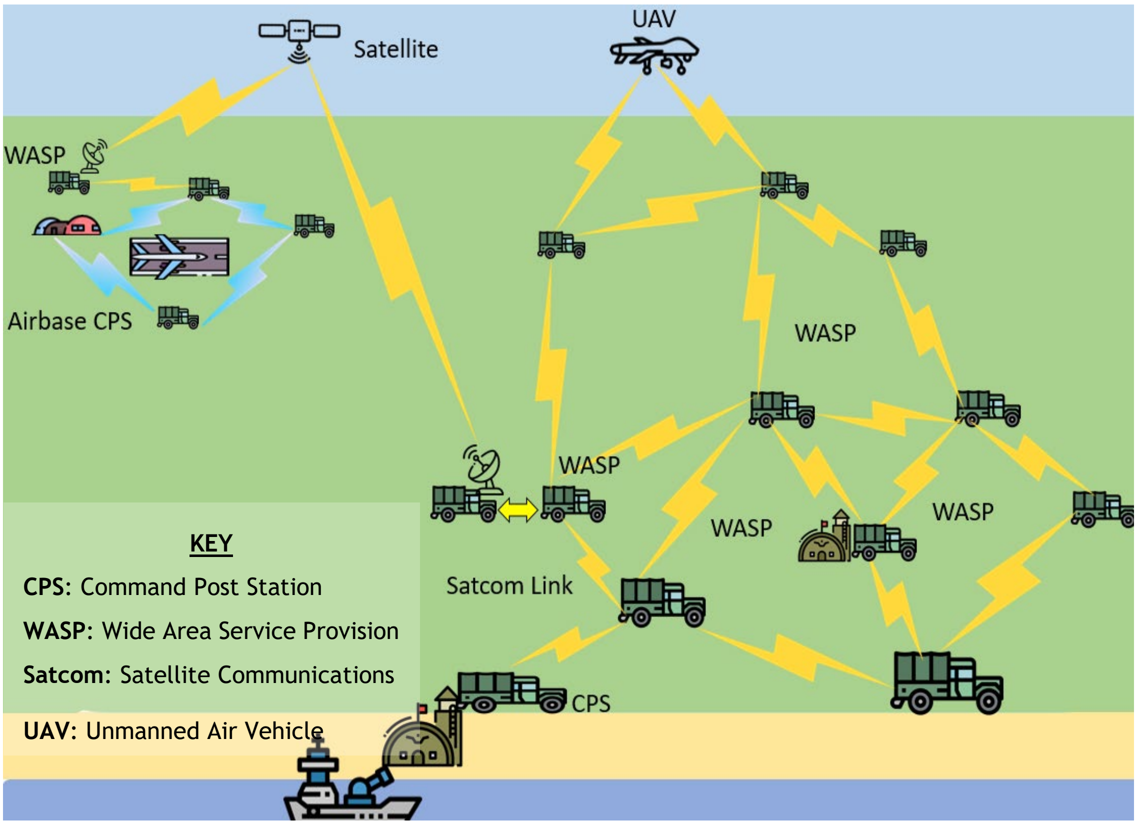
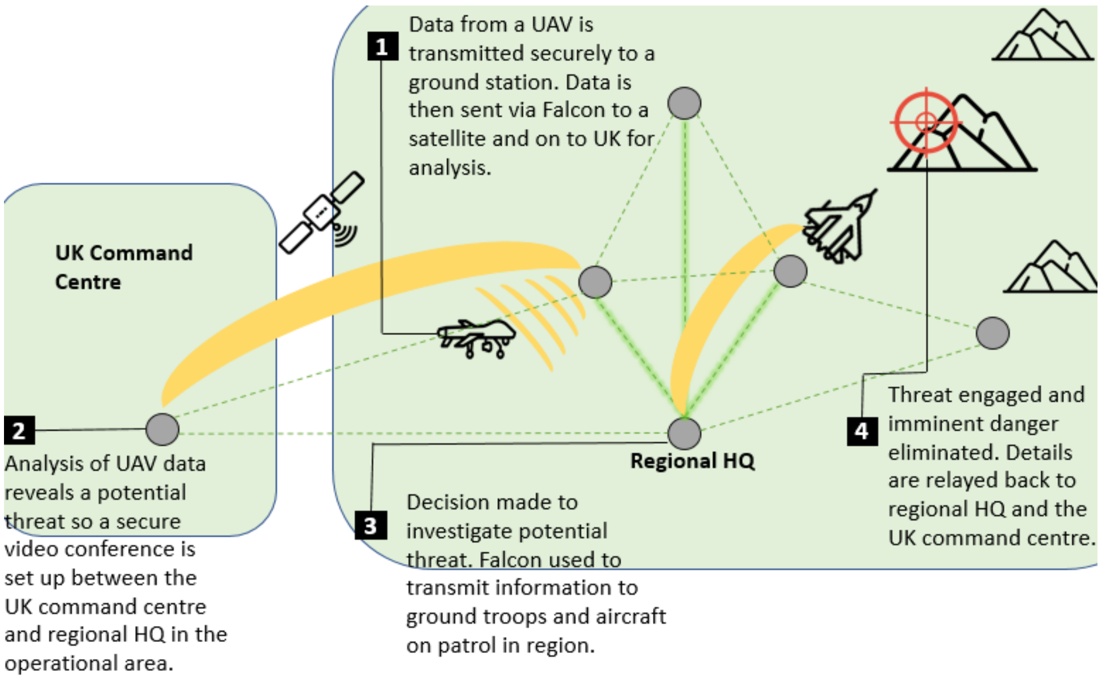

Satellite
UAV
WASP
Airbase CPS
WASP
WASP
WASP
WASP
WASP
KEY
CPS: Command Post Station
WASP: Wide Area Service Provision
Satcom: Satellite Communications
UAV: Unmanned Air Vehicle
Satcom Link
CPS

Figure 14: BAE FALCON Wide Area Network and Local Area Network Service Provision (BAE Systems 2011, 4)

Despite the ability to create such a large and connected communications network, FALCON maintains an effective degree of information security, as "FALCON handles four different levels of information securely" from “restricted” through to “secret”, as according to the BAE Systems official FALCON Fact Sheet. Ensuring only people with an authorisation that matches the security classification of information, can access it. Therefore, decreasing the chances of information security breaches, which could impact the security of peacekeepers. In additional to internal operability of the system which ensures an entire organization is connected with eachother during operations, FALCON provides external interoperability with other organizations to, meaning that in joint peacekeeping operations, “data and video information can be shared securely between Coalition partners” (BAE Systems).

Regarding how the communications and internet capabilities which contribute towards operational and personnel security of peacekeepers, are achieved, in the BAE FALCON, it is the ability of the system to manage and transmit large amounts of data from different sources, simultaneously, and almost instantaneously, at both a local scale and global scale. This ensures that the BAE FALCON is capable of receiving, storing, processing, managing and sharing all mission-critical information, (the most useful of which being in the form of situational awareness) ensuring that command and control elements of the BAE FALCON can act upon that information accordingly, as illustrated in Lawson's Model of Command & Control. To ensure operational and personnel security of peacekeepers. Because if there was a limit to the amount of data the system could process, this could limit the ability of commanders in the organization to make decisions that keep peacekeepers safe.

To capably and effectively transmit large amounts of data, the system relies up the use of advanced internet protocol networks (IP networks) that enables data and situational awareness information to be communicated throughout the global and interoperable FALCON system. Similarly, and equally important in allowing data not only to be sent, but received by different HQs and ground stations, is again the point that all the technological and communications components of the system are connected, forming one big communications network. The "linking service personnel at all levels of command" (BAE Systems) aspect of the FALCON's internet capabilities being the result, as according to the FALCON Fact Sheet. Figure 15 below depicts how this is achieved through data transmission and large-scale connectivity by providing both a "local area system" and "wide area systems which can, if required, provide a secure link back to the UK" (BAE Systems), as according to the official FALCON Infographic.



1 Data from a UAV is transmitted securely to a ground station. Data is then sent via Falcon to a satellite and on to UK for analysis.

2 Analysis of UAV data reveals a potential threat so a secure video conference is set up between the UK command centre and regional HQ in the operational area.

3 Decision made to investigate potential threat. Falcon used to transmit information to ground troops and aircraft on patrol in region.

4 Threat engaged and imminent danger eliminated. Details are relayed back to regional HQ and the UK command centre.

Figure 15: BAE FALCON Information Sharing and Command & Control Process (BAE Systems)

In the BAE FALCON information sharing process, which relies upon a network of hardware interconnected to the BAE FALCON communications network infrastructure, as depicted in the above Figure 15. The first stage in the transmissions is that "data from an Unmanned Air Vehicle (UAV) is securely transmitted to a ground station" (BAE Systems). UAVs are satellites in space which have a bird's eye view of the environment peacekeepers and friendly are operating in. UAV's are therefore capable of capturing and potential threats in that environment through advanced cameras. The data from these cameras is then transmitted to a ground station in the operational environment where FALCON information system infrastructure is deployed. This data can then be relayed via satellite to a UK command centre, for analysis.

When data is analyzed during a peacekeeping operation at the UK command centre, the UAV data may "reveal a potential threat to coalition forces" (BAE Systems). In this scenario, the FALCON information system can further be utilised in enabling command and control users of the system to create "a secure video conference" (BAE Systems) between UK command centre and regional HQ in the operational area. The commander in the operational area who receives the situational awareness through video conference or through another means of communication, then can decide to investigate the observed threat. If the decision is made to investigate the observed threat: "FALCON transmits vital information to ground troops and aircraft on patrol in the region" (BAE Systems). The threat can then be engaged, and danger can be eliminated, removing the threat to peacekeepers. For example, an insurgent, who could kill or injure a peacekeeper and also jeopardise security and continuity of the peacekeeping mission. When the threat has been engaged, a situational report can then be relayed back to Regional HQ and then the UK Command Centre. All of the communication processes and transmission of information and data which sequentially occurs throughout the various stages of this monitoring, detection, and transmission processes, as illustrated in the above Figure 16, is able to happen because each technological component that receives information is interoperable and connected to the overall BAE FALCON information system.

In conclusion, BAE FALCON contributes to operational and personnel security largely through its advanced, global monitoring and information sharing information abilities enabling command and control elements to effectively make decisions based on situational awareness. These decisions from command which can be globally communicated throughout the organization, through transmitting data to ground stations, enables action to be taken and threats to be engaged, which ensure personnel and operational security and safety.

5.3.1 Administrative Controls

Regarding the administrative information security controls of the BAE FALCON, the British Army personnel who operate the BAE FALCON, abide by strict information security standards and procedures. These procedures govern how information is handled in the information system. Information handling refers to the classification of information, disposal of information, removal of information, storage of data and exchange of information.

In the BAE FALCON, one of the most important security aspects of information handling procedures, is the classification of information. Because once information has been given a level of security classification, users of the BAE FALCON can correctly exchange the information throughout the system and minimise the chance of information security incidents. The classification of information applies to all information received from the various communication entities connected to the FALCON infrastructure, such as satellites, computers, and radios, which is to be communicated to through the FALCON information system.

For example, similarly to how, in compliance with British Armed Forces information security procedures, “information is securely exchanged from UNCLASSIFIED up to SECRET”, as mentioned in the official 2011 FALCON Brochure. And the management and monitoring of the FALCON network, which is an administrative control in and of itself, further reflects the importance of information classification, as again “access and control will depend upon a network manager’s level of permissions and authority” (BAE Systems 2011). Ensuring only the right personnel have access permissions on a network, is a vital information security control to protect information, because network managers have arguably the most power and control over a network.

The classification of information is an information security measure that protects sensitive information. And depending on the level of classification of which certain sensitive information has been given, the appropriate access restrictions can be implemented to ensure the information is exchanged by the appropriate methods, and to ensure that it is to be accessed only by people in the organization who have at least the same level of security clearance as the information that is being handled. For example, if information under the classification of SECRET was exchanged to another domain within FALCON information system, only people with the correct security clearance would be able to view that information.

Security classification is an effective information security measure in the BAE FALCON because minimises the chances of information leaks or breaches of sensitive information by implementing access controls and restrictions relevant to the security classification of the information. When information is restricted, it ensures operational security and security of Armed Forces personnel. By ensuring mission sensitive information that could concern their safety, is at minimal vulnerability to information security threats which could lead to the information being received by unintended recipients.

In addition to information classification, facilities that are connected to the BAE FALCON are bound by security classifications whereby “each working area within the HQ can operate at its own security level, depending on the nationality and security clearance of the staff that have access to a particular area” (BAE SYSTEMS 2011). Meaning that facilities can only store information matching the classification level the facility is carrying, and only people with at least the same security clearance allowed to access the facility which stores the information. Again, this minimises the chances of unintended recipients viewing the information.

5.3.2 Technical Controls

As a system that effectively but almost exclusively relies on IP networks to share and receive information, one of the most important technical controls of the BAE FALCON’s IP network, is the splitting of transmitted data. A given amount of data shared in the FALCON network, at a given time, known as ‘traffic’, is “split into small packets” (BAE Systems 2011). Each packet, will then individually, but simultaneously go through the network to securely reach the destination, as “FALCON automatically decides the route along which the message should be sent” (BAE Systems 2011). What makes the FALCON’s data splitting method even more effective in ensuring security and CIA of information, however, is the fact that FALCON automatically reacts to loss of network nodes (the connection points in a communications network where data is received, stored, and distributed along routes of a network), that may result from “enemy EW (Electronic Warfare), destruction of FALCON assets and the disruption caused when FALCON assets have to re-deploy in order to support manoeuvring troops” (BAE Systems 2011).

Electronic warfare, both offensive and defensive, is the ability of forces to use the electromagnetic spectrum (signals including “radio, infrared or radar”) to gain the advantage in conflict. There are various was to conduct electronic warfare. As written by Don E. Gordon in Electronic Warfare (1981), methods include the use of signals as a means of “intercepting, locating, identifying, detecting, jamming, disrupting, deceiving, protecting, analyzing, and cryptanalyzing”. While it is less likely that adversary forces, which may be present in an area would have the technological capabilities of conducting such warfare to an effective degree again large-scale and technologically advanced C4I information system like the BAE FALCON, the above mentioned threats are nevertheless still very real threats that information systems like the FALCON must be protected against. And FALCON’s ability to react to node losses that may occur from the possibility of EW, is an effective way of doing so.

Referring back to the main point of the FALCON achieving network traffic security, and the secure transmission of information, through data splitting, the reason is because data packets are more “resilient to destruction of parts of the network from hostile electronic and physical attack” (BAE Systems 2011). Again, enforcing the effectiveness of data splitting as a technical control which protects the FALCON’s data and assets, and ensures the CIA of information. Data splitting works effectively, because at the data's destination, "the packets are reassembled into their original form at the receiving end" (BAE Systems 2011).

The technical control of data splitting, although differing in method, is similar to the NATO DCIS network layer cryptography method of encrypting data. In that they both have the same effect on the data that is being transmitted – data being transmitted on a network is re-arranged into a form that is indecipherable to unintended network users. Who may try and launch an electronic attack to intercept the data, between the points of information being transmitted from one domain to another within the information system.

5.3.3 Physical Controls

As a rugged and durable DCIS, designed to operate in all environments and be protected against the various kind of threats that may be present in a peacekeeping environment, the NATO DCIS is also equipped with similar physical controls to those of the UN MCC and the NATO DCIS. Such as rugged equipment cases and diverse operating temperatures. As the BAE FALCON is primarily a communications system, primarily relying on internet, largely through the "Bowman Combat Net Radio system and the Skynet SATCOM system" (BAE Systems 2011). The physical protection measures of the equipment that forms these systems, are achieved largely through the exterior structure that houses the equipment, as is the case with the 20-foot steel sea container exterior of the UN MCC, or the biological and chemical proof tent of the NATO DCIS.

In the case of the BAE FALCON, where the equipment that forms the network of the system is used primarily in "WASP" (BAE Systems 2011) (Wide Area Service Provision) vehicles, through the "Trunk Communications System" (BAE Systems 2011), each WASP vehicle has a "container within which the FALCON equipment is operated" (BAE Systems 2011).Figure 16 below from the official BAE Falcon Overview document (BAE Systems 2011) below, illustrates the MAN HX60 (left) used as the standard WASP vehicle in the FALCON WAS, and the FALCON communications radio (right), operated in the container seen at the rear of the MAN HX60. The combination of the physical protection offered by both the communications equipment, and containers of which the equipment is housed, create one very strong physical control, although it is the MAN HX60 vehicles themselves and the containers of which the trunk communications system is housed, that offers the most physical protection.

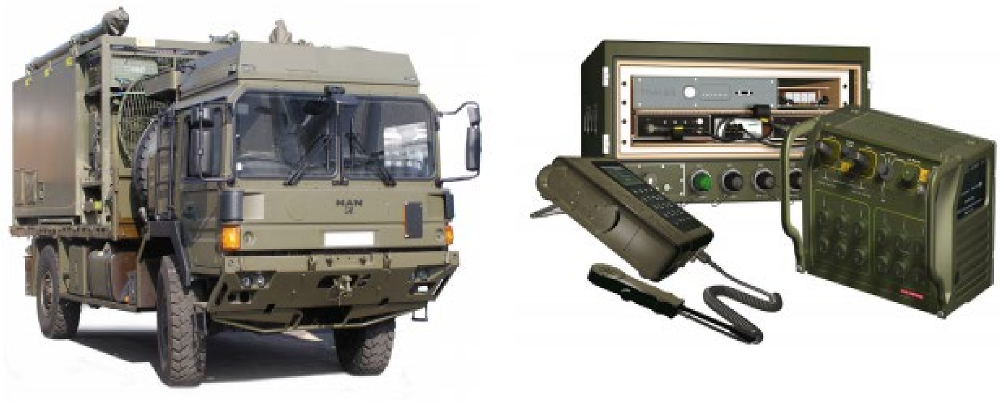


Figure 16: BAE FALCON Trunk Communications System (BAE Systems 2011, 5)

Of course, the equipment that forms the BAE FALCON system, such as radio headsets and laptops, as with the previous two information systems, are extremely tough and durable, like the rugged Dell laptops used in the NATO DCIS. However, the equipment itself cannot match the toughness of the British Army's military-grade trucks that house the FALCON Trunk Communications System - the MAN HX60. The MAN HX60 is armoured with steel and is extremely tough. It is also fitted with "a blast-proof vertical-split-windscreen", as written by The New Haysalian Military. This blast proof windscreen can protect against small-arms fire and explosions, both of which are the most common threats to peacekeepers today and encountered frequently during peacekeeping operations, as has already been mentioned in referencing the report Improving Security of United Nations Peacekeepers (Cruz, Phillips, Cusimano 2017), Chapter 2.2.2 of this thesis, 'Peacekeeping Threats' .

The physical protection measures of the MAN HX60, such as the blast-proof windscreen, although the British Army is not currently directly using it on any of the high IED risk peacekeeping operations it is attached to, is nevertheless still extremely relevant if the British Army was to employ use of the vehicle in any future conflicts areas. Because as is the case in certain peacekeeping missions such as the United Nations Multidimensional Integrated Stabilization Mission in Mali (MINUSMA), IEDs pose a significantly higher risk to peacekeeper than in others, and casualties from IEDs are increasing, as previously mentioned in Chapter 2.2.2 of this thesis, 'Peacekeeping Threats', where the UN Secretary General in the December 2018 MISNMA accounts the significant and increasing threat of IEDs in Mali. An increasing threat of IEDs has also been seen in other missions in different parts of the world too, though so physical protection measures of information systems such as the MAN HX60 blast-proof windscreen are highly relevant and needed.

Regarding the BAE FALCON's Wide Area System (WAS), it is achieved, among other entities connected to the BAE FALCON including UAVs and satellites, primarily through many deployed MAN HX60 vehicles. Each connected to the BAE FALCON through the trunk communications system it contains. The fact that the ruggedized, durable, steel plated MAN HX60 comprises the bulk of the BAE FALCON's physical infrastructure for which the communications technology is contained, is a physical control in and of itself. Because it ensures that the entire portion of the system which is deployed outside of operational HQs, remotely, in 'the field', and is therefore most likely to succumb to threats present in operational environments during peacekeeping operations, has adequate protection. Therefore, contributing towards continuity of communications, which in turn contributes towards the security of peacekeepers. Because the MAN HX60 which houses the communications equipment of the BAE FALCON, is adequately equipped to deal with some of the most dangerous threats present in today's peacekeeping environment – explosions and small arms fire.

6 Conclusions

There is no doubt that peacekeeping organizations heavily rely on information systems during operations as a means of enacting peacekeeper security. Before concluding how and why information systems contribute towards peacekeepers security, it must be first concluded that communications networks, while designed primarily for the purpose of sharing information, are as effective in sharing situational awareness and ensuring peacekeeper security. Even if the network is acting independently and not interconnected to a larger information system such as the BAE FALCON.

Regarding the analyzed DCISs, it is clear that their administrative, technical, and physical controls protect them against information security, respectively. Allowing the peacekeepers who depend on these systems to conduct peacekeeping operations as safely and securely as possible. While peacekeepers rely on the communications aspect of the information systems, they use on operations to enhance their safety and security, they rely equally upon the information security measures of their information systems too. If the information security of an information system is compromised, the security of peacekeepers may also be compromised.

To minimise information security incidents occurring in the information systems of peacekeeping organizations, this paper has shown that administrative controls must be such that an information system is easy and simple to use, yet still be security-tight and possess a wide range of communication and information management functions that enable the personnel operating the system to oversee all aspects of peacekeeping operations to protect peacekeepers. Without going into depth in analyzing the most important DCIS technical controls, it is apparent that they are crucial in ensuring continuity of a system and CIA of information, preventing information security breaches, which could compromise information CIA. The information processed in an information system during a peacekeeping operation is mission sensitive and could be directly related to mission objectives and therefore the peacekeeper's safety. Therefore, one could argue that technical controls are the most important control of an information system in ensuring physical security of peacekeepers. The physical controls of the DCISs analyzed in this paper reflect the diverse and often harsh and remote environments in which peacekeeping organizations operate. The physical controls of DCISs ensure that the systems can operate to the same standard, anywhere in the world, and in any environment that a peacekeeping organization may operate. This ensures that peacekeepers will always receive the same level of security and protection from the information systems they depend on.

While there are differences between the UN MCC, NATO DCIS, and BAE FALCON DCISs analyzed in this paper, in terms of factors such as size, scalability, technological infrastructure, security controls etc, it has also been made clear, that there are certain similarities between them. One thing that has been made noticeably clear, is that the key underlying theme of all the systems, and of future DCISs to come, is the communications aspect. Again, while there are various, albeit fairly slight differences relatively speaking and considering the fact the focus of the DCIS analysis in this paper has primarily been about how the functions of DCISs contribute towards peacekeeper security, it is the communications function of the DCISs which are share a common purpose between the systems. The communications function, although also differing between the three systems in terms of the exact technology and methods for executing it, shares the same purpose of contributing towards peacekeeper security.

As it has been made apparent not only in chapter five, but also in chapters two and three, constant communications and a constant flow of information between peacekeepers on the field and operational HQs is required. Again, reflecting the similarity of the communications function between the UN MCC, NATO DCIS, and BAE FALCON, the form of communications that is required, and the form of communications that the three systems deliver, is operational intelligence and situational awareness. Crucially, so that C2 elements can analyze the data they receive, and act upon it accordingly, making accurate and informed decisions to mitigate threats present to peacekeepers, thus providing them security. Because of this, as well as the harsh and remote environments in which peacekeepers operate, DCISs are the most effective type of information system to peacekeeping organizations. This is because they are an easily transportable and quickly deployable command and control element, managing and communicating information between peacekeepers on the field and fixed headquarters.

In concluding the factors of Deployable Communication Information Systems that contribute to peacekeeper security, it is the combination of DCISs being robust, security tight and deployable enough, to act as a medium of which operational intelligence and situational awareness flows between operational environments and HQs, to be processed and acted upon by a command and control element, in any environment a peacekeeping organization will operate, which is the overall way in which information systems used by peacekeeping organizations contribute towards peacekeeper security.

In addition to obtaining operational intelligence through sampling and field assessments, allowing logistical preparedness to reduce casualties due to poor equipment, the process of information systems obtaining intelligence and situational awareness that can be translated into situational understanding, is perhaps the single most important process that occurs in an information system during peacekeeping operations to enhance peacekeeper security. So that Command and Control (C2) elements can act accordingly in making decisions and issuing commands that avert peacekeeper patrols from threats in operational environments. All being achieved, through the key enabler of interoperability in allowing information flow between an operational environment and Command and Control (C2) elements, as well as with other organizations on joint operations, so a constant state of situational awareness is maintained to prevent inaccurate information or lack of information. Which can occur when stakeholders in an operation do not have access to information due to lack of interoperability.

Table 1 below represents the sequential stages of this information sharing process used by information systems to enhance peacekeeper security. While the graph following afterwards, concludes the necessary information security controls needed to maintain Confidentiality, Integrity and Availability (CIA) of the information in information systems. It is the information security controls of the systems that not only ensure information CIA, but also continuity of the crucial process of intelligence and situational awareness being shared throughout information systems and therefore the ability to provide peacekeeper security. Because information CIA contributes to the continuity of the information systems themselves.

Both Table 1 and Table 2, conclude the findings of this thesis in answering the two research questions of this thesis: ‘how, do information systems used in peacekeeping operations contribute to peacekeeper security ?’, and ‘how does information security, information CIA, and its relationship with information systems affect peacekeeper security?’. Because, when information systems and information security are used in effectively in combination, utilising Interoperability and Command & Control, they are the two key enablers and contributors to peacekeeper security.

Table 1: How Information Systems Contribute to Peacekeeper Security

Sequence	Information Processes	Methods	Contributions to Peacekeeper Security
1	**Threat Detection & Identification**	• High zoom, high resolution imagery (Satellites, UAVs) • Surveillance equipment (CCTVs, motion sensors) • Visually by peacekeeper patrols • Field Assessments & Sampling: - High zoom, high resolution imagery (Satellites, UAVs) - Demographical data collection	• Peacekeeper patrols and Command & Control elements can avert threats and coordinate a plan to neutralize threats such as Improvised Explosive Devices (IEDs) - **Mitigates chance of peacekeeper patrols succumbing to surprise enemy attacks**
2	**Interoperable Communication: Situational Awareness**	• Deployable Communication Information Systems (DCIS) • Portable communications Devices: radios etc. • Satellite communication (SATCOM) • Wide Area Network (WAN) & Local Area (LAN) Internet Protocol (IP) networks • IP networks: both Wide Area Network (WAN) and Local Area Network (LAN) • Communication networks e.g. CAVNET	• **Situational Awareness** shared in an **interoperable** information system ensures: all stakeholders in a peacekeeping operation are aware of potential threats in an operational environment - M**itigates risk of peacekeeper patrols succumbing to threats**
3	**Command & Control (C2): Situational Understanding**	• Analysis of **Situational Awareness** data through data analysis tools to create **Situational Understanding** •Course of action decided from **Situational Understanding** through comparing current environmental state with desired environmental state (Lawson's Model of Command & Control)	•**Situation Understanding** ensures Command & Control (C2) make accurate and informed decisions, translating into accurate and informed orders - **Mitigates risk of peacekeeper patrols succumbing to threats through misinformation, inaccurate information, which could lead to poor decisions**
4	**Command & Control (C2): Orders**	• **Situational Understanding** acted upon: Command & Control (C2) issues orders to a peacekeeper patrol(s) - Video conference - Telephone call	• Strategic and operational decisions that **neutralize or mitigate threats** to peacekeepers in an operational environment issued from Command & Control elements

Table 2: Information Security Controls of Information Systems

Information Security Controls	Methods	Contribution to Confidentiality, Integrity, Availability (CIA) of Information
Administrative	• Security classification and tiers e.g. unrestricted through to top secret, • Access controls to facilities, • Personnel training to operate Information System components such as monitoring or Command & Control centres	Mitigates risk of CIA compromise of information from **human error**
Technical	• Authentication solutions •Firewalls •Antivirus software •Data cryptography	Mitigates risk of CIA compromise of information from **cyber threats**
Physical	• **Physical Access & Surveillance Controls:** area security clearances, fences, gates, guards, security lighting, surveillance equipment (CCTVs, motion sensors) • **Environmental Controls:** e.g. Humidity Ventilation Air Conditioning (HVAC) • **Equipment Protection:** e.g. temperature and weather durability, physical toughness and durability	Mitigates risk of CIA compromise of information from physical threats to **tangible data assets**

References

Printed sources

Agre, J., Vassiliou, M., Alberts, D. 2014. C2 Re-envisioned: The Future of the Enterprise CRC Press.

Baber, C., Harris, D., Stanton, N. 2012. Modelling Command and Control: Event Analysis of Systematic Teamwork. Ashgate Publishing Ltd.

Black, J. 2006. A Military History of Britain: From 1775 to the Present. Praeger Publishers Inc.

Bourgeois, D.T. 2014. Information Systems for Business and Beyond. Saylor Foundation.

Builder, C.H., Bankes, S.C, Nordin, R. 1999. Command Concepts. Rand Publishing.

Cruz, C.A. & Phillips, W.R. 2017. Improving Security of United Nations Peacekeepers: We need to change the way we are doing business. United Nations.

Department of Defense. 2001. Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms. Department of Defense.

Endsley, M. R. 1988. Design and Evaluation for Situation Awareness Enhancement. Human Factors Society Annual Meeting. SAGE Journals.

Fortna, P. 2008. Does Peacekeeping Work? Shaping Belligerents' Choices after Civil War. Princeton University Press.

Gordon, D. 1981. Electronic Warfare. Element of Strategy and Multiplier Combat Power. Elsevier.

IRMA. Grid and Cloud Computing: Concepts, Methodologies, Tools and Applications. 2012. IGI Global.

Kallio, K. 2017. Peace Operations Supporting Efficiency by Organization. Laurea University of Applied Sciences.

Kenyon, H.S. 2009. NATO Deploys Command & Control Tool in Afghanistan. Pp. Multinational Operations Newsletter.

Koops, J., MacQueen, N., Tardy, T., Williams, P. 2015. The Oxford Handbook of United Nations Peacekeeping Operations. OUP Oxford.

Krämer, B., Papazoglou, M., Schmidt, H. 1998. Information Systems Interoperability. Research Studies Press.

Orr, G.E. 1983. Combat Operations C3I: Fundamentals and Interactions. DIANE Publishing.

Ruoslahti, H. & Tikanmaki, I. 2019. How Are Situation Picture, Situation Awareness, and Situation Understanding Discussed in Recent Scholarly Literature? Laurea University of Applied Sciences.

Solana, J. 1999. The Washington Summit: NATO steps boldly into the 21st Century. NATO Information Service.

Stair, R., Reynolds, G. 2012. Fundamentals of Information Systems. Cengage Learning.

Stair, R., Reynolds, G. 2012. Principles of Information Systems. Cengage Learning.

Vacca, J.R. 2009. Computer and Information Security Handbook. Morgan Kaufmann.

Wiederhold, G. 1996. Intelligent Integration of Information. Springer Science & Business Media.

Yau, HK. 2014. Information Security Controls. Adv Robot Autom 3: e118. Department of Systems Engineering and Engineering Management, City University of Hong Kong.

Electronic sources

Airbus Defence & Space. 2014. Deployable Communication Information System. Accessed 20 November 2019. https://www.youtube.com/watch?v=cMgOOIjiFLc

BAE Systems. No date. FALCON fact sheet.pdf. Accessed 12 June 2020. https://www.baesystems.com/en-uk/product/falcon

BAE Systems. No date. FALCON info-graphic.pdf. Accessed 12 June 2020. https://www.baesystems.com/en-uk/product/falcon

BAE Systems. No date. FALCON overview.pdf. Accessed 12 June 2020. https://www.baesystems.com/en-uk/product/falcon

BBC. 2016. Balkans War: A Brief Guide. Accessed 6 June 2020. https://www.bbc.co.uk/news/world-europe-17632399

Boston, J. 2014. Bandwidth vs Throughput. Accessed 12 December 2019. https://www.avalan.com/blog/bid/368397/Bandwidth-vs-Throughput

Defense News. 2014. NATO Eyes Deployable Comm System for High Readiness Forces. Accessed 19 February 2020. https://www.defensenews.com/global/europe/2014/12/10/nato-eyes-deployable-comm-system-for-high-readiness-forces/

EDRM. No date. Glossary – Data Integrity. Accessed 6 June 2020. https://www.edrm.net/glossary/data-integrity/#:~:text=Data%20integrity%20can%20be%20compromised,such%20as%20fires%20and%20floods.

Espen, B.E. 2001. NATO Review. Peacekeeping Past and Present. Accessed 3 May 2019. https://www.nato.int/docu/review/articles/2001/06/01/peacekeeping-past-and-present/index.html

International Standard Organization. ISO 14001: 2015 Environmental Management Systems – Requirements with guidance for use. Accessed 15 June 2020. https://www.iso.org/standard/60857.html

International Standard Organization. ISO 9001: 2015 Quality Management Systems – Requirements. Accessed 15 June 2020. https://www.iso.org/standard/62085.html

Krishnanand, B. 2018. Test Design Using The OODA Loop. Accessed 19 February 2020. https://medium.com/testvagrant/test-design-using-the-ooda-loop-d66484557b31

Lockheed Martin. No date. Electronic Warfare. Accessed 20 January 2020. https://www.lockheedmartin.com/en-us/capabilities/electronic-warfare.html

NATO. 2006. Interoperability for Joint Operations. Accessed 19 February 2020. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120116_interoperability-en.pdf

NATO. No date. What is NATO. Accessed 23 September 2019. https://www.nato.int/nato-welcome/index.html

PBS. 2005. Innovating & Improvising. Accessed 19 February 2020. https://www.pbs.org/wgbh/pages/frontline/shows/company/lessons/

PC Mag. No date. Cryptography. Accessed 12 December 2019. https://www.pcmag.com/encyclopedia/term/cryptography

Presse, A.F. 2017. The 1990s Balkan Wars in Key Dates. Accessed 6 June 2020. https://www.voanews.com/europe/1990s-balkan-wars-key-dates

Prezi. 2014. Features and Functions of Information Systems. Accessed 16 April 2014. https://prezi.com/xlfk2dojj1vd/features-and-functions-of-information-systems/

Sharland, S. 2018. Security of UN Peacekeepers: The Minefield of Politics, People & Principles. Accessed 23 October 2019. https://www.aspistrategist.org.au/security-un-peacekeepers-minefield-politics-people-principles/

The British Army. No date. Homepage. Accessed 6 June 2020. https://www.army.mod.uk/

The British Army. No date. What We Do. Accessed 6 June 2020. https://www.army.mod.uk/what-we-do/

The New Haysalian Military. No date. HX Series Large Utility Transport. Accessed 20 January 2020. https://nhmilitary.weebly.com/utility-vehicle-transport-largemedium-rheinmetall-hx-series.html

United Kingdom Government. No date. Ministry of Defence – About Us. Accessed 6 June 2020. https://www.gov.uk/government/organizations/ministry-of-defence/about

United Kingdom Government. No date. Organizations – Ministry of Defence. Accessed 6 June 2020. https://www.gov.uk/government/organizations/ministry-of-defence

United Nations. 2011. Security & Rule of Law in the Field. Accessed 23 October 2019. https://www.youtube.com/watch?v=UtegUGSK1bg

United Nations. No date. UN Overview. Accessed 23 September 2019. https://www.un.org/en/sections/about-un/overview/index.html

United Nations. No date. UN Structure. Accessed 26 September 2019. https://outreach.un.org/mun/content/un-structure

United Nations. No date. UNFICYP Fact Sheet. Accessed 18 October 2019. https://peacekeeping.un.org/en/mission/unficyp

United Nations. No date. What is Peacekeeping. Accessed 15 October 2019. https://peacekeeping.un.org/en/what-is-peacekeeping

United Nations. No date. What We Do. Accessed 23 September 2019. https://www.un.org/en/sections/what-we-do/maintain-international-peace-and-security/index.html

United Nations. No date. UN Card: 10 Facts. Accessed 6 June 2020. https://www.un.org/en/sections/about-un/un-card-10-facts/

United Nations. No date. Troop and Police Contributions. Accessed 6 June 2020. https://peacekeeping.un.org/en/data-troop-and-police-contributions

United Nations. No date. United Nations Contributions by Rank CSV File. Accessed 6 June 2020. https://peacekeeping.un.org/en/data-troop-and-police-contributions

United Nations. No date. Growth in United Nations Membership, 1945-Present. Accessed 6 June 2020. https://www.un.org/en/sections/member-states/growth-united-nations-membership-1945-present/index.html

United Nations. No date. Fifth Committee Approves $6.51 Billion for 13 Peacekeeping Operations in 2019/2020. Accessed 6 June 2020. https://www.un.org/press/en/2019/gaab4328.doc.htm

United Nations Global Service Centre. 11 October 2018. UNGSC 2018. Accessed 16 May 2019. https://www.youtube.com/watch?v=OgGajwJEKgs&t=175s

United Nations Global Service Centre. No date. UNGLC Homepage. Accessed 10 October 2019. https://www.unlb.org/

UN-SPIDER. No date. UNITAR Operational Satellite Applications Programme (UNOSAT). Accessed 23 October 2019. http://www.un-spider.org/space-application/emergency-mechanisms/unitar-operational-satellite-applications-programme-unosat

Walkowski, D. 2019. What are Security Controls? Accessed 27 October 2019. https://www.f5.com/labs/articles/education/what-are-security-controls

Walkowski, D. 2019. What is the CIA Triad? Accessed 19 February 2020. https://www.f5.com/labs/articles/education/what-is-the-cia-triad

Figures

Tables