A Case Study for Cyber Security Assessment on Tactical Command and Control Systems

Ö. Doğan K. M. Koşaner

***Abstract*—The Tactical Command and Control System is a system of systems which can also be defined as network of networks. Like all other network systems, command and control systems are vulnerable to cyber attacks. In this paper an overview of command control system and the cyber security risks are given. Then case studies about the cyber security evaluation of two ASELSAN command control systems are presented and the solution procedure designed is introduced.**

***Index Terms*—Cyber Security, Tactical Command and Control Systems, Vulnerabilities in Command and Control Systems**

I. Introduction

Tactical Command and Control System is a system of systems. It can be considered as a mission driven system to achieve network centric operation (NCO). It is usually a distributed system using communication network. In missions the success of a C2 system is dependent on communication and computers. The information should be delivered to system from component and data should be gathered in the system and should be presented. Thus the command and control systems become a possible target for cyber attacks. These cyber attacks are many sided and difficult to handle. Some attacks can be detected in very long time.

In this paper cyber security issue in command and control system is discussed. In section 2, an overview of a tactical command and control system is presented. In section 3 the importance of the cyber security in command and control system is discussed, using the general definitions in literature and the vulnerabilities and security requirements in command and control systems. In section 4 the case study about the cyber security evaluation of two command and control systems is explained. The evaluation process and the results are presented. Finally we conclude our paper summarizing the findings.

Ömer DOĞAN is with the ASELSAN A.Ş., PO Box 1, Yenimahalle, Ankara, 06171, TURKEY. Tel: +90 312 592 2353, Fax: +90 312 592 3030, e-mail: omerdogan@aselsan.com.tr.

Kerem Mustafa KOŞANER is with the ASELSAN A.Ş., PO Box 1, Yenimahalle, Ankara, 06171, TURKEY. Tel: +90 312 592 2686, Fax: +90 312 592 3030, e-mail: kmkosaner@aselsan.com.tr.

II. Tactical Command and Control Systems

Tactical C2 systems consist of software, methods, and procedures that allow commanders to make decisions and control their forces [1]. The scenario of the overall situation and the view of the operation area should be presented to the mission commander for awareness. Awareness provides better decision making opportunity to the commander. A commander has to be aware of each unit in the battlefield. C2 system should present all this data from forces and units to the commander effectively for control purposes. In order to control forces and units there should network infrastructure to provide communication. Components of the system are connected to variety of inputs and outputs. Many systems are integrated. Thus the alignment of interfaces and full integration on communication infrastructure is the primary concern. But when the system and the number of components get bigger the performance and security of the communication and the data becomes another concern.

Secure and effective communication is critical in military organization. The communication should be robust and reliable. In a command and control systems there are large number of units and each units provides critical data to the network of the system. This data could be critical data like tactical picture, target data for engagement, mission order or sensor data. Thus, the reliance on information, computer and communication Technologies for conduct of military operations has increased [2]. These technologies have become the main target for opponents in tactic field; therefore the security of them has become vital. In this section importance of the information and communication in command and control systems is discussed. Rest of the paper concentrates on the security of them against cyber attacks.

III. Cyber Security In Tactical C2 Systems

A. Importance of Cyber Security in Command and Control Systems

Current trends in defence systems show that there is a huge demand on information, computer and communication. Due tothis fact, IT infrastructure is one of the main facts for defence systems, especially for Command and Control Systems. Command and Control Systems are based on the

integration, interoperability. Technologies to support military operations. and networking of many systems making it a large single system as such we can call it a "system of systems" [2]. In this situation, opponents have opportunity to attack the systems. This issue forces the system designers to take extra care on the unwanted attacks over IT systems to make the complete system durable against enemies [4].

In general, security in Command and Control Systems is a two dimensional problem. One is the physical security of the facilities that the parts of the systems are located in. No one can do this better than military. Organizations often concentrate on external attacks, almost exclusively, mainly because security audit tools and modelling techniques are readily available which aid in finding vulnerabilities and fixing those [7]. Insider threats are misperceived and have high impact. The success rates of insider threats are higher, because they are familiar about the system and the targets. The second one is information security of the system, which is more demanding and challenging part. This is also called cyber security, which is not clearly understood at all the levels [4].

In parallel to the unpredictable and unstable development of the information technologies, many risks have emerged due to computer attacks. Cyber security issues are arising out of digital information, worldwide networks and application interconnection as well as data dissemination. Issues that make the designed system vulnerable to cyber attacks are the main concerns of the command and control systems design.

B. *Definitions Related to Cyber Security*

There are many definitions related to the cyber security. One of the accepted definitions is given as Information Assurance. Information assurance is defined as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation [5]. Information assurance is derived from information security. Information security is directly related to Confidentiality, Integrity and Availability. Information security has grown from practices and procedures of computer security.

Confidentiality refers to limiting information access and disclosure to authorized users and preventing access by or disclosure to unauthorized ones [3].

Integrity refers to the trustworthiness of information resources. It includes the concept of "data integrity"-namely that data have not been changed inappropriately, whether by accident or deliberately malign activity. It also includes "origin" or "source integrity" – that is, that the data actually came from the person or entity you think it did, rather than an imposter.[3]

Availability refers, unsurprisingly, to the availability of information resources. An information system that is not available when you need it is almost as bad as none at all. It may be much worse, depending on how reliant the organization has become on a functioning computer and communications infrastructure [3].

C. *Generic Vulnerabilities and Security Requirements in Command and Control Systems*

Any computer network or information system is vulnerable to two types of attacks. These are passive and active attacks. Passive attacks can be traffic analysis and release of message contents. Unfortunately, passive attacks are generally very difficult to detect. Designers should consider this type of attacks during design phase such as by using encryption techniques. Active attacks involve modification of data streams or the creation of false streams. These types of attacks fall into four categories, which are masquerade, replay, modification of messages and denial of service (DoS)[4]. Appropriate security mechanisms are designed and used to detect, prevent or recover from a security attack. There are many security mechanisms that help to detect the cyber attack. These are encipherment, digital signatures, access control, data integrity, authentication Exchange, traffic padding, routing control, notarization, trusted functionality, security label, event detection, auditing, recovery, etc[4].

There are four general vulnerabilities that can be seen in Command and Control Systems. These are unauthorized access to data, clandestine alteration of data, identity fraud and denial of service (DoS). All of these vulnerabilities may have deep impact on the running phase of the Command and Control System [4]. For instance, unauthorized access to data on system computer may result in inflicting severe damage to an army by obtaining and using classified or unclassified information by an adversary. Similarly, military planning may be severely affected if clandestine alteration of data at system computer is done by enemy. The identity fraud may result in modification of situational awareness through insertion of unwanted/changed information, issuing of fake orders, etc. All these will affect the effective working and psychological situations of defence forces. While the application of DoS attacks on a command and control system, the time critical operational planning and completion of tasks will be affected [4].

The main goal of the requirements to prevent the vulnerabilities informed is to achieve confidentiality, integrity and availability of the data and maintain system configuration through security guidelines and accountability of personnel authorized to access the information sources. Following security services are required to cater the security requirements

[4]:

Authentication: Identifying the user identity through various means such as passwords, fingerprints, digital certificates, etc.

Access Control: Permission or authority to perform specified actions as authorized in policy guidelines [5].

Data Confidentiality: Protection of data against unauthorized disclosure [5].

Data Integrity: The assurance that data received and is same as transmitted by authorized user [5].

Non-repudiation: Providing protection against denial by participants once participated in communication [5].

Availability: Ensuring availability of a capability or system at all times or whenever desired/required [5].

IV. Case Study

Tactical C2 Systems are classified according to their functional area, such as Air Defence, Fire Support, Maneuver, Intelligence and Combat Support & Combat Service Support (Personnel and Logistics). ASELSAN developed Tactical Fire Control System and Fire Support Automation System (AFSAS) in the fire support functional area and Air Defence Early Warning and Command, Control, Communications, Computers and Intelligence (C4I) System (HERIKKS) in the Air Defence area. In coordination with Turkish Armed Forces cyber security evaluation is being conducted on these systems to determine whether the data and the information system of the systems are adequately protected against cyber attack. In this section first the developed systems will be introduced and the then evaluation results will be presented.

A. AFSAS

ASELSAN Fire Support Automation System (AFSAS) is designed to provide the most effective, efficient and timely fire support that the corps need by integrating fire support units with the other functional areas of the battlefield.

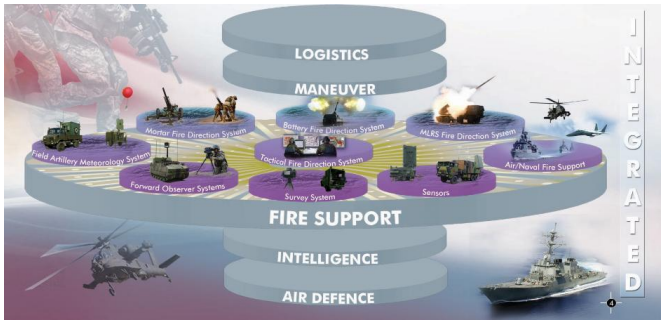

Fig. 1. Sub components of ASELSAN Fire Support Automation System

ASELSAN Fire Support Automation System is a unique combination of subsystems designed by ASELSAN for tactical and technical fire direction that covers the entire fire support functionality, ranging from the uppermost command centres at the corps level to the lowermost individual units at gun and forward observer levels. AFSAS is defined as system of systems.

AFSAS provides planning and execution of fire missions to shoot a target with the most appropriate weapon system and ammunition at the most appropriate time. It provides for maximum utilization of the fire support assets available on the battlefield.

AFSAS provides integrated and automated support for planning, coordinating and controlling of all fire support assets such as field artillery (including mortars and multiple launch rockets), observers, radars, met stations and survey systems.

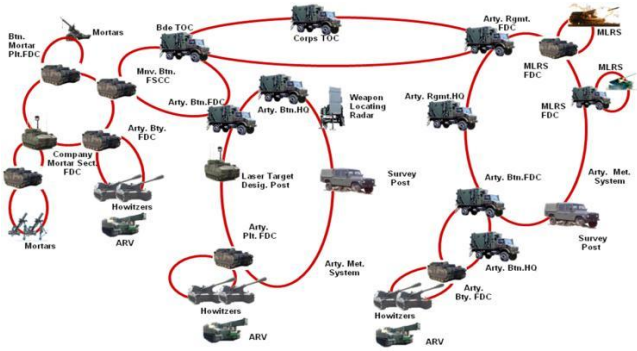

Fig. 2. The Communication Network Structure of ASELSAN Fire Support Automation System.

B. HERİKKS

HERİKKS is an Air Defence Early Warning and Command, Control, Communications, Computers and Intelligence (C4I) System that manages the air defence activities on Tactical Level. It was developed by ASELSAN and is in use by Turkish Armed Forces since 2001.

Fig. 3. Sub components of Air Defence Early Warning and C4I

System (HERIKKS)

The mission of HERİKKS is to create a recognized air picture in real time (Sensor Fusion) by using the air threat information received from various mobile and stationary radar systems in tactical battlefield and to assign appropriate air defence weapons to the selected targets (Threat Evaluation Weapon Assignment (TEWA)).

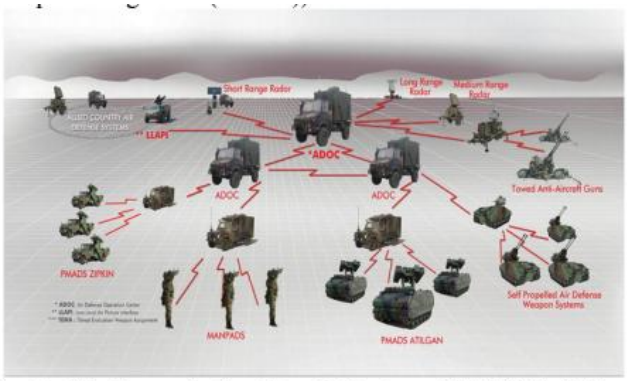

Fig. 4. The Communication Network Structure of HERİKKS. Different networks such as Sensor/Weapon Network, Command/Control Network, and Weapon Network are established as necessary as illustrated in the figure.

HERİKKS consists of Air Defence (AD) command posts at Army, Corps and Brigade Level, interface units for long, medium and short-range AD radars, interfaces for AD weapons systems and interfaces to another Command and Control systems in the battlefield. HERİKKS organize these discrete systems so that they act as a coherent integrated air defence system.

HERİKKS, provides the communication among system components either by

- Wireless Networks (Radios, Radio Links, etc.)
- Cable Communications (Copper lines, fiber optical)

HERİKKS has open system architecture, giving scope for sensor and weapon development, and modular hardware and software on a distributed architecture.

C. Cyber Security Evaluation

Turkish Armed Forces decided to conduct cyber security evaluation on the critic systems. The software and hardware components of the AFSAS and HERIKKS systems were evaluated. The purpose of the evaluation was to identify cyber security weaknesses of the systems and decide the additional actions needed to further strengthen the systems against cyber attacks.

Cyber security issue is a multi dimensional problem. The physical security part is under the responsibility of the owner of the system which is Turkish Armed Forces in our case. The security of the equipments and hardware should be provided and physical accessibility of the system should be prevented. The information security of the system is under the responsibility of the developer of the system which is ASELSAN in evaluated systems. The Information security is directly related to the availability, integrity, authentication, confidentiality and non-repudiation of a command and control system. The system are designed and developed concerning these security issues. The issues are valid for both software and hardware (computer, communication devices, weapons etc.) components. The implementation of the issues is presented below:

Availability is a design criterion for our products. The criteria are checked from the beginning of the software and hardware development phases, to the end of the integration phase. Regarding the international standards the availability tests are conducted in each phase. The purpose of these tests is to guarantee whether the system functions properly under all circumstances or not.

Integrity is considered as one of the base criteria for our products. In our products there are several authorization levels to provide the integrity of the information. This authorization levels are defined in coordination with Turkish Armed Forces. Only authorized user can edit or change the data throughout the system. Unauthorized users can not change, transfer or copy the data without the permission of the authorized users.

Authentication is one of the critical security items for protection of the systems against unauthorized users. Each component is protected with special authentication mechanism. All of the software or hardware components are accessed with several level of authentication input from the user.

Confidentiality is protection of the system against unauthorized disclosure. Confidentiality criteria are defined in coordination with Turkish Armed Forces in all phases. Confidentiality is provided both with hardware and software structures. For instance the special military connectors are used for hardware input part of the devices. Thus unauthorized users can not connect to the system without special knowledge of connector specification. In software development and deployment process hardening operations like authentication, firewall protection, port limitations, antivirus protection, database encryption, external hard drive limitation, deactivation of unused services and applications etc. are the concepts of confidentiality. Additional to software precautions, the communications devices have their own security protocols providing encrypted communication over radio.

Non-repudiation provides a protection against denial. In our all user operations are logged to files in order to keep the record of the user attractions. In any suspicious situation, the logs are used as a proof of misuse. The levels of the logs can be arranged concerning need of the user.

From the beginning to the disposal of the system, cyber security risk definition is evaluated concerning the cyber security criteria. For each level of evaluation, the risks are

defined with approximation as follows:

- Baseline the current system structure
- Define the critical components/issues
- Analyze the security risks
- Define how to cope with the risks
- Realization of the precautions and feedback to the system

After each analysis cycle, the procedure starts from the first step until the final decision is given. For each design criteria, possible cyber security risks are decided. Then the risks are classified by following equation:

Risk Value = Probability * Impact (1)

The final risk classification is presented on the table below. The values on the table can vary application to application:

TABLE I
RISK CLASSIFICATION TABLE

Risk Value	Insignificant	Minor	Moderate	Major	Catastrophic
Rare	Low	Low	Low	Moderate	Moderate
Unlikely	Low	Moderate	Moderate	High	High
Moderate	Low	Moderate	High	High	Extreme
Likely	Moderate	High	High	Extreme	Extreme
Almost	Moderate	High	Extreme	Extreme	Extreme

Using the risk classification table, the solution of cyber security risks are prioritized. The higher the priority level, the former the solution is done. By using this procedure all the cyber security risks are handled.

V. Conclusion

We have reviewed the cyber security issue of command and control systems. As the command control systems are huge systems called as “systems of systems”, the large number of risks and corresponding vulnerabilities exists. Therefore opponents have a great tendency to attack such systems. In the developed to classify threats, specify attack mechanisms, verify protection mechanisms, and evaluate consequences [9].

The vulnerability, survivability, etc. of given can be analyzed before the cyber attack occurs. Cyber attack simulation systems are the main future work for the security of the military systems. Significant research result has not been produced yet because of the extreme complexity of the cyber attack and defence problem. Search space is enormous, good data on attacks and defences does not exist [10]. In future new cyber security techniques should be designed against all types of attacks to protect the systems more efficiently, using the cyber attack simulation systems for tests. of development process of the system, the security weaknesses should be identified and fixed at all steps of the process. Possible security risks should be identified first, and then the risks should be classified to prioritize the cyber security solutions.

The cyber security issue is a multi dimensional problem. All the shareholders of the system should involve in protection activities against cyber attacks. Even if the system is developed as a secure system, the physical environment that the system will be used should also be secure. There are many methods in the literature that can be used for cyber attack protection. The one we have presented can be used for similar systems but each system should be analyzed individually for its own cyber attack protection mechanism.

VI. Future Work

Technology is one of the primary change agents in the military of today and likely of the future [6]. Cyber attackers can achieve their military and strategic goals without the need for physical armed conflict. They gain asymmetrical war power although they seem small and insignificant. Boundaries are not divided between physical, logical and between military and civilian [8]. The cyber attack techniques and vulnerabilities will rapidly change. Thus the cyber security protection has become a living process, new types of cyber attacks should be followed and the systems should be kept updated against new types of attacks. The procedures that we have presented should also be updated in future by considering current cyber attack techniques at that time. In order to take precaution against the cyber attack techniques, there are detection tools to detect malicious activity within network. But it is not possible to identify the cyber attack. Therefore tools cannot take action against them. Simulation techniques should

REFERENCES

[1] Rand. (2009). Controlling the cost of C4I upgrades on naval ships. A study report for US RAND Corporation. National Defense and Research Institute USA (2009).
[2] Malik, A. A., Mahboob, A., Khan, A., & Zubairi, J. (2011). Application of Cyber Security in Emerging C4ISR Systems. In J. Zubairi & A. Mahboob (Eds.), Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies (pp. 223-258). Hershey, PA: IGI Global.
[3] Available: http://it.med.miami.edu/x904.xml
[4] Stallings, W. (2003). *Cryptography and network security principles and*
[5] CNSS. (2010, April 26). *National Information Assurance Glossary*. Committee on National Security Systems. Instruction CNSSI-4009 dated 26 April 2010
[6] T. K. Adams, “Radical destabilizing effects of new technologies,” Parameters, vol. 1998, pp. 99-111, 1998.
[7] A. Iyer and H. Q. Ngo, "Towards a theory of insider threat assessment in "In Proceedings of the 2005 International Conference on Dependable Systems and Networks Yokohama, Japan: IEEE Computer Society, 2005, pp. 108-117.
[8] Jung-Ho E., Nam-Uk K., Sung-Hwan K, and Tai-Myoung C. Cyber Military Strategy for Cyberspace Superiority in Cyber Warfare.

CyberSec, page 295-299. IEEE, (2012)

[9] Chi, S. D. Park, J. S., Jung, K. C., & Lee, J. S. (2001, January). Network security modeling and cyber attack simulation methodology. In Information Security and Privacy (pp. 320-333). Springer Berlin Heidelberg.

[10] F. Cohen "Simulating Cyber Attacks, Defenses, and Consequences", IEEE Symposium on Security and Privacy Special 20th Anniversary Program, Berkeley, CA, May, 1999.