2011 3rd International Conference on Cyber Conflict
C. Czosseck, E. Tyugu, T. Wingfield (Eds.)
Tallinn, Estonia, 2011 © CCD COE Publications

Cyber Security on Military Deployed Networks

A Case Study on Real Information Leakage

Cpt. Fabio MULAZZANI, Ph.D.
2nd Signal Alpine Regiment, Italian Army
and
Free University of Bozen/Bolzano
Bolzano, Italy
fmulazzani@unibz.it

Lt.Col. Salvatore A. SARCIA', Ph.D.
General Staff, Italian Army
and
University of Rome "Tor Vergata"
Rome, Italy
asarcia@disp.uniroma2.it

Abstract- **This paper reports on real information leakage occurred in a multinational mission. To investigate the nature of the leakage, we performed a survey among the military operators which showed that technical and cultural problems were key elements of the security shortfall. We also show that military deployed networks present some peculiarities with respect to infrastructure homeland networks. Therefore, the former should be managed differently from the latter. In particular, we highlight two reasons concerning either the operators or the networks: (1) Temporary nature of deployed networks and (2) Lack of training and guidance (es. SOPs). Finally, we propose a new approach that would strengthen the defense attitude of signal units and check whether protection activities are effective and reliable.**

Keywords: Military Field Data Network; Security Leak; Country Case Study; Human Resource Management, Cyber Offense

Disclaimer: This paper is a product of the authors designed to provide an independent point of view. It does not represent the opinions or official position of the Italian Army.

I. INTRODUCTION

On November the 28th 2010 several thousand classified documents were published on the Wikileaks website. This fact triggered cyber defense actions for almost all Governments targeted by the information leakage. How did this leakage happen? Firstly, personal responsibilities should have been taken into account, i.e. the soldier who stole the document and gave it to Wikileaks. Secondly, under what circumstances can highly classified documents be retrieved so easily? From a security perspective, governments' data networks (and, as such, those belonging to Armed Forces) supporting the treatment of classified files are usually properly supervised by a team of highly specialized and reliable servants defending the network from cyber threats. Such cyber defense services can then be easily maintained within national networks such as those within the national territory. However, military networks are present in a variety of areas of operations around the world, and they need to be managed (including security issues) in the location where they actually are. The administration of the network is locally-based because the link to the national data network is usually limited (e.g., at most 1 Mbps) – these circumstances make operational military networks quite different from the other governmental networks. It is clear that cyber-attacks would target the weakest area of a network, as well as operational networks may be considered as the target of cyber-attacks word-wide.

This paper presents a case study of a real incident occurred within an operational contingent that one of the authors dealt with some months ago. Moreover, it presents the analysis of the possible root causes that resulted in the incident. We compare and contrast domestic and operational (abroad) networks one another, trying to find the elements that make the military network deployed on the field so interesting for cyber security. The case study will describe the physical layer of the network and expand on software applications that determined security leakage. Our research question (closely stated below) is to figure out whether or not cultural factors such as background, educational level, and country-wide habits of the persons in charge of the network management (stakeholders) can be considered primary reasons of the security leak which we are referring to.

In order to investigate our research question, we performed a survey within the community of stakeholders involved in the management of the targeted network. The survey was oriented to (i) identify relevant security aspects and (ii) assess the stakeholders' awareness on cyber defense. Finally, from the analysis of the data collected from the survey we developed some proposals to address the issue of the security of military networks on field mission.

The rest of the paper is structured as follows. In section 2 we offer a review of the main IT security guidelines adopted by the Italian Army. In section 3 we propose a detailed description of the case study and the structure of the survey. In section 4 we illustrate the results of the survey previously described. In section 5 we illustrate our proposal for a new organizational approach for cyber defense. Finally, in sections 6, 7 and 8 we state the conclusions, the future works and the remarks.

II. RELATED WORKS

With [1] and [2] the Italian Army produced the directives on the security of classified and unclassified telecommunications and information systems, also on the basis of [3]. The purpose of the mentioned directives is to (i) clearly identify and define the organizational structure of the bodies responsible for the Information Security (INFOSEC) aspects; (ii) describe the formal procedure to require the homologation of the network; (iii) remind that operating systems must be certified according to international criteria like ITSEC or ISO/IEC 15408 – Common Criteria (CC) [4] [5] [6].

ITSEC is the acronym for Information Technology Security Evaluation Criteria and is a structured set of criteria for evaluating computer security. The evaluation consists in the examination of IT features and in a penetration testing of the Target of Evaluation (TOE). ITSEC identifies seven ascending levels of confidence that can be placed in the TOE, the levels are coded from E0 to E6. ITSEC can be seen as the natural evolution of the Trusted Computer System Evaluation Criteria, frequently referred to as the Orange Book [7] [8]. The Orange Book was commonly perceived as "too strict" in formal definitions that is because ITSEC has the purpose to create an environment flexible enough to identify new requirements sets when new security problems are found. In ITSEC is very important the concept of IS security requirements *reliability*. In particular, the *reliability* is seen as trust both in the *effectiveness* and in the *propriety* of the security systems that were designed and implemented. *Effectiveness* describes how the system responds to the attacks, and *propriety* identifies all the aspects related to the realization of the product.

ISO/IEC 15408 (CC) is a standard that aims to evaluate whether security facilities of information systems are properly designed and implemented. The CC supports understanding of "what the product does" (security functionality) and "how sure you are of that" (security assurance). From a practical perspective, CC provides a methodology, notation, and syntax to specify security requirements by means of three documents (Part 1, Part 2, and Part 3).

The CC aims at being a keystone for ISs *consumers*, *developers*, and *evaluators*. The CC states that any security analysis should examine the physical environment a system will exist in, the asset requiring protection, and the purpose of a system to be evaluated (target system). It then mandates a listing of the assumption, threats and organizational security policies, leading to a set of security objectives to be met. Using the objectives, a set of security requirements should be generated. Requirements that recur in various systems and settings become the Protection Profile (PP), which is intended to be reusable and defines the target system's security requirements known to be useful and effective in meeting the identified objectives, both for functions and assurance. The PP also contains the rationale for security objectives and security requirements. Evaluations, including various types of penetration testing, should then be carried out to determine a level of compliance with PP.

Even if ITSEC is being replaced by CC, a mapping between the two on the evaluation levels is given in [9].

A further support in the field of IT security is offered by the ISO/IEC 27000 family standard [10] that is a group of information security standards, it was developed on the basis of the publication BS 7799 "Code for Information Security Management" first issued in 1995 by the United Kingdom's Government Department of Trade and Industry (DTI) and the British Standard Institute.
ISO 27001 aims at offering a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS). ISO 27002 describes a set of information security management objectives and controls. ISO 27003 provides a set of guidelines to implement ISO 27000 standards. ISO 27004 provides a set of metrics to measure the efficiency of the ISMS. ISO 27005 provides a set of guidelines to conduct an information security risk management. ISO 27006 provides a set of guidelines to the various certification bodies on the process for certifying other organizations' ISMs. ISO 27007 provides a set of guidelines to those who audit ISMSs against ISO 27001, that indicate the best way to do so. Unfortunately, even if both public and private sector organizations have recognized the importance and benefits of ISO/IEC 27000 family, neither in [1], nor in [2], nor in [3] a reference to it was made. Further relevant research can be found in [11] and [12] where there are several theoretical and empirical studies that have been conducted with the purpose of offering models and frameworks aiming at better prioritizing cyber security threats.

III. CASE STUDY

The area of operations where the incident took place covered a wide area of the entire deployment territory. Among the common services such as telephone and radio network, the units were also served with three distinct data networks.
The first network, called "Lotus", was provided to the units by a Multinational Information Technology Service. Lotus was a VPN over Internet on which IBM Lotus software held about 50 clients. The purpose of Lotus was to offer (i) an Internet connection (especially in field of operations), and (ii) a support for collaborative tools such as the ones provided by IBM.
"Army-Net" and "Mission-Net" were managed by the signal unit. The former was a class "B" network by means of satellite links. Army-Net had about 400 users and was only employed by personnel of the contingent. Amy-Net supported several services such as: (i) Proxy internet connection; (ii) Unclassified information sharing (typically emails and documents); and (iii) Classified information sharing (usually preformatted messages) – the encryption of the signal was provided by ciphers connected to PCs allowing the treatment of classified information.
The third network, Mission-net, counted almost the same number of users as Army-Net, and it was settled to exchange both "Unclassified" and "Restricted" information; national classified information could not be shared over Mission-Net, however. The Mission-net access was provided to the units by means of microwaves backbones secured by Telesy KD03 IP cipher. Since the two potential security leaks were discovered in Mission-net, our case study focuses on this latter.

A. *MISSION-Net*

Before the discovery of the leaks, the Mission network had ten servers offering different services. They were as follows:

- Four Microsoft Windows 2003 Domain Controller Servers;
- One Web server based on Linux Debian;
- One Mail server base on Microsoft Windows 2003 and Altn Technologies MDeamon;
- One Microsoft Windows Server Update Services (WSUS) server;
- Two Sophos Anti-Virus servers working over a Microsoft Windows 2003 Server operating system;
- One FTP-Storage server based on Windows 2003 Server;

A military specialist, with the role of information system and network administrator, managed all services stated above. A military operator assisted the specialist in the daily work. The specialist was in charge of several duties, such as (i) repairing the network physically (ii) maintaining software applications, (iii) analyzing new process-oriented software applications not being supported yet; (iv) supporting the work of the Help Desk for the resolution of users' PC problems related to network services; (v) administering servers, routers, software licenses received for the mission.

B. *Relevant variables*

In order to investigate the nature of information leakage over deployed data networks of our case study, we identified some variables. Consequently, we devised some questions to survey some of those variables within an operation unit deployed in the field. The aim was to investigate to what extent the identified variables may be relevant to the explanation of the identified information leakage. Firstly, we identified the *turnover* of the operators as one of the variables to take into consideration. In fact, in the analyzed case, we noticed that the administrator changed with a frequency of a semester and, sometimes, of a quarter. The *inadequacy of a relevant percentage of users' PCs* was another identified variable. In the case study, about 30% of the users' PCs needed to be changed with more modern and adequate machines. The *length of the hand-over* from a contingent to another was considered as an additional variable. The incoming administrator worked only one week together with the outgoing administrator before the latter left. During that time, the incoming administrator received both the administrative and technical orders and hints to manage the systems. *Network topology change* was another variable relevant to the analysis. In the case study, the topology was also changed in terms of physical locations of servers. The *number of different locations* in which servers were dislocated seemed to be a relevant variable as well. In our case, the servers of Mission-net were distributed among four different locations. *Number of movements* was another relevant variable. We also identified as a relevant variable the *length of the relocation activity* as well as the *timeframe that the headquarters allotted* to the unit to complete the relocation.

C. *The Identified Leaks*

The first leak related to the possibility for those users not properly configured in the domain (i.e. with administrators rights) to access other users hard drive with the "C$" functionality. That functionality exists by default on Windows operating systems, and allows accessing other network users in anonymous mode – even without leaving any record on the access log file. With that functionality it is possible to have full permission (i.e., read, write, or delete) on the files of the remote hard drive. For example, a user that is not properly logged to the network domain, and has administrator rights, simply needs to write in the Windows Start menu run line the IP address of the PC being accessed followed by c$ (i.e. \\172.16.5.246\c$) and run the command.

The second leak related to the possibility, for those who could have accessed the mail server, to download all emails stored in the email server. Units and headquarters have not discovered yet whether or not someone downloaded information stored in the network servers. This is the reason why we refer to the information leakage as potential. In the program directory of MDeamon existed a folder containing a sub-folder for each hosted user. This folder hosted msg-format emails waiting for being downloaded by the local client. If either the administrator or someone else having the opportunity to access the mail server wanted to read the mail of a user, then the violation would be easy and painless. One simply would enter into the proper MDeamon folder and open the mail file using any editor. Additionally, reading attachments of a mail would not be problematic as well. Once the mail file would be opened with an editor, it would be necessary to copy and paste the attachment into an empty file with the proper extension.

D. *The Research Questions*

We identified two research questions:

a. *What technical and cultural factors affect security leaks within deployed data networks?*

b. *What actions are usually known by military operators for installing classified data sharing networks?*

   b.1. *What actions are usually known by those operators for increasing the level of security once a security leak is identified?*

Question a. aims at investigating technical (i.e. availability of technological devices) and cultural (i.e. security procedures knowledge) elements affecting the security of a deployed military network. It is worth noting that, signal units can usually be grouped into two categories: (i) those operating deployed networks and (ii) those operating non-deployed (i.e., infrastructure) networks. Questions b. aims at figuring out whether operators are prepared to install and operate secure deployed networks and (b.1.) whether those operators know the procedures to be taken after information leaks are discovered.

E. *Survey design*

Based on our experience in the field as specialists, we hypothesized that the problems stated above occurred for two reasons:

a) *Operators of deployed networks usually do not focus on security issues.*
b) *Network users are considered not to be harmful for the network security.*

We investigated these two hypotheses surveying those who operated the networks where information leakage was discovered. The survey we handed out is in annex "A". The survey is structured in six parts:

a) *Interviewed clustering. This part includes questions from 1 to 3 and aim to group the answers in homogeneous sets according to criteria like the rank of the interviewed, his background knowledge and his practical experience;*
b) *MISSION network knowledge/familiarity. This part includes questions form 4 to 8 and aim to collect (i) the intervieweed perceived security of that network, (ii) what are the features that they believe that contribute best to the security, (iii) the intervieweed knowledge on the MISSION network security features.*
c) *Question 9 is oriented to collect the perception of the intervieweed in creating or maintaing secured network like the MISSION.*
d) *Theoretical knowledge test. This part includes questions from 10 to 17 and are oriented to measure the theoretical knowledge (based on easy or medium diffiuculy questions) of the intervieweed on cyber security.*
e) *Question 18 is oriented to identify what is the perceived direction of a possible threat for the network.*
f) *Primary source of information.This part includes question 19 and 20 and aims to verify if the intervieweed (i) know what is the primary source of information for secured network and (ii) know where to get information for the procedures to adopt to install or maintain a secured network like mission.*

The questionnaire was submitted to 25 signal unit Officers, Warrant Officers, and Soldiers on duty in a Multinational mission where Italy participated in.

IV. DESCRIPTION OF THE RESULTS

The results of the survey are described below.
Interviewees clustering – (Question 1) the survey was submitted to a total of 7 Officers, 10 Warrant Officers, and 8 Soldiers. (Question 2) Almost all of the Officers with a rank not greater than Captain had a University degree in IS or Telecommunication topics, the rest of the people did not even have a high school diploma in IS or Telecom topics. The relevant thing was that 2 out of 3 Officers with rank greater or equal to Major did not have a degree (nor University or High School) related to IS or Telecom. (Question 3) All of the interviewees had a vast practical experience in the field because 14 of them participated in 2 to 4 missions, 5 of them 5 to 7, and the rest of them participated in 8 or more missions.

Mission network knowledge/familiarity – (Question 4) 17 interviewees perceive the Mission network as "secured enough", one Officer had "no idea", the rest of them were almost equally distributed between "very secured" and "somewhat secured", see Figure 1.

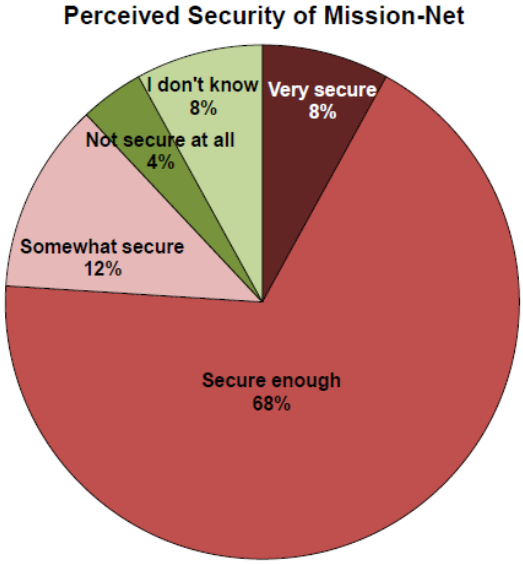

Figure 1. Answers to Question 4 – Perceived Security of Mission-Net

(Question 5) 19 interviewees believed that the sole contributor to the security of the Mission network was encryption, 4 argued that the security was provided by means of "network encryption" and "firewall", and 3 believed that a third contributor could be the anti-virus. Note that, no firewall system was installed in Mission-net. (Question 6) 18 interviewees knew that in the last year the Mission network was affected by viruses or trojans, 2 heard about "steeling information" or "unauthorized access" (this fact was reported by a soldier among the interviewees). The rest of the interviewees did not mention any significant event related to security. (Question 7) Almost all interviewees answered correctly. But, the answers were incomplete. They all knew that there was "network policies", but only few identified other factors as relevant to security. 2 interviewees maintained that a firewall was running to guarantee security. (Question 8) 18 interviewees did not remember whether a security check-up was ever performed, and 7 interviewees answered that the check-up was performed over the previous 6 month, see Figure 2.

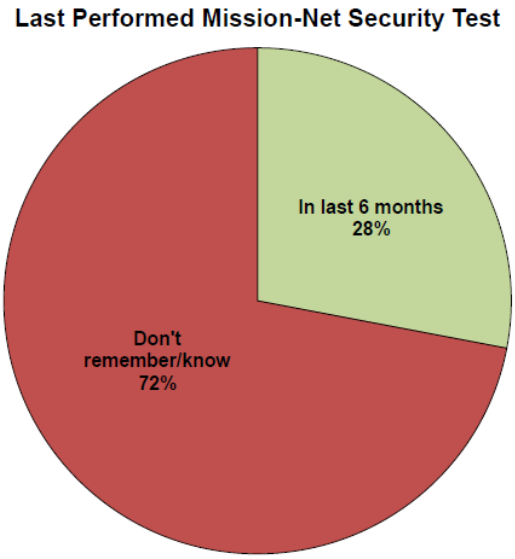

Figure 2. Answers to Question 5 – Last Performed Mission-Net Security Test

Interviewees' confidence in installing/maintaining a secured network – 17 interviewees believed to be "confident" in installing/maintaining a secured network. The rest interviewees selected "fair confident".

Theoretical knowledge test - The mean of the correct answer for all the interviewees was 45%. The mean for all the Officers was 54% of correct answers, Warrant Officers obtained 40% of correct answers, and soldiers 42%.

Perception of threat – (Question 18) the results showed that the great majority of the interviewees (20 interviewees) did not perceive internal users of the network as a threat for security.

Primary source of information – (Question 19) 19 Interviewees did not know the ISO standard proposed. Only one out of 6 asserted to know the standard. (Question 20) The interviewees stated that they used a Standard Operational Procedure (SOP) to install/maintain/supervise a secured data network as Mission-net. But 19 of them declared that the SOP was not provided by the line of command. 2 argued that the document was unavailable because restricted. 4 mistakenly declared that the document was available in a specified internal website.

From a general perspective, the survey showed that interviewees (i) believed that network security was primarily given by ciphers' physical encryption (ii) had poor knowledge of the primary concepts of cyber security (iii) did not perceive internal users of the network as a potential threat. We believe that this situation is due to two factors:

a) *Temporary nature of deployed networks,*
b) *Lack of training and guidance (es. SOPs).*

V. A NEW ORGANIZATIONAL APPROACH TO CYBER DEFENSE

Cyber defense is a relatively new area of concerns for governments and military alliances. The spread of technologies and the low cost of devises and machines turned an impressive number of people into potential information smugglers. Since there exists a rich market where stolen information can be traded, information sales have become a flourishing and profitable activity world-wide. Cyber-attacks aiming at worming out classified information generally take place through infrastructure networks of governments, companies, and institutions. Cyber-attacks against deployed networks are usually less frequent than the ones targeting infrastructure networks. However, the consequences of this kind of information leakage may be drastically severe for the troops deployed in the area of operations. Our case study shows that the fact that military operators underestimate potential information leaks is one of the main reasons for successful cyber-attacks against deployed networks. To assume that users of deployed networks are not able to attack deployed networks can eventually prove to be a great mistake. Secondly, before being deployed onto the field, signal troops should be trained on specific security aspects characterizing networks of interest.

Cyber-defense systems should be based upon three levels of defense. The first level should implement static protection such as identification, authorization, cryptographic protection, and access control. The second level should have mechanisms for collecting information and monitoring the state of the network. The third level should constantly evaluate the network protection [14]. Additionally, as our survey shows, operators' cultural aspects should be taken into account. To check whether or not the security level of our networks is effective we propose a new way of organizing cyber defense units (Figure 3).

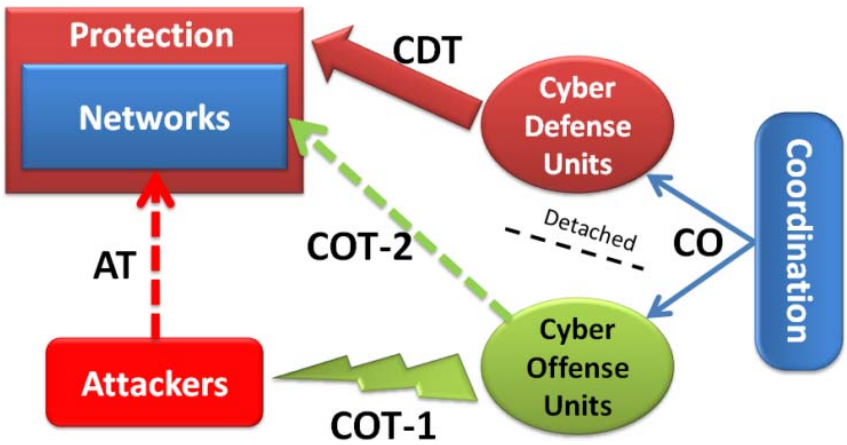

Figure 3. A new organizational approach to cyber defence.

Kotenko [13] proposes a multi-agent approach to cyber-security where teams of agents-malefactors, defense agents, and agents-users are simulated. However, Kotenko's approach cannot be applied to safeguard the security of our deployed troops because it is not always possible to have such simulating infrastructure for deployed networks. Moreover, we argue that a multi-agent approach is worth for experimenting and training signal units, but cannot guarantee the level of security required during operations. As showed in Figure 3, to safeguard our troops we propose a model which is still based upon three different bodies: defense, offense and malefactors (i.e., attackers) teams. However, we do not propose to delegate the assessment whether the level of cyber-security is adequate to a multi-agent framework. This assessment has to be done by a specialized team of people who can constantly evaluate the security and immediately report to the commandant of the mission.

The structure in Figure 3 can be used either for infrastructure or deployed networks. The novelty is that what we currently call cyber defense units should be split into two different kinds of units (detached): (i) those dealing with the protection (sheer defense) and (ii) those dealing with the offensive aspects of the defense. New cyber defense units should only have cyber defense tasks (CDTs) such as settling, maintaining, and protecting their networks. Cyber offense units should play two different roles: the role of attacker against external attackers – performing cyber offense tasks no. 1 (COT-1s) in Figure 3 – and the role of attacker against their own networks – performing cyber offense tasks no. 2 (COT-2s) in Figure 3 – To have detached units dealing with cyber offense only can better differentiate the preparation of offensive operators such that they can be focused on performing specific actions against external attackers. Employing a cyber-offense unit specialized in performing offensive tasks is worth for verifying whether or not the protection activity of cyber defense units is reliable and effective as expected. This situation would also strengthen the defensive attitude of cyber defense units since it would be 100% certain that either infrastructure or deployed networks would be under constant attack at least by cyber offensive units. In case of security shortfalls, the proposed organizational structure (Figure 3) would reduce the latent period between the beginning of the security problem and when the problem is discovered. This would reduce the probability that real attackers worm out sensitive information. In the case study, the operators realized the potential leaks after different months. On the other hand, a constant competition between cyber defense and cyber offense units would bring about an increase in security. Notice that, since cyber defense and offense units should operate synergically, a coordination function would be required. This would guarantee the integrity and the legal framework of the whole cyber activity.

The proposed organizational model stems from what, in science, is called "empirical approach". Empiricists emphasize those aspects that are related to evidence. Knowledge can only be discovered in experiments. We propose an empirical approach to cyber-defense meaning that the only way of assessing whether security of our information is guaranteed is to constantly try out this security through employing *ad hoc* offensive teams playing the role of attackers. Empiricism is the other side of the coin of *a priori* reasoning as, in statistics, prior

information is complementary to information arising from an empirical distribution. The idea of an empirical approach to cyber defense is to use both kinds of information: 1) *a priori* information, i.e. the one dealing with known and expectable attacks, and 2) empirical knowledge, i.e. what a real offensive team playing the role of attacker can do in the situation.
However, it is clear enough that instead of only having a multi-agent framework or a human-based security assessment approach, it would be better, when possible, if our troops could rely upon both systems.
It is important to note that cyber offensive units could only simulate attacks based on what is already known (*a priori* information). In other words, they cannot perform unknown attacks. Nevertheless, they may devise new attacks with the twofold aim of either increasing their ability or checking the network at a higher level of security (empirical approach). However, we know that the organizational structure depicted in Figure 3 is not enough to guarantee security of either infrastructure or deployed networks. Nevertheless, our proposal has a good potential for verifying and assessing the level of security that operators should guarantee on sensitive and sometimes critical information stored over the maintained networks.
Based on the results of the survey, we believe that it is mandatory that signal units develop SOPs to guide and standardize procedures of installation, maintenance, and administration of deployed networks. SOPs should also refer to authorized software applications. A good habit would be to describe information leakage in terms of lessons learned which would eventually update SOPs. What we really suggest is to change the way of thinking of cyber-defense in favor of an empirical approach. Only by trying out information security can we assess whether our defense system is effective.

VI. LIMITATIONS AND THREATS TO VALIDITY

It is always difficult to generalize data collected in only one environment. For this reason we argue that our analysis has some threats to external validity that have to be taken into consideration when using our conclusions in a more general context. However, our organizational solution can be applied without limitations either to infrastructure or deployed networks. Based on expertise of the authors in international environments, we maintain that problems discussed in the case study are commonplace. Consequently, even though the surveyed population is not representative of the statistical population of the signal operators, we believe that technical and cultural problems identified in our case study are fairly common to operators of other nations similar to Italy. Therefore, the proposed results are worthwhile and can be taken into account before the deployment of operational units.

VII. CONCLUSIONS

In this paper we described real information leakage which took place during a multinational operation where Italy participated in. Our research questions aimed

at investigating whether cultural and technical aspects concerning military operators could affect the security of deployed networks. Even though the limitation of the performed survey could not be completely generalized, we showed that deployed networks are settled based on the idea that they are temporary and then do not require high security measures. The second point was that military operators believe that cipher devises can solve all information leakage problems. We showed that this is not the case mainly because there is no guidance for those operators to avoid information leaks which are not dealt with by ciphers.
Finally we illustrated an organizational solution to cyber defense which we called "empirical approach to cyber defense" such that it would be better to have two different and detached kinds of signal units: (i) those dealing with installing, maintaining, and protecting networks (cyber defense units) and (ii) those dealing with offensive tasks against either real attackers or their own networks. This approach would strengthen the defense attitude of signal units and check whether protection activities are effective and reliable.

VIII. FUTURE WORK

It would be worth using the identified variables to statistically evaluate whether there exists a significant correlation between those (independent) variables and information leaks (binary dependent variable). We also argue that our empirical approach to cyber defense should be tested in field before being applied. Therefore, further research is required in order to investigate whether or not having two detached kinds of units (defensive and offensive) is worthwhile and viable in practical terms.

FINAL REMARKS

F. Mulazzani developed sections 1, 2, 3, and Annex "A"; S.A. SARCIA' developed sections 5, 6, 7. Sections 4, 8, 9 were developed jointly by the two authors.

ANNEX "A"

1. **What is your rank?** (a) Soldier (b) Warrant Officer (c) form 2nd Lt. to Cpt. (d) Major or above.
2. **Do you have a degree on Information Systems or Telecommunication issues?** (a) Yes (b) No; If yes, what is the degree level? (a)High School Diploma (b) BSc (c) MSc (d) Specialized Master Course.
3. **So far, how many missions (including the present) have you attended dealing with IS or telecommunications issues?** (a) 1 (b)2-4 (c) 5-7 (d) >8.
4. **How secure do you believe your network is?** (a) Very secure (b) Secure enough(c) Somewhat secure (d) Not secure at all (e) I do not know.
5. **Among the following aspects, which one do you consider the best contributors to the security of the Mission network?** – you can choose more than one - (a) network encryption (b) firewall (c) intrusion detection (d) identity (e) access control (f) traffic monitoring (g) vulnerability scanning (h) anti-viruses (i) other – specify.

6. **Have you had or known of these events in the Mission network in the last year?** (a) Viruses or trojan horses (b) Employees steeling information or allowing unauthorized access (c) Hackers targeting your systems (d) Lost or stolen backup tapes (e) Lost or stolen computers or data storage (f) None, if other specify.
7. **In the Mission network which of the following is allowed?** (a) Network use policies for employees (b) Automated patch management for security (c) Smart password policy (d) Spam control (e) Spyware protection (f) Virus protection (g) Firewall.
8. **When was the last time that Mission network was tested for security issues?** (a) More than one year ago (b) In last year (c) In last 6 months (d) In last 30 days (e) I do not remember or I do not know.
9. **How do you feel confident in either creating new or maintaining secured data networks like the Mission?** (a) Highly confident (b) Very confident (c) Confident (d) Fairly confident (e) No confident.
10. **We don't want our packets to get lost in transit. Which OSI layer is responsible for ordered delivery of packets?** (a) Network (b) Link (c) Transport (d) Physical
11. **What can a firewall protect against?** (a) Viruses (b) Unauthenticated interactive logins from the outside world (c) Connecting to and from the outside world (d) other.
12. **This is a program or file that is specifically developed for the purpose of doing harm:** (a) Buffer overflow (b) Bastion Host (c) Malware (d) Ping sweep.
13. **This is a program in which malicious or harmful code is contained inside apparently harmless programming data:** (a) War dialer (b) Spam trap (c) Trojan horse (d) email.
14. **A way of verifying a message's integrity after transport across a network is through the use of:** (a) A message authentication code (b) Steganography (c) An encryption key (d) A cipher.
15. **Which statement best describes the advantages of public key encryption**? (a) Keys are exchanged publicly without an eavesdropper being able to decrypt messages (b) Knowledge of one's public key does not yield knowledge of their private key (c) Encryption performance is faster than secret-key encryption (d) A and B only (e) B and C only.
16. **Which of the following best describes what is removed from a hard drive when a file is deleted from the hard drive?** (a) The MBR record, the FAT record, and the Directory Table entry (b) The FAT record, the Directory Table entry, and the data clusters that the file occupied (c) The FAT record and the Directory Table entry (d) The FAT record, the Directory Table Entry, and the Partition Table
17. **What is a secure process for keeping confidential information private?** (a) GnPG (b) PGP (c) network cipher (d) password protection (e) other.
18. **What do you think would be the main reason for most of the information security breaches?** (a) external hackers (b) poor programming (c) internal employees (d) bad firewall settings.

19. **Do you know ISO/IEC 15408?** (a) yes (b) No **– If yes what is that for?** (a) instructions to create secured security sytems (b) evaluation criteria for IT security techniques (c) cypher certification to be used in networks like Mission (d) other, specify.
20. **Do you use any SOP developed by the Army to install/maintain/supervise a secured network like the Mission?** (a) Yes (b) No – If yes, can you tell where this SOP is available (a) don't know, I got it from friends (b) it is a restricted document, can't tell (c) from an Army web site, please specify.

REFERENCES

[1] Department of the Army, Signal Soldier's Guide - Field Manual, March 2009.

[2] Italian Army General Staff – Security Office, "Software Systems, Telecommunication and Security – Unclassified documents, 2008.

[3] Italian Army General Staff – Security Office, "Software Systems, Telecommunication and Security – Classified documents, 2008.

[4] ISO/IEC 15408-1, Information Technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model, 2009.

[5] ISO/IEC 15408-2, Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components, 2008.

[6] ISO/IEC 15408-3, Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components, 2008.

[7] U.S. Department of Defence, Trusted Computer System Evaluation Criteria, December 1985, DoDD 5200.28-STD.

[8] U.S. Department of Defence, Directive: Information Assurance, October 2002, DoDD 8500.01 E.

[9] Bundesamt fuer Sicherheit in der Informationstechnik, "Application Notes and Interpretation of the Scheme (AIS): ITSEC to CC Mapping with Specific Attack Potential," 2010. [Online]. https://www.bsi.bund.de

[10] ISO/IEC 27000:2009 Information technology – Security techniques – Information security management systems – Overview and vocabulary (2009).

[11] F. Hare, "The Cyber Threat to National Security: Why can't we agree", in Conference on Cyber Conflicts, Tallin, Estonia, 2010, pp. 211-225.

[12] S. Liles, "Cyber Warfare: As a Form of Low-Intensity Conflict and Insurgency", in Conference on Cyber Conflicts, Tallin, Estonia, 2010, pp. 47-57.

[13] I.V. Kotenko, "Multi-agent Modeling and Simulation of Cyber-Attacks and Cyber-Defense for Homeland Security," IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Dortmund, Germany, 6-8 Sep. 2008.

[14] I.V. Kotenko, A.V. Ulanov, "Agent-based simulation of DDOS attacks and defense mechanisms," Journal of Computing, Vol.4, Issue 2, 2005.