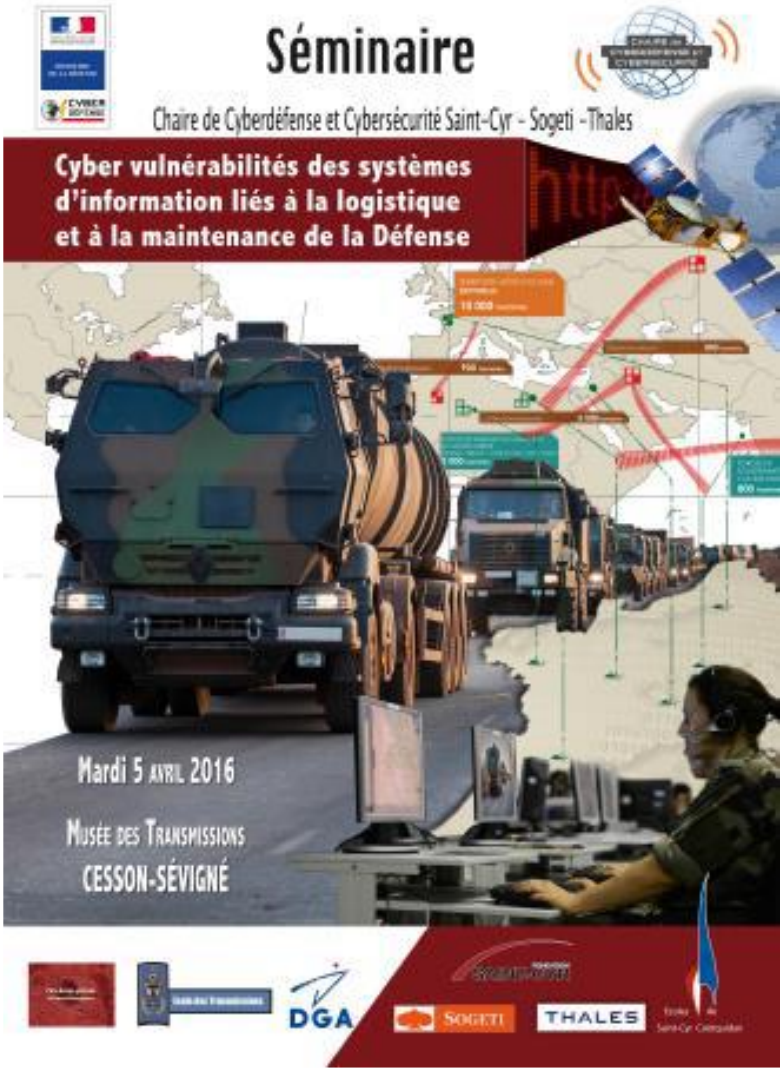
Cyber vulnerabilities of information systems related to logistics and maintenance of the Defense

Tuesday, April 5th, 2016 - Musée des Transmissions de Cesson-Sévigné



Summary Report of the

Seminar for the Saint-Cyr Chair of Cyberdefense and Cybersecurity - Sogeti – Thales

Translated from French

Presentation

Logistics and maintenance have a central role in the design and management of logistical support for external operations as well as on national territory. They include the materials to support troops, transportation, requests, supplies, repairs, and assistance deployments to units.

Nowadays, in order to be more efficient, there is an increased use of logistics and maintenance information systems, which allow for better anticipation and reactivity in the planning and management of operations. This goes together with an increase in the exchange of information with civilian companies to which office maintenance and logistics functions have been outsourced.

However, "cyberconflict," which is now an important component of conflicts in general, can effect these systems and paralyze or disrupt their proper functioning. It is therefore important to take cyberthreats into account in the design of these systems and their daily operational implementation. Properly controlling them is crucial to ensure efficient logistics and maintenance to support our forces.

This is one of the challenges that lies ahead for land logistics in the future, and this is why (following the three previous seminars) on Tuesday, April 5th, 2016 Écoles de Saint-Cyr Coëtquidan organized, with the l'École des Transmissions and DGA Maîtrise de l'information, as part of the work of the Saint-Cyr Chair of Cyberdefense and Cybersecurity - Sogeti - Thales, a new seminar on "Cybervulnerabilities of information systems related logistics and maintenance of the Defence." Here is the summary report.

Glossary

CCPA : Centre de cyberprotection des armées.
CEPIC : Commandement des programmes interarmées de cyberprotection
CSOA : Centre de soutien aux opérations et aux acheminements
CTTS : Centre de transport et transits en surface
CVSS : Common Vulnerability Scoring System
MCO : Maintien en conditions d'opération
MCS : Maintien en condition de sécurité
NEB : Numérisation de l'Espace de Bataille
RFID : Radio Frequency Identification
RSSI : Responsable de la sécurité des systèmes d'information
SIA : Système d'information des armées
SIAG : Systèmes d'information d'administration et de gestion
SIL : Systèmes d'information logistique (LIS – Logistics Information System)
SILRIA : Système d'information logistique de suivi de la ressource interarmées
SIOC : Systèmes d'information opérationnelle et de commandement
STCIA : Socle technique commun interarmées

Introduction

During the Battle of Verdun in 1916, the French Army was able to hold the font by establishing an enormous military logistics operation to carry equipment and supplies to the front and also to rotate in the freshest possible troops in order to oppose the Germans. This operation was carried out using the Voie Sacrée ("Sacred Way"), a road that connects Bar-le-Duc to Verdun, which was vital strategically and allowed for the weekly transport of a total of 90,000 troops and 50,000 tons of materials by traversing almost one million kilometers in all and mobilizing 3,500 trucks. This logistical effort enabled France to win a decisive battle for the outcome of the First World War.

It is through this example that general engineer (ingénieure générale) Marie-Noëlle Sclafer stresses the importance of approaching logistics from a cyber-perspective when managing a military venture. Because they do not deal with operational information and because they operate on the periphery of weapon systems, logistics systems are often unclassified, and for security reasons remain not very visible even though they are essential in order to conduct proper military operations. These systems are open to the outside world and are heavily interconnected with highly classified systems but also with the chaotic world of cyberspace. It is always the weakest link of a structure and is targeted by attackers; the logistics information system therefore becomes a target, especially by opportunistic attackers. This does not go against the direction in which technologies related to weapons and support are evolving. They present opportunities and enable significant gains in the field as financial gains. Also, it is imperative to make these advancements secure in order to make the most of them.

A – The place of logistics within the NEB: importance of logistics flows and maintenance within MINDEF's missions

A.1 – The specifics of military logistics through practical cases

In his general presentation about military logistics specifics, Colonel L'Hostis recalls that historically the military leads logistics. In the nineteenth century, Baron Antoine de Jomini, a contemporary of Carl von Clausewitz, drew a link between logistics and tactics. According to him, logistics is "the practical art of moving armies," resupplying is therefore necessary to have satisfactory conditions. Logistics are compared to an umbilical cord: When command can rotate troops to Verdun, when the effort is focused on artillery because it has many quality shells for the artillery equipment, when the French Acrmy resists ten months thanks to the Voie Sacrée, it is easy to see the full importance of logistics. This is illustrated well by the Battle of Verdun in 1916 with the Voie Sacrée. Looking back in history, this part of military logistics is illustrated during the landing of June 6th, 1944 (invasion of Normandy). We often forget that the logistics operations started at the beaches and that the delivery of munitions, fuel and all the necessary resources, in this context, is a feat especially since at the time the military did not have information systems like today. General Dwight Eisenhower said in 1944: "There are no tactics without logistics. If the logistics said no, it is because it is right"[1]

[1] Original quote in English unknown, original French translation in text: "Il n'y a pas de tactique sans logistique. Si la logistique dit non, c'est qu'elle a raison."

and his contemporary Somerwell added: "Good logistics alone can't win a war. The bad logistics alone can lose it."

Colonel Philippe L'Hostis draws attention to the fact that the widespread practice of maintaining order through the military in overseas operations in recent years has made some forget about the importance of logistics. In the late 1950s, logistics "leadership" shifted to civilian companies with the emergence of new technologies and information technology. The military then began to follow, even if pulled the private sector, though military logistics keeps its specific features. It has the function of supporting military administration (in terms of administrative, legal and financial functions) and offers support in order to: live, fight, and mobilize (health, safety, medical support, petroleum, troops, munitions, transport, environmental protection, maintenance requirements, and stationed resources). Faced with these multiple tasks in different domains, information systems are a way to meet these demands with the objective of keeping a global vision and good performance. Since then, the military has begun improving performance with the clear objective of building the supply chain, to increase jobs, troops or finances, for example. For a logistician, anticipation, management and distribution are very important and he or she must find the right balance between storage and distribution. But the reduction of troops and land can necessitate using the international private sector, which can cause security problems. In the organization of the supply chain, distribution is a part of the process that is important for performance in terms of acceleration of the logistics flows and management of the resource in reverse logistics. This is the return of repairable spare parts to France to reintegrate them into the industrial supply chain for reconditioning. In the organization of the supply chain, this point is crucial and it is imperative to become more and more efficient in the field of reverse logistics. Distribution adapts to storage as logistics adapts to tactics. It involves sending, within a few days in national territory, the correct quantity of resources with the effective assistance of information systems.

The Centre de Transport et Transits en Surface (CTTS) implements transport functions at an inter-armed forces level. It organizes national and regional transport missions and factors in the management of transit platforms and regular lines. The Centre de Soutien aux Opérations et aux Acheminements (CSOA) has functional authority over the CTTS, it deals with routing and delivery.

- Transport is the moving of a resource without transit or customs operations. In other words, it is a movement on the mainland without changing the mode of transport (road, air) from point A to point B.
- Routing (acheminements) is a combination of transport types (change of mode, customs operations).

These were looked at in the examples of the operations SERVAL and KAPISA, given to demonstrate the importance and specificity of military logistics. The vulnerability of convoys (soft targets) for example that are moving for several days must be given serious consideration. A military logistician must anticipate moves, understand tactical maneuvers, and work to maintain stability for the logistics actors to work. The tactician must give the logistician the capacity to respond to provide the support needed. In short, we must never forget that logistics are an area where we must be very vigilant as it is a vulnerable easy target.

A.2 - Cyber vulnerabilities of existing systems and the need to take them into account

Logistics Information Systems (LIS or Systèmes d'Information Logistique - SIL) overall have the same vulnerabilities as operations and command information systems (Systèmes d'Information Opérationnelle et de Commandement - SIOC). However, LIS vulnerabilities impact many areas. Lieutenant Colonel Thierry Kessler-Rachel begins by talking about the role of the Centre de Cyberprotection des Armées (CCPA). Under the authority of the Chef d'État-Major des Armées (CEMA), it handles the assessment (certification) of information systems, performs controls and produces reports linked to cyberdefense. The CCPA is part of the Commandement des Programmes Interarmées de Cyberprotection (CPIC) alongside the Centre Interarmées pour l'Administration et l'Interopérabilité des SIOC (CIADIOS). The latter has a different vision and process model, showing the information systems using different maps. The best known, the land occupation maps (le plan d'occupation des sols), allows decision makers to visualize where the information systems are located and how they interact. The Systèmes d'Information d'Administration et de Gestion (SIAG) and SIOC are grouped by functional zones. The logistics functional zone is under the authority of a manager who makes all the decisions on projects related to LIS. The logistics functional zone is divided into four functional areas that correspond to different types of equipment (land, aeronautical, naval, health, etc.). The objective of CIADIOS is to streamline all information systems to, for example, prevent duplication. It also formalizes the tasks for the military (interservices) in a process of procedures designed to maintain good operating conditions (Maintien en Conditions d'Opération MCO) by splitting up operations in order to automate and better define the requirements. All this is useful in order to understand the potential impact of exploitations of vulnerabilities in the information systems.

The person responsible for the logistics functional zone reminds us that the LIS must be secure and the projects under control. The logistics functional zone is strongly linked to other domains (human resources, health, finance). LIS is subject to the usual vulnerabilities of SIOC but they can, however, be underscored. They are interconnected with many other elements such as weapon systems and external partner systems. In addition, LIS are studied differently from SIOC. The usual canons of risk analysis for the SIOC highlight confidentiality. Moreover, secure networks are specifically designed for this. Because they are highly interconnected and because they permeate to many tasks, LIS are not generally classified as confidential but restricted. The availability of LIS, however, is of paramount importance as SIOC rely on globally available support networks (like the satellite network for example). Integrity, in both cases, is treated the same way.

The exploitation of cybervulnerabilities can impact the sytem integrity and allow for direct access to weapon systems, with the possible effects of collateral damage to financial or commercial partners, the delivery of equipment, or the military's reputation can be undermined. The vulnerabilities of information systems are usually split into several possible categories:

- **Governance, employees of the project**. If there is no authority employed, the chief information security officer (CISO or Responsable de la Sécurité des Systèmes d'Information - RSSI) in the case of obsolete systems, for example, cannot ensure proper management. Without governance and structure in the project, there is no

direct administrator. This weakness prevents the overall implementation of corrections and updates.

- **Various heterogeneous information systems.** This involves many different professions, numerous personnel and issues of obsolescence of software and hardware.
- **Maintenance of security conditions (Maintien en Condition de Sécurité MCS).** The implementation of MCS is generally a complex process.
- **Default system configurations or support network**. These vulnerabilities are due to non-compliance with security rules by the user who does not refer to the guidelines.
- **Support network.** It may have vulnerabilities as well the extensions of it.
- **Increased technicality of information systems**. Complicated administration, which must be supported by the manufacturer.

Overcoming these flaws is not easy. One first needs to know exactly what there is to defend then to understand the implications of an attack on the system. One must also use assessments and certifications, allocate finances and educate the hierarchy of the risks and safeguards associated with the use of the system. For this, it is possible to set up risk management tools for potential risks and there should be an appointed RSSI. As a means of threat detection, we are able to install sensors. It is also possible to reduce the surface area of attack by returning to less sophisticated methods, but that would prevent the use of new features and advances, which could allow for technological developments. To deal with an incident in a given timeframe, working in a downgraded mode can be a short-term solution (fax, transport), as well as the use of a reservist if he or she is well trained to react or the establishment of a continuity plan. To summarize, knowing what there is to defend involves doing the necessary mapping of systems to then being able to understand the risks and initiate response plans to reduce them.

B – Considering Vulnerabilities

B.1 – Considering the security of logistics systems: requirements in their definition and the administration / control of the systems

During this seminar, Michel Vieillard highlighted the importance of integrating information systems with a comprehensive approach to security. The securitization of information and weapons systems are most often safeguarded to protect information and their accessibility is not fully taken into account with security measures under the pretext that maintenance systems do not transmit sensitive information. But now, as everything is more and more interconnected, new technologies make it difficult to secure defense systems, operational information systems, and systems for logistics information and weapons, and systems for the private sector, infrastructure and services. The idea of overall security is of paramount importance; for example, on an airplane, the weapons system, support systems, and all others will be interconnected and without taking into account the security of all these interconnections, the aircraft may stay grounded. Remember, security risks can come from the environment and they can potentially have consequences for the system, as safety risks can come from the system that can have potential consequences in the environment. Specifically,

malicious acts concern security and accidents concern safety according to the model defined in the thesis of Ludovic Piètre-Cambacédès on the relationship between safety and security.

There is a dematerialization and a digitization of exchanges and the use of off-the-shelf[2] computer products create more cybernetic vulnerabilities. The MCS aspect is also considered very important: It is possible to deliver a highly reliable and efficient product (system) that can guard against known attacks, but if the MCS is not implemented and tracked over time, the product (system) can become vulnerable. Yet there is an increasing digitization of weapons systems that place strong constraints on the military operational staff in terms of operating the systems. This results in an increase in the outsourcing of maintenance systems that leads to a proliferation of interconnections with the private sector, allowing for new vulnerabilities to emerge if these information systems are connected to the internet. The DGA studies the risks in terms of the overall security of all systems, whether it is the systems for weapons, support, information or maintenance. It takes factors in the need to establish and follow the maintenance of security conditions (MCS) protocols or risk the threat becoming bigger and bigger. In fact, attackers will follow all security system developments. Without updates, they may be able to penetrate systems.

One LIS security solution is to put them on already secure systems, on INTRADEF and INTRACED, or the joint military technical platform (Socle Technique Commun Interarmées STCIA). In all cases, securing systems is a constant process that does not become stronger over time. We must therefore consider the entire lifecycle of systems and look at LIS like the interface systems with weapons systems, interfaces that must then be secured or one could risk seeing them become a weak link in the system. Beyond these protective measures, the priority of the SSI centers is to consider cyberdefense (lutte informatique défensive - LID) in deployed systems with the goal of having a constant view of a system's security status.

The private sector is potentially a weak link because its platforms are less classified and an attacker can easily test the security of a company. This creates the need to analyze the security and risks to identify threats and incidences, to know what to protect, and to understand the impact on systems. Note that cooperation is very important in the development of certain weapons systems like the Tiger helicopter for example. Similarly, elements in these systems that are particular to France « spécial France » should be looked at; they are cooperatively developed and this concerns the maintenance of the condition of the equipment, we must do the same with the MCS. It has become imperative to consider system usability in order to limit human errors because if the security mechanisms are too restrictive, users will bypass the security mechanisms in order to do their jobs (a military response to an emergency situation requires an immediate reaction). Another risk involves the impact of the classification of materials in logistics systems because this can create new areas of the service that are very restricted.

In conclusion, the DGA prepares for the future, launches initiatives on new technologies and supports the forces to control cyber-risks linked to these new modes of operation. Security must be understood in a comprehensive manner, including all the system life cycle phases and protective measures must be imposed on manufacturers. Lastly, LID measures should be implemented on all systems (network sensors or detection for example).

[2] A product that is mass produced and not specifically for a project. They are used to reduce design, manufacturing and maintenance costs.

B.2 - The example of the Air Force in the supervision of logistics flows, looking at threats and corrective measures (MCS)

Commander Martin and Commander Bustos-Salidas try, within the Groupement Aérien de l'Informatique Opérationnelle (GAIO), to include software engineering (to develop SIO for the Air Force), support operations (administration and support systems essential for flight operations, implementation and securitization of tablets shipped in airplanes) and cyberdefense missions (MCS of LIS and SIOC, cybersurveillance, and the creation of a hub for intervention). MCS has three objectives for the Air Force: a) the first is to understand the limits of our cyberspace. This is an ongoing challenge because every day applications appear and disappear and make the contours of cyberspace blurred, shifting, and dynamic. Being able to map, identify and describe the applications is certainly not easy and involves understanding the components, defining and identifying its physical and logical limits, and modeling its internal and external dependencies. b) Secondly, MCS allows one to set an acceptable level of confidence, to evaluate, to determine the level of safety of the system, and to meet accountability requirements. c) Third, it must be able to be used as a basis for information in the case of a cyber-incident, to determine the operational impact (and thus the loss of capacity), to confine the incident and then to eradicate the threat and to recover to make the system healthy. The more the system is defined qualitatively, quantitatively and geographically, more effective the cyberdefense capabilities will be.

The implementation of MCS in the Air Force is done through the RSSI using a dedicated system created by GAIO, called PAVENSIS. The MCS also relies on the Centre d'Analyse de Lutte Informatique (CALID), which transmits known vulnerabilities to GAIO and requests appropriate solutions. GAIO uses the CVSS (Common Vulnerability Scoring System) and helps the RSSI to determine the level of criticality and in developing corrective measures. MCS allows one to maintain the level of confidence in the system until the end of its life cycle. In regards to LIS, we can say that they are vulnerable. Some may be outdated because the life cycle of an information system does not necessarily accommodate the life cycle of the equipment. They are often isolated because they are too dedicated to one area such as being strongly associated to the equipment. Nevertheless, all systems must work together and the means of exchange are already implemented sometimes via USB, even if the interconnection of systems is updated. Thus we end up with obsolete systems making numerous exchanges. If we add State control to this, which is partial because it is in part entrusted to the private sector, there is an expansion of actors involved. Lastly, we have no transparency in terms of the software components provided by the private sector and the condition of the supplied components. However, to integrate MCS in overall security, we must be able to predict the processing times in order to plan ahead with determined procedures and integrate and formalize non-regression testing. We must, consequently, integrate the private sector in the MCS process. The threat is global and the response must be global. There should be a set of requirements respected by the manufacturers, they should provide the inherent vulnerabilities in their software components. The Air Force has reached the first level of maturity regarding MCS, of which GAIO is in charge. With the knowledge of a new level of threat, the trained mangers of the SSI should be armed and have the sufficient maps to fill in gaps.

B.3 - NATO: What are the responses regarding the vulnerabilities in the supply chain of the alliance?

According to Colonel Jean-Luc Mercadier, NATO has software (logistic apps) to manage logistics. There are two networks in NATO, one dedicated to operations (very secure, classified NATO SECRET) and another dedicated to business (less secure, classified NATO RESTRICTED or NATO UNCLASSIFIED). Logistics is considered relevant to operations and thus it remains very compartmentalized, nothing is accessible through the internet. A LogFAS (Logistics Functional Area Services) is an application among others (ADAMS, EVE, CORSOM) that supports the logistics division of NATO that covers many areas including the delivery of resources. It relies on a common database that can be interconnected with the outside world. These software modules are integrated in defense planning as well as operational planning. Through the logistics system ADAMS, the NATO system is connected to the national deployment systems, which involve many interfaces (one per country) and therefore many points of vulnerability. Thus each nation brings themselves up to the security standard. To this end, the future version of logistics software will use a service bus architecture that helps streamline interfaces and thus better protects them.

NATO is a strategic concept based on three pillars: collective defense, crisis management, and cooperative security. Since 2002, all statements that followed NATO's summits talked about the cyber domain. Article 5 (specifically on collective defense and the Alliance) has, since the Wales summit in 2014, raised the issue of responses to cyberattacks to the highest level. That is to say that the collective response to a cybernetic attack of a member country is now confirmed. This is not a new subject to NATO as one nation already suffered a major attack: the infrastructure of Estonia, for example, was attacked in 2004 and was then defended by the Alliance. Moreover, NATO has assessed the impact of military cyberattacks by observing the paralysis of the command infrastructure of Georgia during the Russian attack in 2008. To deal with this, NATO has set up a policy on cyberdefense that focuses only on its own resources (the command structure), leaving the States to manage the protection of their national systems in a sovereign manner. The cyber stance of NATO (defensive only) therefore essentially focuses on the SIC that are owned and operated by NATO. The Alliance also protects national extensions because they support the system for consulting allies, which is vital to their ability to react as a coalition.

The idea of "cyber" is found at every level, including on the North Atlantic Council where the Defense ministers are found. The two NATO strategic commands share capabilities: the Allied Command Transformation (ACT) leads the initiatives to transform NATO's structure, forces, capabilities and military doctrine and the Allied Command Operations (ACO), located at SHAPE, is responsible for the planning and execution of all the Alliance military operations. SHAPE is developing a body that addresses "cyber situational awareness," which relies on studies about threats against systems, network conditions and finally it looks at the impact these threats can have on operations. One cyber "task force" is dedicated to this task. "Cyber as a domain" can be looked at as if it were another type of space like the air, sea, land and space; this would be part of the cyber-division at SHAPE. This gives the operations command the ability to coordinate with national actors and, in case of war, to absorb the legal parts of a conflict and thus to implement a whole range of strategic options in response to an incident.

C – The logistics information systems of today and tomorrow

C.1 - SIA: the future information system of the military

The information system of the military (Système d'Information des Armées - SIA), launched in late 2012, was presented by Lieutenant Colonel Samuel Duval and Jacky Tétaud as a system that encompasses SILRIA. The goal is to factor in the digitalization of operations, providing an overall guarantee of functionality to meet the needs of all in the environment. It is the sole successor of many SIOC and in particular the SIOC: SICF, SIC21, and SCCOA. It provides coherence to the participating SIOC and implements some subsystems. This system, created based on the idea that closer integration is necessary, is based on the Socle Technique Commun Interarmées (STCIA). The goal is to pass from the logical stand point of military spheres to tasks, combat is joint by nature and so are logistics. The building-blocks (SIAC2, SORIA, SILRIA) will be integrated little by little into the STCIA base. Built on joint technical platforms, different services (directories, email, document management, etc.) are made available to the entire system as are all the security services.

The information system factors in SSI in a comprehensive and coherent way to provide high-level protection, security, integrity, availability and reliability. It relies on platforms (STCIA, STC E) to bring the security services (GSYS, GSEC) to the entire SIA on the intranet (INTRADEF, INTRACED). To ensure overall sustainability, the principles of MCO and MCS will be applied. Services provided by the STCIA (document repository, collaborative work portal, instant communication) are also safe: secure OS, integrity control, antivirus, access control, unique authentication, auditing, and remote access. We must find a balance between the features of the system and its deployment in order for it to be used effectively under real conditions. The SSI essential functions in place are protected by strong authentication with the introduction of smart chips, with IGCNG certificates, with two authentication systems in series, and finally with authentication through the use of “macro-droits et de micro-droits” (macro-administrative rights and micro-administrative rights). There is a partitioning of the network with one dedicated to technical administration (unique access), including physical separation from the network infrastructure and operating and administrative networks, and user workstations. Operator workstations are on a dedicated LAN. In terms of the principal SSI functions, business continuity plans or recovery plans (PCI / PRI) are implemented to ensure wide system accessibility. There are also monitoring functions and cyberdefense (lutte informatique défensive - LID) supervision through centralized logs with the GSEC application. There is also a technical oversight and centralized operational tool (GSYS). The integrity of the system is accounted for through antivirus solutions (on user workstations, servers, email). An electronic signature device is linked to the official email.

It should be noted that the challenge in 2016 is the transition of the SIA onto FROPS 2.0, which follows the FROPS 1.0 deployed by DIRISI and is a system that allows exchanges on the national, bilateral and combined levels. The changes to SIA built on FROPS ensure continuity of end-to-end exchanges between France and the theaters of operation.

C.2 - Operational challenges of controlled security: SILRIA

SILRIA (Système d'Information Logistique de Suivi de la Ressource Interarmées, a logistics information system to track inter-service military resources), explained Lieutenant Colonel Duval, aims to ensure the traceability of logistics resources in transit and provide an organizational tool for routing and movement. Once the resource is sent by the sender, the logistician requests a transport-delivery directed to CSOA. The center chooses the mode of dispatch and reserves the types of transportation that it prioritizes according to the resource and the theater of operation. Once the orders are given, the resources are followed because each time they pass a logistics node, an event is created which ensures traceability. SILRIA offers a content management tool for contents as well as containers in inventories (especially for containers). At the end of the chain, the receiving unit confirms the correct delivery (quantity and quality) by sending the information to the information system. More specifically, the user created a unit to transport (that can be one resource or several) on which he or she sticks an RFID tag and also a barcode. SILRIA produces all transit documents required for the delivery (customs, transport manifest of hazardous material). Starting from the loading and shipping, the parcel is entered into the delivery system and it is followed throughout the possible disruptions to reception. RFID technology uses radio frequency identification. SILRIA requires the installation and collection of new equipment: specific barcode terminals (for interoperability with NATO systems that often still use the barcode), portals that can read groups of packages and pallets, terminals that can read RFID tags passive and active, laptops, SILRIA mobile kits (in theaters of operation), printers (for labels), and RFID reading points for storage container areas.

Patrick Delorme clarified that behind SILRIA there are modules that handle the organization of transport, logistics flows and exchange interfaces, for example. Similarly, the datacenter module reports on the operations conducted on SILRIA. The system is built into the SIA program like “bricks” laid on STCIA, along the same lines that the building-blocks for security, management and technical service are integrated. Thus SILRIA benefits from the SIA security programs. Once the security analysis is done, there are basic rules to ensure the security of the system. Specific terminals, dock doors, and active antennas are points of vulnerability for example; organizational measures must be implemented that address these vulnerabilities. It should be noted, and this is very important, there is no WiFi transmission on SILRIA, this was a decision made so as not to run into difficulty securing the Ministry of Defense (Ministère de la Défense) warehouses.

Captain Palacio details three major families of interfaces: resource management (SIMAT, SILCENT, ATAMS, etc.) that provide SILRIA with the description on the package to ship, the fleet manager (ARTEMIS) that manages all the mainland transport missions of CTTS to the military and services, and the financial management (HERMES) that contracts out road transport to civilian providers. Each interface produces different communications (packing, delivery, reception, transport requests, cSonfirmation / cancellation of an order). A logistics interface module (Module d'Interfaçage Logistique - MIL), part of STCIA, mediates between partner systems and SILRIA via a service bus. It is possible to send exchanges by file, web service or email. Internally, a MES (a second service bus) allows for MIL to reprocess messages in order for them to be integrated into SILRIA. There are several feared scenarios,

such as the loss of a connection point between SILRIA and partner systems, eavesdropping to pick up data, a lack of control over the origin of information, disclosure of sensitive data to a third party, or the capturing of a file transfer. Faced with these undesirable scenarios, solutions have been put in place: authentication to access the MIL, PRI PCI with a backup site, format controls, rules for dealing with communications by corresponding systems that meet specific business rules, protection mechanisms (certificates), and logging of exchanges.

Lastly, Guy Venture lays out the various risks related to the use of RFIDs and the solutions envisaged. He first highlights the differences between RFID and WIFI. The latter allows access to a network while the RFID only captures information. Under SILRIA, a transport label (passive RFID) is produced to be read by TS (mobile PDA) or at a dock door for large volumes. For the active labels headed for containers, there are two possible devices: the mobile PDA and the fixed reading point for active RFID (PLFRA) to automatically capture information on the entry and exit of the zone.

What are the risks inherent in such a system?

- Cloning: this is when a label or tag is copied exactly. This can easily be achieved because standards come from the market and are public. To counter this threat, we can associate the SSCC code to XTID (registration plate chip) which alerts us to wrongdoing.
- Impersonation: electronic device that responds like a label/tag but without being able to reproduce the visual. The product messages however is not perfect and can be detected by analyzing the signal.
- Denial of service: interference or overwhelming of a reading device by emitting false signals. The solution may involve looking for the source to neutralize it (site survey radio), or using the barcode as an alternative to RFID.
- Tracing: RFID is used to remotely monitor an object and thus potentially a military convoy. To counter this threat, it is possible to put an active tag to sleep or to remove the segment at risk.
- Replay: the recording of the information exchange (radio) after recording, is very difficult to implement.
- Relay: the introduction of a device between the tag and the reader allowing the tag to move farther from the reader while maintaining the connection.
- Brute force: transmitting a series of random or sequential codes to penetrate or disrupt a system until causing a denial of service.
- Destruction: the deactivation of a tag. The label can be reprinted and the active tag replaced. We must monitor sites to ensure that there are no malicious actors.
- The illegal transmission of data: some tags have a memory capacity capable of carrying information without the knowledge of the transporter. However, there is no “user memory” on SILRIA labels, and the active tags are erased at each logistics node, which reduces the scope of the threat.
- Virus: theoretically possible but very difficult given the very low level of memory in the RFID tag.

C.3 – Outlook on future logistics systems

The outlook, presented by Colonel Jean-Louis Vélut, looks at the 2025-2030 time horizon. Logistics is a complex world that connects many players. When we speak of support, we speak in essence of a complex world. In addition, the French military and in particular the Army can intervene in often difficult air-land environments: with uneven advantage due to the geography, in contact with the local populations (friendly or hostile), with the deployment of often dispersed ground forces, and with weak logistical self-sufficiency. From entering the theater of operations up to the communications units, the support of these ground forces requires implementation time that is difficult to shorten. Lastly, the logistics of an operation should be scalable and responsive to adapting to the changes in pace and intensity of commitments.

The concept of supporting the Army follows several guidelines, which have an impact on the LIS:

- Unicity of a maneuver: it involves incorporating and integrating all support tasks. The LIS must, therefore, be able to synthesize data.
- Savings: soldiers have a duty to save often limited resources (e.g. guided munitions) and with accurate data provided by the LIS, these savings can be realized.
- Adaptability: for a logistical deployment to be effective on the ground, it should be adapted to the forces. The information systems architecture must facilitate this ability to adapt.
- Continuity: the support of ground forces is a continuous support. Data links and servers must be secured to avoid disruptions and data loss.
- Anticipation: the logistician needs to be able to anticipate maneuvers. He or she must rely strongly on calculations, assessment and forecasting.
- Responsiveness: usability of software.
- Ability to last and endure: hardiness of the hardware.
- Ability to deliver anytime anywhere: interoperability, particularly with coalition allies.

LIS are still in the process of evolving, thus helping to optimize performance and reduce financial costs (allocated for maintenance of outdated LIS). The opportunities for development are numerous. Regarding the logistics of weapons systems, predictive maintenance is an interesting area. It involves using sensors to detect if certain systems or subsystems will pose problems (wear, obsolescence etc.) at a given time so that replacement components can be provided. In the near future, connected objects will be part of everyday life for a soldier, particularly in the field of health (medical bracelet for example). Robotics is a growing trend in the civilian and military worlds. It is likely we will see in next ten to fifteen years the first semi-robotic convoys of helicopter drones, or the automated handling of their operations. In this area, the Americans and the Israelis are ahead but these technologies are still very expensive. In addition to cost-effectiveness, these devices pose ethical issues (for example, what perception will the population have about robotic convoys?). Taking the example of the regimental information system (Système d'Information Régimentaire - SIR) used by the Army, Colonel Vélut draws attention to the need to improve the human-machine interface. If an interface is too complicated, then there is a reduced effectiveness in using the system. In this area, the civilian world offers interesting solutions.

The Army is developing a plan to update its equipment: the SCORPION program. It revolves around the arrival of the GRIFFON that will replace the VAB, and JAGUAR that will replace the AMX 10RC. Beyond these new vehicles, SCORPION will incorporate through infovalidation (optimizing the exchange of tactical data) a set of weapon systems. In this context, a new information and communications system, the combat information system for Scorpion (Système d'Information du Combat Scorpion - SICS), will be central to this infovalidation. The latter will also affect logistics. Moreover, support for SCORPION units, which are highly reactive and mobile, will probably necessitate the development of new modes of action in logistics.

Cyber-risks are considered in ongoing studies. Their origins can be linked to organized groups or hostile military actors. Even a low cost approach (such as the extraction of big data) can cause considerable damage for a unit. Cyberattacks can impact, for example, the world of health and medical confidentiality, rare and crucial resources support, and outsourced support. It is important to protect tactical and logistical data used by our forces in order to preserve their security, and if necessary, to allow their use as part of legal investigations. Lastly, LIS ensure efficient land logistics, if cyber vulnerabilities are considered and protections are in place. From this perspective, the adaptability and training of users to use the digital systems of tomorrow are crucial.

D - Increased outsourcing and interconnection with the Internet: advantages and dangers

D.1 - Military and commercial interfaces supported by LIS: vulnerabilities and solutions

Under the public-private partnership signed between the Ministry of Defense and the group OPAL Defense (of which THALES company is a part), Wulfran Charnoz presents the organization and the cyber challenges of the information system designed, deployed and managed by Thales at a Balard location (seen as an extension of INTRADEF). The information system is made available so the Ministry of Defence can store a number of applications to be used. The physical site is protected by access controls, intrusion detection and video surveillance. Clean rooms (“salles blanches”) are available to allow the Ministry to install the applications they need. The CPCO part, where the logistics component is present, is connected to the core network managed by the manufacturer. The flux supports of these LIS pass through the SIC, which are operated by THALES. Their accessibility is managed under the partnership. Regarding the assessment and certification of all the SIC on the Balard site, many efforts are carried out like risk analysis, engineering and validation, and security. Having an approval certification is meaningful only if we maintain an acceptable level of safety over time. To assure optimal security, it is therefore necessarily to implement MCS coupled with a number of operational and technical measures that control the interfaces between the system and the bases of the manufactures. The MCS facilitates one to make an objective analysis of vulnerabilities, measure changes in risk levels so that they are at acceptable levels and where the risk exceeds the acceptable threshold for approval, it uses corrective patches or any other operational or technical measures. The MCS process covers the design and operation phases. When developing a system, it is necessary to model, the

automation of many actions at the time when the process takes place. Once the set of alerts are within the tool, it automatically analyzes the characteristics of the problems to calculate a first environmental CVSS score. For example, if a vulnerability is exploitable through the internet but the system is not connected, the issue may have a very high CVSS environmental rating, its CVSS rating will remain fairly low. This will allow them to collect a number of the vulnerabilities for the CVSS that are less critical for the system and integrate them into the MCO cycle. If there are large vulnerabilities, a more detailed analysis is carried out that can lead to the development of an emergency patch. These are validated with a reference platform at THALES before production. These measures are taken to avoid introducing viruses on the trusted domain at Balard and to ensure that the product installed on the site is the one that was validated with the reference platform. All incoming data is passed through clean stations, always with the aim of fighting against viruses. To maintain the accessibility and integrity of the Balard sites, they are held to the MCS process and they ensure that any developments incorporate safety measures. The current trend for MCO equipment integrates signature stations that allow for one to sign and encrypt source codes given to clients. This measure ensures that things introduced into the equipment are legitimate.

D.2 - The Box@SME (Box@PME): a remote security solution among subcontractors

This project, presented by Olivier Mesnil (Soprasteria) aims to secure the supply chain from end to end. Currently, major organizations and the State use many particularly vulnerable subcontractors. In the aerospace industry, 70% of the value of an aircraft is created by thousands of SMEs, which become a multitude of potential weak points. SMEs are much more exposed than larger organizations because they do not have the same resources, financial or human. Drawing on this, the project is to create a network of SMEs to provide them with collaborative and shared security, by proposing a network box linked to a cybercenter that is able to respond to attacks, which offers SMEs the resources of a larger group. The SMEs will receive a box that collects security information through monitoring modules, allowing each company to more easily detect attacks at its level, and at the cybercenter to detect attacks on a larger scale in the whole ecosystem, and then to analyze the objective of the attacks on a wider scale. The center provides aid in the case of incidences and support to the SMEs.

Conclusions

To conclude the seminar, Colonel Jean-Charles Nicolas, the director of studies and forecasting at ETRS (directeur des études et de la prospective de l'ETRS), thanked all stakeholders and actors involved in the preparation of the conference. One should bear in mind the need for a comprehensive approach to fully respond to and establish up-to-date benchmarks to obtain reliable mapping of the deployed systems.

Even if the LIS are part of SIOC, they have some specific features of their own. Military logistics are complex and dependent on operations and their tempos. However, LIS are also indispensable effective levers in the maneuvering of logistics without which tactical maneuvers could not be performed properly. Vulnerable systems must be made to be cyber-secure without hampering the user interface and ease of use. LIS need to be user-friendly or

run the risk of users finding workarounds in order to fulfill their missions. They should be easily managed by SIC to be effective and operational. Because of the many interfaces with other information systems - particularly in the private sector – system flaws are potentially multiplied. There should be, therefore, a long-term effort to maintain the necessary level of confidence in a system and to do this one should practice maintenance in security conditions continuously and constantly evolve. The future is rich in opportunities: connected objects, predictive maintenance, robotization. These examples are not yet fully realized but they clearly represent a trend that will grow in the coming years. These issues should be addressed immediately. The private sector demonstrates that practical implementations of these are already functional. Two existing technical solutions were presented through the Balard project and the Box@SME (Box@PME) security solution. These provide protection and security in regards to information exchange.

These points of confidence are indispensable for users to have the level of confidence essential to the success of their professional activities in service to the nation.

Véran Le Cornec and Gérard de Boisboissel, CREC Saint-Cyr, April 2016