Summary report of the seminar on April 7th, 2015

"The cyber-resilience of weapons systems on the horizon in 2020/2025"

Musée des Transmissions, Cesson Sévigné

Within the framework of activities of the Chair of Cyberdefense and Cybersecurity

Saint-Cyr / Sogeti / Thales

As an extension of the seminars of February 12th, 2013 and March 12th, 2014 on cyberconflict and the Land Forces and Armed Forces, Écoles de Saint-Cyr Coëtquidan co-organized on Tuesday April 7th, 2015 with the Ecole des Transmissions and the DGA Maîtrise de l'Information (as part of the activities of the Chair of Cyberdefense and Cybersecurity, Saint-Cyr, Sogeti, Thales) a new seminar on the theme "the cyber-resilience of weapons systems on the horizon in 2020/2025."

Open to personnel across the Defense, it was a place for discussion and reflection on the issues of resilience that need to be addressed, starting with the design of future systems for the Armed Forces. It was also an opportunity to present examples of the effective cooperation between the three actors of the Pôle d'Excellence Cyber de Bretagne. It came as a result of the political will of the Minister of Defense, Jean-Yves Le Drian, to make the "Grand-Ouest" (Greater West) a major actor in regards to French sovereignty in cyberspace, a subject with increasing pertinence that is demonstrated day by day.

Introduction to the seminar:

Introducing the seminar, General Yves-Tristan Boissan spoke about the SIC 2015 symposium that had already covered the subject in a round table discussion facilitated by Colonel Aymeric Bonnemaison on February 13th. He pointed out the need to integrate (beginning upstream from the design) our future weapons systems and security in order to face cyberattacks and also to ensure that during an operation that weapons systems can recover, providing continuity in information technology.

However these requirements, once articulated, must be developed in order to give rise to concrete action. This brings the risk of having to adapt conventional programming approaches of our future weapon systems, or of having to adapt the conduct of our operations by including cyberthreats.

The goal of this is event is, therefore, to analyze the specific forms of resilience of the Armed Forces on the horizon for 2025. At this time the cybernetic parts of operations will have been fully integrated into the architecture of the future weapons systems of the Navy, Air Force and Army.

The general principles of cyber-resilience:

Cyber-resilience is the ability of an information system to withstand a failure or cyberattack and to return to its original state after the incident, or the ability of any body to regain its initial properties after a significant impairment. The idea can be applied to a physical system as well as to an individual or an organization. By definition, resilience is one of the fundamental elements of a military institution. As we enter the cybernetics era, this issue (as old as military units) takes a new form.

This translates into an organization through its ability to continue functioning and to resist internal and external aggressions, whether voluntary or not. The level of resilience is measured by criteria such as: the structure of the organization in place, the human resources devoted to the functioning of the system, redundancy and hardening of systems and equipment, procedures in place, competencies acquired through dedicated education and training, a thorough knowledge of the state of operation of the system, and the ability to diagnose a potential failure.

Applied to cyberspace, cyber-resilience therefore entails planning upstream and taking appropriate measures to ensure the recovery of information systems and / or weapons systems. In addition, the innovative aspect of resiliency in the cyber world is that it can be

applied to situations: where uncertainty reigns in regards to security of systems (viruses with uncontrolled impact); where the integrity of the system is no longer guaranteed; where the system activity may be degraded (corrupted or altered data) or inoperative (inactive communications); where the risks of spreading the threat is possible if system interconnections remain open, which together may require changing to degraded modes, or the isolation of certain parts of the S.I.

In the era of cyberconflict, examining the resilience of the Armed Forces, in this way, leads to the assertion that it is built on two inseparable pillars.

- The first is a technical pillar: Weapons systems must be able to cope with a cyberattack and, if an attack cannot be stopped, it must be able to recover as quickly and as completely as possible so the units can continue their mission. It is therefore necessary to design and implement security measures that are in-line with possible attacks and procedures for dealing with attacks and the resumption of activities adapted to the specific working contexts of the Armed Forces.
- The second is the human and organizational pillar: The resilience of weapons systems cannot be created in isolation from the resilience of the organization itself. It involves understanding how a cyberattack on essential weapons systems could jeopardize the organization. This cyber dimension must be fully integrated in the conduct of operations so that if a cyber-crisis occurs it can be managed accordingly by command, which involves, in particular, putting in place human resources and adapted organizational devices.

During the first session several speakers endeavored to define the general principles of cyber-resilience in the design of weapons systems:

Thus **Jean-Pierre Lebée** spoke of the cyber-resilience lifecycle: Taking resilience into account in the design phase of the systems, by identify risks and protecting systems from cyberattacks, and also in the operational phase by detecting threats, solving problems and addressing post-attack recovery.

Risk identification must be analyzed using a dual approach, bottom-up (what are the risks in the systems that I have to protect) and top-down (what are the consequences to the mission). This is a thorough approach using played-out scenarios (pentests among others) on the systems once they are designed.

Systems protection inherits long-standing information technology expertise: system redundancy, data backup and recovery, security (encryption, system separation), strong coding rules, and failsafe functions (automatic system behavior helps to avoid any risk in case of a detected problem). This expertise should to be re-evaluated in relation to cyberspace vulnerabilities, incorporating new design responses: "traitor tracing" functions in ad hoc networks, resilient routers. There should be rules that apply to organizations and personnel using these systems: training and awareness raising among personnel, security procedures, strict computer hygiene rules, and audits and controls.

In the operational deployment phase, cyberattack detection methods are available: technical probes on networks and systems performing traffic analysis and reporting alerts, integrated anti-virus, and business probes[1] that allow one to identify cyberattacks by detecting abnormal business behaviors. France, moreover, has asserted its desire for sovereignty in terms of detection.

[1] “sondes métiers”

The resolution of problems, if not automatically integrated into systems through real-time mechanisms in high urgency cases, should be evaluated and analyzed by a human before any intervention or response is triggered. This expertise involves upstream training of operators, management of configurations, and using tools for supervision and decision support, which would be easier to use if graphical visualization tools accompany them.

Recovery is ultimately the phase in which the system returns to the nominal system operation.

All these elements must be included in the resilience of future weapons systems, but more importantly, included in all the system life-cycle phases and in their environment (transport, maintenance).

The detection and handling of cyberattacks on weapons systems is a major objective brought up by **Lieutenant-Colonel William Dupuy**. From the simple with fleeting impact, to the complex with persistent impact (that require long implementation periods), cyberattacks vary. There is a wide and varied range and Lockheed Martin created the "Kill Chain" model that describes the 7 successive stages of cyberattacks: Reconnaissance, Weaponization, Delivery**,** Exploitation**,** Installation, Command and control, and Action on objectives.

Generally, weapons systems structures are designed to have very few points of access or openings to cyberattackers. Despite fears of treason (which has allowed access into the most defended fortresses in history), these systems usually enjoy substantial protection, not only because of their limited interconnection, but also because they use atypical technologies. An attacker thus has few means to study them, has no tools readily available to him/her, and these systems are not very interconnected so they are therefore difficult to infect.

Nonetheless, these systems, hardly studied by those who could help protect them, cannot be considered protected from cyberattacks. Restricted by correction cycles (validation and long corrective solutions), they are not only vulnerable but they are attackable.

However, they are vital. It is therefore absolutely necessary to monitor them continuously, with active not static surveillance. Thus it is necessary to estimate the level of a threat and adapt to the threat by having a risk analysis that follows the logic of the attacker (in order to determine its intended impact). In fact, the cyberattacker has a goal, means, operating modes, operational stakes, but on the whole the attack is difficult to model statistically. It is therefore necessary to be constantly adaptive, with the ultimate aim of dissuading the attacker from taking over our system by trying to think like him/her. That is, to supplement our traditional method of the approach of the weak link (where a system is seen as the sum of potential vulnerabilities), to the approach of the maximum effect (where a vulnerability can be used to the advantage of the system).

It should be noted here that some operational systems are difficult to update because they are deployed in the field. Yet using them may make it easier to detect attacks to which it could be potentially vulnerable, thus improving both the protection of these systems and the resilience of the organization that uses them.

According to **Lieutenant-Colonel François-Régis Vigneau**, cyber-resilience is an operational issue before being a technical issue, as we will see in more detail in the following paragraph. It involves both response actions to minimize the impact of attacks and to ensure service continuity, and requires a decision at the organizational level before ordering the returning to normal.

The major players are operational professionals, with the support of operators and the support of the cyberprotection chain as well as trainers in the preparation phase.

In terms of preparation, first the system should be mapped as well as the data needed for the activity, underlying systems, and support and environmental systems. Following this there should be a systemic analysis to determine the most vulnerable elements: Who has control over the data, what is acceptable or not in terms of lack of accessibility, what degraded mode of use is possible and for what duration, the Single Points of failure (SPOF), and our ability to take action in the system. Lastly, it should analyze what defines the critical area of the system and the possible and acceptable levels of impact or degradation.

It then becomes possible to study the continuity plan and the recovery of the operation and to list the processes of operation in the different modes or states of the system, as well as the limitations or the associated impact. This plan can then be submitted for approval by an authority or organizations that can judge its feasibility and relevance. Then it should be tested regularly during exercises in order to confirm its support to the mission, to train staff and to detect changes in the environment (which could call into question the solutions adopted).

Cyber-resilience is like a continuous Quality Process,[2] an analysis loop that evaluates solutions and problems that cyberthreats pose at the operational level when detected during tests or in action, and it resumes analysis based on a corrective back loop.[3] Since the level of certainty is never sure, this Quality Process must be continuous and vigilant. For example, some malwares sometimes reinstall themselves on a machine even if it is reset through penetrating the boot systems. This indicates that corrective action is not sufficient alone if it is not integrated and monitored overtime in terms of its impact.

The cyber-resilience of weapon systems, the Scorpion case:

In response to the question of what is the right approach to securing a weapons system, **Philippe Leroy** of Thales first responded by describing the new constraints specific to weapons systems. In particular, he talked about the fact that several components of these systems are currently COTS (Component on the Shelves) or use civilian technologies adapted for the military (Ethernet, Operating Systems, etc.). Weapons systems are complex and numerous, increasingly designed within the environment of multinational cooperation (OCCAR: A400, TIGRE ...) and therefore one must take into account the manufacturer support of each one, the requirements of various missions and the different constraints of their use. Weapons programs cycles are significant and must integrate the risks associated with the obsolescence cycles of system subsets (in particular COTS). Private technology is now dominant in many areas of information system development and is closely linked (ex: cloud, system mobility, application security, etc.) with the private sector product cycles, which are faster than those of the programs of the Defense.

In addition, our system defense must remain active in the face of threats and their evolutions, which requires a method of technical proactive support called security maintenance (Maintien en Condition de Sécurité - MCS). It is designed in the program definition phase, and includes operational elements such as anticipation and intelligence, and active supervision.

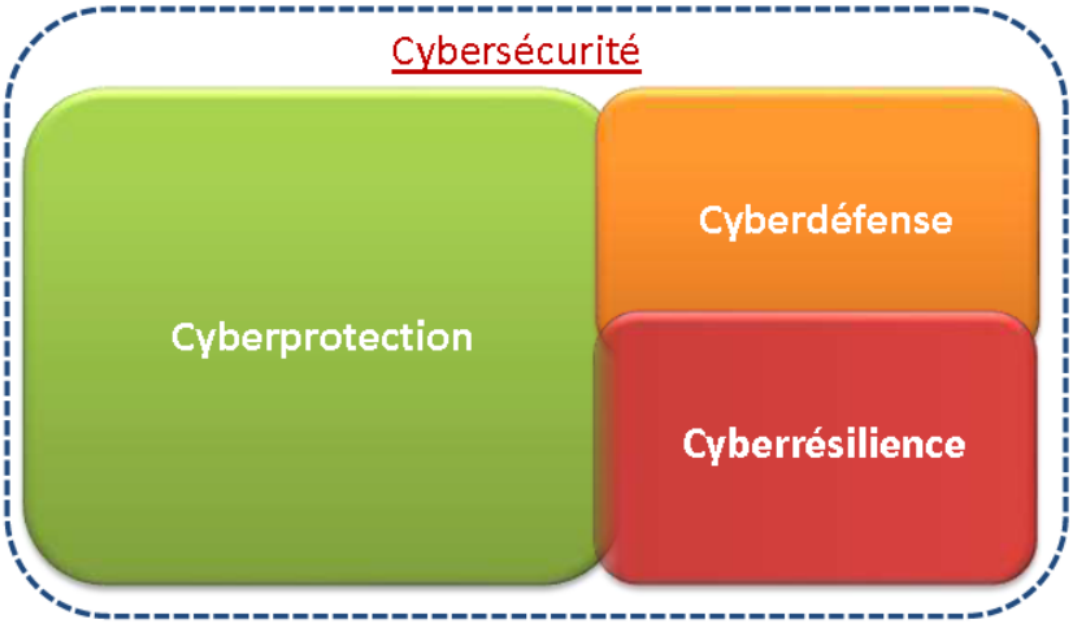
Looking at cybersecurity components, cyberprotection is static in nature, while cyberdefense moves to being active, and cyber-resilience has to be proactive at the intersection of cyberprotection and cyberdefense. Anticipating attacks (through intelligence and proactive

[2] "Processus Qualité"
[3] "rétro boucle corrective"

monitoring of technical vulnerabilities) and adaptability in the event of problems (mechanisms and processes for technical or operational resilience) should be anticipated upstream in the program risk analysis phase. For example, security operations procedures, supplied with security records and initial S.A. certification/approval, contribute to resilience.

To this end, studies have recently been carried out, notably through several PEAs. One example is SARSYA (Sécurité des ARchitectures des SYstèmes d'Armes), which led to the definition of resilient architectures contributing to the security of weapons systems through the securing of data links, the protection of sensitive information found in features of local security components and the methods of management and control.

Thus, the process of Maintien en Condition de Sécurité (MCS) must be used over the entire lifecycle of a system with the goal of ensuring its operational availability, maintaining its certification over time and ensuring that its configuration can face threats that are always evolving and are increasingly targeted.



Translation: Cybersecurity, cyberprotection, cyberdefense, and cyber-resilience.

In terms of the Army's future weapons systems, **Lieutenant-Colonel Régis Demaie** addressed the cyber-resilience of Scorpion, which is still being developed. He said that there is no resilience without protection and defense and that the scope of cybersecurity has expanded to more precise formalized methods required by MCS[4] for all our systems.

While the cybersecurity mechanisms of today are often compared with a force that must support a siege sheltered behind walls (cyberprotection), the Lieutenant-Colonel refers to Thucydides by stating that the thickness of the walls is nothing compared to the will of men. This is why the force also has the capability to be mobile, which is represented by cyberdefense. One of the main points of the new ministerial instruction (instruction ministérielle) 125-1516 that governs armament operations, compared to the old one, is the operational maintenance component (Maintien en Condition Opérationnelle - MCO), which has become essential in the study of a program. Similarly, cybersecurity needs should be formalized along with functional needs through a statement of security objectives (Fiche d'Expression Rationnelle d'Objectifs de Sécurité - FEROS) to fit the technical specifications

[4] Maintien en Condition de Sécurité

for industrial labor. Furthermore, MCS is a major factor in ensuring that the system in place has a lasting level of security, a prerequisite for approval/certification.

Downgraded for the Scorpion program, the main security effort must be carried out to protect the cybersecurity of the new Scorpion combat information system (Système d'Information du Combat Scorpion - SICS). This unique commanding officer to soldier system combines capabilities that were previously scattered throughout the regimental information systems and in all the terminal information systems.

As for the two new vehicles, the Jaguar and the Griffon, they will have vetronics architecture that will connect all the functions of these digital platforms. In fact, any vulnerability of a component can have consequences on the entire platform or even on the whole combat unit, via the radio networks and the information systems. In addition, maintenance and simulation mechanisms will have access to these platforms, and on the whole it will interface with more than thirty other digitized systems. Consequently, after defining the parameters, conducting the risk analysis, and conveying the needs, the Scorpion program formulated and transmitted a FEROS to the DGA in order to ensure a good level of cybersecurity for these machines of the future.

In addition, in order to ensure the physical resilience of the computerized systems, manual mechanical back-up modes are on all systems since a computer failure must not prevent the vehicle from performing essential survival functions such as mobility or ability to attack.

During a 2009 afghan operation, two viruses infected theater networks causing the absence of feedback on the tactical reference situation causing the inability to provide the necessary support and the inability to transmit certain orders. Based on the RETEX, **Philippe Mandle** developed the idea of the survivability of a system, a capability allowing a device to accomplish its mission in operational mode in a context of intentional aggressions while ensuring the survival of its components.

In the Scorpion GTIA example, survivability is the evaluation of the severity of the operational impact on the ability of the GTIA to carry out its mission and the vulnerability analysis of the critical GTIA components, but not the survivability of the individual systems of which it is composed.

The approach used on Scorpion requires the identification of critical functions (ex. locating), identification of critical systems and personnel (personnel whose loss leads to loss of capacity, critical equipment, weak points in the organization), and the identification of threats. The next step is to manage risks by developing ways to prevent them, these can be preventative systems (additional armor, tactical cloud, ...), organic (redundancy, ...), users (operators), or mixed (using a degraded mode of the system).

Included early in the system design, survivability is an innovative, multidisciplinary approach that complements conventional approaches with a system of systems approach, at the center of the Scorpion GTIAs of tomorrow.

The cyber-resilience of weapon systems: air, maritime and space systems:

The RAFELE combat aircraft (which aims to eventually replace 12 different aircraft types in the French Air Force and the French Navy), is the combat system at the heart of the Air/Air, Air/Ground, Air/Surface and Reconnaissance of the French Air Force missions says **Jean-Louis Guéneau** of Dassault Aviation. RAFALE must efficiently carry out all these types of missions day and night, at all times, in all theaters, sometimes (often even) very far away in

complex contexts and with total interoperability with all national and allied forces. It must guarantee its users high efficiency across the whole spectrum of the missions, through the controlling of the level of tactical awareness of the situation and the survivability. Taking into account the human factor is essential and imposes real-time and uninterruptible operating requirements. Consolidation of all the critical information for the purpose of operation safety contributes to crew confidence, avoiding "system" disorientation. Pilot/crew centered, highly flexible and able to function autonomously, it carries out all the defensive and offensive missions of a combat aircraft.

The RAFALE embedded system is involved with the interaction of the crew and all flight management, energy management and mission management functions involving sensors, communications, armaments and various others things. This system consists of a large number of proprietary computers communicating via dedicated digital buses. All the software used has millions of lines of code. The main features of this system are proven operational reliability, real-time reactivity, it is often uninterruptible (some functions cannot be turned off on an aircraft), and a user-friendly crew interface, which allows for automatic control (that is complete control of the systems). Robustness is based on environmental requirements as well as segmentation and isolation of functions, the technical tactical segregation and on the recent integration of the outside world. Confidentiality is attained through the use of specific devices (loading and deletion of sensitive data, isolation of confidential data, etc.). In this system where no single failure should interrupt the mission, robustness comes from functional and physical redundancy, and from monitoring and differences. Lastly, the operation in degraded modes to provide service, for example, in the absence of some of the input information, is a subject of particular interest. The RAFALE embedded system is therefore considered to be very robust against various types of failures, which contributes to its resilience, with functions programmed at the levels of critical needs and operational security. Also, it is developed by several companies in order to guarantee business and defense confidentiality. Even if this embedded system ensures physical and logical redundancy, it is also an element of a more complex group of systems created to be in coherence with the other tools used by the Armed Forces. As such, it is open to the outside world through interconnection that the pilot can take with him, such as smartphones or tablet PCs. Some components are also sensitive because they are dependent on other external systems such as a GPS. Lastly, NATO procedures and standards, which we do not own, involve separating sovereign code from the non-sovereign code in airplanes in order to guard against any security weakness.

Open systems bring many challenges that change over time. It is this openness of open services, international cooperation, standardization of interfaces but also dual uses, external support, and the risk of major technological breakthroughs, that pose new threats to our future embedded systems.

To address this, measures are regularly taken or will be taken:

- on the organization: regarding personnel and environments (such as organization and distribution of work, etc.), measures taken in regards to hardware and software used (verification, automatic generation, integrity verification, qualification), measures taken to control system-wide coherence (modeling).

- on the protection of systems: with the choice of an information processing architecture, subject to the tactical choices of the crew, the implementation of physical and logical redundancies (hot or cold), controls (monitoring), degraded modes, change control of software configurations, and advanced data protection (ex: management of keys in independent networks).

Thus, no system can afford to remain the same. The resilience of RAFALE to cyber risks is currently based on structural robustness, with functional redundancies (hardware and software), and modes to be used in the case of the absence of certain information. Nevertheless, vigilance is essential and involves active monitoring by the Dassault teams dedicated to this end.

Lieutenant-Colonel Sébastien Vinçon suggested that we extend this thought to show that the resilience of the weapons systems should not be seen as an end, but as an additional asset aimed at boosting the resilience of all activities.

The Air Force has identified 60 critical systems, of which RAFALE is only one element, but it is certainly central and vital. To ensure the cyber-resilience of these systems, it strongly advocates for a strategy to deter cyberattacks through segregation and redundancy of essential functions, by diversifying technologies, by strengthening the agility to reconfigure its information systems (because there is often not enough time to repair an attacked system during an operation), and by strengthening the organization, processes and operational and support methods of its activities. Several simulation platforms are needed to ensure training and proper implementation of this strategy given the scale of the strategy and the broad spectrum of critical systems to be covered.

For Navy surface vessels, Lieutenant Commander **("Capitaine de Corvette") Nicolas Malbec** presented the three reasons cyber-resilience is needed for combat ships: automation of systems, their interconnection and the massive use of navigation aid systems like the GPS, and AIS or electronic charts. Looking at the 2020-2025 horizon, he also indicated what a cyber-combat post could be on a ship in the future.

Today, military satellites are essential and ensure the coordination and relay of transmissions globally, and in particular in maintaining a link with the French mainland in external operations. However, a satellite does not troubleshoot itself, but it could make small changes with some software adjustments. Also, cyber-resilience must be integrated before their development, says **Commander Xavier Houpe.**

Currently, satellites are technically very complex in order to ensure the resilience of communications in the event of problems or failures: this includes multiple redundancies, complementary systems, and autonomy of its on-board computer. Resilience is also at the organizational level through adapted structures and redundant centralized management on several sites, with partitioned networks. The principles to be adopted to face cyberattacks thus have the same philosophy as those of resilience:

- There should be no single-point of failure.
- The gateways between the nominal and redundant functional chains allow for overall reliability. Many systems are thus doubled to have nominal and redundant components. However, some imagine in the future, like ship Captain (Capitaine de Vaisseau) Le Sellier de Chezelles, that there can be orbiting satellites that lower costs and do not require the redundancy for some systems.
- Within the central program, the FDIR (Failure Detection, Isolation and Recovery) function consists of hardware modules (CRM) and software functions to detect any failure of software or equipment that could endanger the mission or damage the satellite, to isolate this failure and to restore the satellite operations and the mission through one or more on-board action. The reconfiguration sequences can be programmed by the ground crews.
- Some systems are oversized (the number of cells on the solar panels for example).
- The control systems are grouped in several geographical locations.

- Restricting stream transmissions using standard protocols.
- Simulation before any reconfiguration of the payload on identical platforms, platforms where any problem can be repeated.

With such high-resiliency design, cyberattacks (if they are not impossible) have a low probability of incapacitating the satellite because the principles adopted surrounding satellites and resiliency guarantee a high level of security. In addition, attack identification is facilitated by the fact that the networks communicating with the satellite are certified/approved, and are therefore safe except for internal intrusion. To deal with such contingencies, "devolution exercises"[5] are regularly held several times a year. Lastly, in the event of large-scale attacks, satellite autonomy should enable it to ensure minimum operational recovery.

Human and organizational cyber-resilience:

The military as an organization must face the challenges of cyberwarfare, and venturing to consider these questions is not only the concern of information systems specialists. On the contrary, the news shows us the devastating effects of cyberattacks on information systems and their impact on our society which, although they have not yet proved fatal, show the potentially catastrophic impact that such attacks on our weapons systems could have. Resilience is therefore a concept that must be integrated into the conduct of operations and the personnel components that contribute to it in order to maintain operational management of the mission.

Thus **Gérard de Boisboissel** has attempted to model the impact of cyberattacks by separating cyber-resilience at the local level (the weapons system itself) from the global level (the Armed Forces as an organization). On the local level, cyber-resilience is a tool of resistance to a cyberattack for the system and its ability to maintain or restore its normal operations (the effectiveness of the organization that uses it depends on this). At the global level, organizational resilience is the ability to be tough under intense conditions with change and stress.

At the local level, cyberattacks can reduce the system's capacity or its quality of service. The system then enters a degraded mode; degradation is tolerated if it does not exceed the acceptable maximum threshold and it will be fixed later with corrective actions.

At the global level, a first characteristic is that there is a time lag between the attack of a system and it being acknowledged by the organization, followed by another time lag necessary for its analysis. A second is that the disturbances felt after an attack are not necessarily identical to those felt on the system. It may be less serious for the organization (if the system is not a critical system, or there is a redundant system that can be activated), or it could be more serious. Let us take the example of data theft on a critical system. This system will remain functional and its efficiency will still be optimal; however, for the organization, the threat posed by this data theft is very serious and can go as far as needing to shut down the system even if it remains functional.

It cannot therefore be asserted that the overall resilience of an organization is the sum of the different levels of resilience (of each of the local systems) or even that the overall resilience of the system is that of the weakest link of the system. It is necessary to consider other aspects for analysis at the organizational level such as certain sociological factors (stress, human availability, the quality of the training of actors, ...), and also managerial factors (the strategic

[5] "Exercices de dévolution"

impact of the attack, the risks of a spread, and the distortion[6] of its impact ...). An attempt at modeling could be:

- Mission = objective + duration + means (which are the different local systems)
- Mission risk = function (threats, vulnerabilities)
- Local system interference = function (nature of the system, system degradation, time of attack)
- Propagation (spread)= function (magnitude of attack, duration, penetrability of the systems)
- Distortion (balance) = function (impact of attack, overall criticality)
- Overall perception = function (Σ disturbance (s) of local systems + propagation + distortion)
- Operational decisions = function (overall perception, mission, mission risks, means)

The goal of the decision made by the organization is thus dependent on context and criticality. As mentioned above, they take into account the mission and initiate the corrective actions that they deem appropriate based on the analysis of criticality and risks linked to the problems caused by the attack.

Decision-making at the organizational level may thus go against the logic at the local level and they may take a position in favor of optimal military action support as a function of time, degree of criticality of systems, and the mission. It could be restoring degraded systems to the nominal mode and the choice to remain in degraded mode, to switch to redundant or isolated system(s), whether or not to isolate the degraded systems, or to potentially further develop the mission.

From this analysis, **Battalion Commander ("Chief of Battalion") Pierre-Arnaud Borrelly** defines a cyber operational sequence for military action at the organizational level:

- Inform - Alert - Protect - Block - Restore

For intelligence and early warning, the problem of anticipation lies in the identification of threats and in monitoring, which depend on the quality of intelligence and the quality of the alert. However, the uncertainty of intelligence leads the bodies in charge of operations and planning to the first position of resilience. This has been defined as the plasticity of the organization to continue operating and to adjust constantly, at least to the pace of their decisional loop and actions.

It is possible to imagine, in terms the "notion d'effet" used by military staff for planning, the different consequences a cyberattack could have on resilience. An effect is a change of state or attitude, a physical or intangible result, a consequence of specific military or non-military actions aimed at a specific target or objective. At the operative level, it concerns the overall threats of the theater or threats shared with major subordinates. At the tactical level, it concerns local actions, the small effects limited to the zone of operation and the impact on the operative effects.

The results of a cyberattack can be the ones intended by the attacker and they can be confused with the effects felt by the Defense Staff (l'Etat-Major) because the organization is not very resilient and it fully feels the negative impact. The effects may not be felt for two reasons: the organization is resilient to the point of toughness that it does not realized that it has been the object of an attack and it does not suffer any consequences; or the organization does not have the means of measurement and analysis that would allow it to measure the size of an enemy attack (like gamma radiation passing through a living organism). Lastly, the most common

[6] "La distorsion"

case is that the impact felt is different from the effect intended and so there is a distortion of the impact intended by the enemy. It is in this field of distortion that resilience is found because it denies the opponent the ability to impose their will on the organization.

Thus, cyber-resilience should be the fruit of the combination of an intelligence-monitoring capability (anticipation and alert function), a learning capacity (analysis and training function) and the capacity to endure (continuity of action function).

At the level of the Defense Staff, the center of gravity is a capacity (or geographical location) from which a military force or any other entity (country, alliance) derives its freedom of action, power or will to fight. It is a target for the enemy (to destabilize the military force targeted), and an objective for the organization itself, which must protect its vital systems. The center of gravity is based on essential capabilities (its main means), which have fundamental requirements (resources required), but is subject to its own critical vulnerabilities (those of its constituent parts). To be effective, an attack or a defense seeks to have an impact through damage in the first case, or in the second case through the protection of critical vulnerabilities of the center of gravity.

If the center of gravity makes it possible to identify within an organization what is vital to a system, the resilience effort must not only focus on the protection of its vulnerabilities (which would translate into structural fragility due to continuous adaptation under hostile conditions), but to be effective it should adapt to the overall needs of the essential capabilities through an approach that combines operations and exploration.

In terms of the resilience of soldiers and units in the face of cyberattacks, **Colonel Francis Chanson** analyzed the impact of cyberthreats on battlefield foot soldiers, where the enemy is traditionally elusive but real. Now, in cyberspace, the enemy is intangible and the combatant does not know the origin of the attack. A cyberattack is thus asymmetric (even terrorist in nature) and combat tools are perceived as useless, thus depriving the soldier of the conventional ability to react (which is destabilizing for the combatant).

Faced with this new method of enemy action, the determining factors are the command's ability to adapt the conduct of an operation and training. All actors in the cyber-chain must be trained, which is not much of a concern for officers and sub-officers,[7] but requires a great deal of consideration for the troop ranks.[8]

Through a comparison between the resilience of a cyber-combatant and a resilient combatant, it can be seen that the factors determining ones resilience in combat are absorption (the strength of a group helps to collectively overcome aggression), adaptation, and training. Even if self-esteem may seem to be a key factor, it does not seem obvious that Digital Natives (those at ease using digital technology) are more resilient on the battlefield than their comrades who are not. It is once again the strength of command that will make the difference in combat, and it is therefore an axis of additional training for military managers using the weapons systems of tomorrow.

According to **Colonel Jean-Charles Nicolas**, today training has been focused on cyberprotection and cyberdefense, and it is clear that this is not the case for cyber-resilience. In an initial analysis, it should perhaps be given equivalent priority.

To this end, cyber-resilience is described (in some documents) in order to better explain and the subject. In this way, DIA 3.40 (the mapping of MINDEF procedures) and DGSIC's

[7] "sous-officiers"
[8] "militaires du rang"

documents describe cyber-resilience. While the PCA/PRA and PCI/PRI elements are clearly explained, it is clear that the operations chain of command on one hand, and the SIC chain on the other hand, are the main actors in the cyber-resilience in connection with the cyberdefense operational command.

Drawing on this, there is a notable difference between the current and sparse training available and the estimated need. The improvement of specific cyber-resilience training activities, the development of specific training courses on robust architecture and a better understanding of critical capabilities and services would be a good first step. Moreover, it is essential to include in this education component, dedicated training through exercises dealing with crisis management, and address the skills required to work in degraded mode. In parallel, a RETEX process should make it possible to measure progress and to develop the concepts and trainings.

To conclude, it is a matter of establishing a roadmap with the employers, in terms of training, in order to include the right level of the cyber-resilience dimension.

Captain Antoine Roussel, to conclude the seminar, reviewed the parallels we can draw between the resilience of the Armed Forces and the evolution of military technology over the course of history. To this end, he presented the origin and evolution of the Gribeauval system, the first system of weapons in a contemporary sense. It was adopted in 1764 following the Seven Years' War and was based on a compromise between mobility and firepower. Fully operational since the 1770s, this artillery equipment used during campaigns of the Revolution and the First Empire, outperformed that of its adversaries despite an attempt to reform and simplify the system in 1803. The system was restored to its original state in 1816 and its principles were re-introduced through the "Valée system" until the adoption of new equipment in 1853. The longevity of this system, the adaptability of the equipment to different operational constraints outside of those which were there when it was designed, highlight the two pillars of resilience: technology and humans. At the technical level, collaboration with the industrialists (founders) made it possible to streamline and standardize equipment in order to facilitate control and maintenance operations (interchangeability of the pieces, assemblies and sub-assemblies to varying degrees). The principles of use are guided by the same imperatives as the specialization of artillery equipment (field, garrison, siege, and seacoast),[9] and dedicated equipment (means of transport, lifting, field forge, artillery vehicles).[10] Also, officers and servants for the first time received specialized education and training for inter-army maneuvers, while creating an artillery identity. In fact, the adoption of this system also led to the creation of an independent artillery weapon with the establishment of an organic chain of command based on brigades and permanent regiments subordinate to the main weapons inspector, and a territorial chain of command linking the production centers, arsenals, schools and regiments. Lastly, the working methods inherited from the Gribeauval (technical centralization in the design and weapons testing) were consolidated by the creation of the Comité Technique et du Dépôt Central in 1795, a predecessor of the Section Technique de l'Armée de Terre.

Conclusions:

The purpose of this seminar on Tuesday, April 7th, 2015 was to present different sector approaches to define cyber-resilience principles and to complement them with real experiences in order to clarify their scope, to determine their requirements, and to contribute to their consideration throughout the life-cycle of a weapons system.

[9] (campagne, place, siège et côte)
[10] (moyens de franchissement, de levage, forges de campagne, voitures d'artillerie)

To conclude this seminar, **Captain** ("**Capitaine de Vaisseau"**) **Le Sellier de Chezelles** defended the idea that cyber-resilience should be integrated into cyberdefense and cyberprotection. These days, it is clear that no system will be sufficiently robust to withstand all cyberattacks over time and that we will not be able to expect 100% security of our systems from evolving threats. There is always the risk of a technological breakthrough that could make our protection systems obsolete.

Also, it is important that the cyber-resilience concept be factored in technically (by integrating it into the design of our weapons systems), and into the organization of our Forces at all decision-making levels, from the unit level up to the level of the Defense Staff.

Cyber-resilience is achieved through the development of resilience mechanisms that must be tested prior to potentially being implemented by organizations. Also, personnel must be trained, both the technical experts who operate the weapons systems, and also decision-makers at a higher level who are able to handle crisis management overall. However, this must be adjusted to need and must include cost considerations to avoid unnecessary redundancy in systems and to foster adaptability.

It is therefore necessary to remain flexible and vigilant, and to rely on attack simulation platforms adapted to each profession.

Gérard de Boisboissel,
April 2015