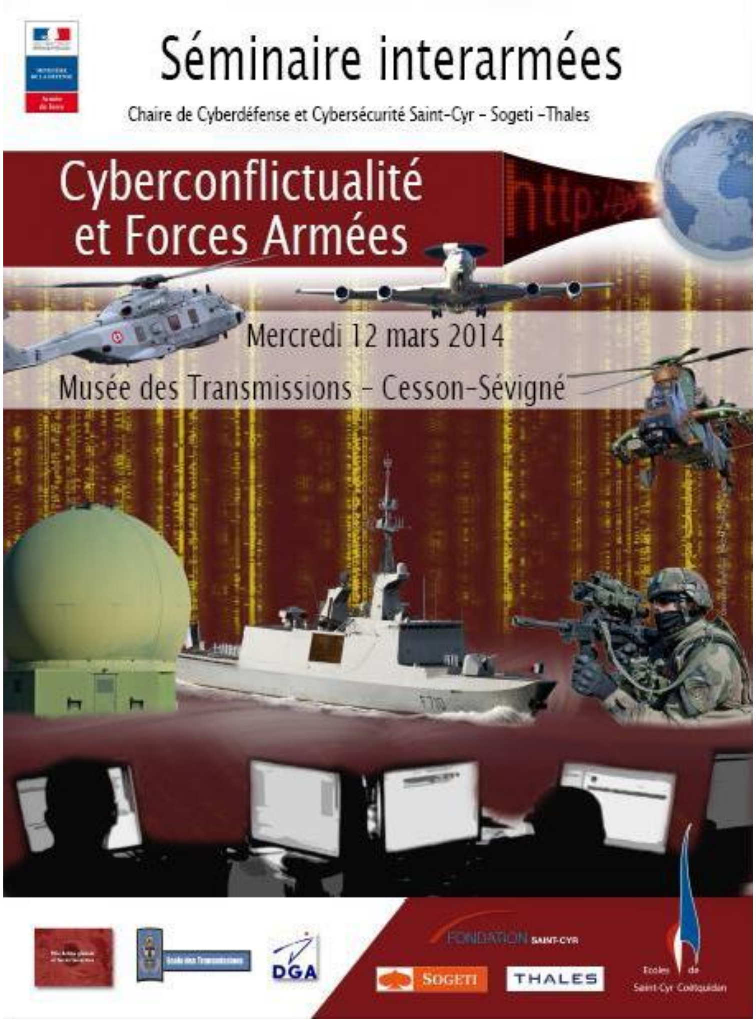
Summary report for the seminar held on March 12th, 2014

"Cyberconflict and the Armed Forces"

Musée des Transmissions, Cesson Sévigné
As part of the activities of the Chair of Cyberdefense and Cybersecurity
Saint-Cyr / Sogeti / Thales


Séminaire interarmées
Chaire de Cyberdéfense et Cybersécurité Saint-Cyr – Sogeti –Thales
Cyberconflictualité et Forces Armées
http://
Mercredi 12 mars 2014
Musée des Transmissions – Cesson-Sévigné
Ecole des Transmissions
DGA
FONDATION SAINT-CYR
SOGETI
THALES
Ecoles de Saint-Cyr Coëtquidan

As an extension of the seminar of February 12th, 2013, which dealt with cyberconflict and the ground forces, this seminar was organized with the support of the École des Transmissions and the DGA-MI. It brought together just under 100 people, mostly military personnel of the three armies and Defense personnel.

Gathering mainly Defense personnel, and opening the event to military inter-service[1] personnel, the gathering had several objectives:

- To deal with the issues characteristic of cyberspace and their specifics for the Army, the Navy and the Air Force.
- To tackle the specifics of military training for each of the military schools in initial training of military officers.
- To respond to the objectives of the Pôle d'Excellence en Cyberdefense de Bretagne, which relies on, among other things, the organizers of this seminar (Saint-Cyr / Sogeti / Thales, ETRS, DGA-MI), that conduct research for the Ministry of Defense and the nationwide cyberdefense community, thus responding to the 4th axis of the priorities of the Cyberdefense Pact, explained by the Minister of Defense Jean-Yves Le Drian on February 7th, 2014 (at the same place).
- To respond to the objectives of the Pôle Action Globale et Forces Terrestres du CREC Saint-Cyr to analyze changes in conflict and to contribute to higher education through research at Saint-Cyr Coëtquidan.

Those represented included the Defense Staff of the Armed Forces[2] (EMA, EMAT, EMM, EMAA) and a group of schools providing initial officer education (Navale, Ecole de l'Air, Saint-Cyr, EOGN, as well as l'Ecole des Transmissions). DICOD was also present for a Web TV report on cyberdefence.

As the themes covered during the day were very dense, the spectrum of topics covered was very wide. This seminar made it possible to have a first inter-service gathering and to give people involved in the cyber domain a chance to meet and discuss. In the future the aim is to formalize a date at the beginning of the year for the Pôle d'Excellence en CyberDéfense du Grand Ouest to organize a regular meeting between the major regional actors and to continue studies surrounding cyberconflict strategy, to give more structure to the Armed Forces both for the ranks and for France as a major force and for its operational effectiveness.

Introduction to the seminar:

The protected systems of the early 2000s focused on perimeter defense of systems and networks, but the events in Estonia and Georgia made us realize that we need to go beyond simple passive security and that we must protect our systems, which have become indispensable. The political impetus of the 2008 "Livre Blanc" paves the way for a comprehensive active defense strategy, with protection of our systems, permanent surveillance and rapid reaction in the event of attacks.

Following up, 2013 was for a year for improving cyberdefense: in addition to the Livre Blanc published in 2013 and the military programming law (Loi de Programmation Militaire - LPM) of December 2013 (which serves as a legal support for specialized action), the Minister of Defense Jean-Yves Le Drian launched several specific projects, including the creation of the Pôle d'Excellence en Cyberdéfense de Bretagne with 6 axes of effort and 50 specific activities. In order to implement the cyberdefense policy wanted by the Minister and promoted by the General Cyber Officer Admiral Coustillère,[3] there appears to be a need to

[1] Inter-army, "interarmées"

[2] "Etats-majors des Armées"

[3] "l'Officier Général Cyber l'Amiral Coustillère"

develop an up-to-date inter-service doctrinal corpus from conception to implementation, with documents adapted for each military branch. For example, in the summer of 2014 there will be a cybersecurity implementation document for ground forces based on three pillars: cyberdefense, cyberprotection (formerly SSI), and cyber-resilience (resistance and recovery).

In terms of comprehensive training, factoring in the specifics of cyberdefense requires combing the general skills of an SSI specialist to become a cybersecurity expert, which includes additional skills such as cryptography, for example. The additional technical skills required in the training of military personnel draw on expertise developed in the civilian world, and therefore they have an even greater openness in the training that they provide.

For the more specialized military trainings, the ETRS offers new types of trainings that integrate the handling of cyber-incidents (sometimes linked to CALID). Training should also be implemented that involves operational training exercises for our Forces with specific cyber-incidents included in maneuvers.

With respect to human resources, job creation is planned, with jobs that are modeled and redefined using an inter-service approach. Outside military personnel and supporting the Forces, is the Réserve Citoyenne CyberDéfense, which is made up of volunteers and was launched in 2013 in 5 regions (including Brittany) for awareness-raising missions. The Réserve Opérationnelle Cyber is less advanced and should be worked on in 2014.

In terms of doctrines, the CICDE issued a concept document on cyberdefense in 2011 and the DIA 6.3 doctrine in 2012, related to domain 6 of the SIC, it defines the means, organization and responsibilities needed in order to handle cyberdefense issues.

Faced with a ministerial push, the CICDE produced a new doctrine document, the DIA 3-40 for operations (3) in cyberspace (its own domain = 40). It describes the characteristics of cyberspace as being a fifth field, and also a bedrock that supports the other four fields: air, land, sea and space.

According to DIA 3-40, cyberdefense includes three types of measures: LID, the use of networks to gain intelligence, and offensive operations (LIO), which is consistent with the NATO doctrine. Its mission is to aid military operations (preparation and conduct) in the functional support of ministries and the Ministry of Defense in the event of a cybernetic crisis.

The five main underlying principles are:

- A single chain of command that ensures coherence that is centralized and specialized.
- Supporting civilian competencies through cooperation and exchange with the private sector and academia.
- Continuity of the mechanism.
- Respect for the legal framework of French and international law.
- The mobilization and the consistent involvement of SI users.

The operational management of the LID has two components: a specialized component with CALID, linked to the operators, and an operational component with effects on the networks that are in contact with the operational command. The offensive cybernetic component mentioned is very centralized and under the control of the highest strategic levels of command.

There is also the idea of cybedefense intelligence (Renseignement d'Intérêt CyberDéfense – RIC), which allows one to get useful intelligence from cyberspace (ex: new virus, enemy network information, etc.).

In a global way, this doctrine lays out the principles for operation in cyberspace but with specific implementation for each branch of the armed forces. It is the general cyber officer ("l'Officier Général Cyber" – OG Cyber) who ultimately gives the directives, such as in the case of the rapid intervention groups (Groupes d'Intervention Rapides - GIR) managed by CALID, but under the orders of OG Cyber.

The logic behind environments:

The Defense Staff[4] from the different services presented their visions on the specifics of their military branches in cyberspace. Cyberspace is its own domain, with strategies to control other domains. Controls in cyberspace consist of controlling one's own operations to guarantee operational continuity, in order to deprive the opponent of any such opportunity. Thus, in cyberspace, understanding the environment is a prerequisite to understanding support, and this implies that there is a need for unicity of control and command.

In the aeronautical field, faced with this whole issue, it was mentioned that the weak links of weapons systems are the private sector systems which should be controlled, and command systems, and that protective combat systems must be used, even if there are delays. The need to integrate the technological components that come from the private sector necessitates integrating security mechanisms into weapons or information systems at the outset of their design and should involve all state and commercial actors. The Air Force must also be able to intervene militarily in cyberspace in order to ensure their operations and the cybersecurity of their essential missions that are currently in action.

In terms of the maritime domain, it is not possible to send many SIC experts on a ship or a submarine. They must therefore provide support from the base; this emphasizes the dependency on sea / land transmission links. The cyberattack data then must be collected and transmitted to land for more in-depth analysis, which poses a problem for nuclear submarines. Dependency and vulnerability are now being taken into account with on-board SCADAs, which help prepare a vessel's seaworthiness (with sometimes ancillary functions such as ventilation). Personnel training therefore remains a priority and must be carried out, along with other things, through cyber exercises.

Lastly, in terms of the land domain, there are shared characteristics with the other military branches at strategic and operational levels, but with an apparent limit at the GTIA level and below, where the specifics of the environment become more marked. With the digitization of infantryman (FELIN, integrated infantryman equipment and communications), which is among a multitude of interconnected actors, network barriers are gradually being pulled back for a better efficiency. Info-valorization on the battlefield relies on communication between systems (sometimes automated) in order to make decisions and act more quickly. The old systems are being progressively integrated into the coming inter-service information system (Système d'Information des Armées - SIA), which will link all inter-service information systems at each level in real-time. Personnel education is also promoted so that the system has good reflexes in case of cyber problems, and a habit of non-dependence on non-operational platforms (Facebook, private mails etc.) is cultivated, always keeping people at the center of the action.

Threats and trigger thresholds:

[4] "Etats-Majors"

A threat to the security of information systems, which can be ever-changing, constant, and evolving, is a risk component, which is measured by threat, vulnerability and impact. However, a threat is biased by human perception and the unpredictability of people, especially in cases of crisis management. Security solutions vendors target their advice toward certain threats, according to their interests. In fact, according to these actors, there should have been 20 million malicious codes in 2013, but this figure also includes other types of the same strain of virus, and we must look below the surface and at what is actually there in reality. It is therefore advisable to be cautious when listening to the current anxiety-ridden discourse of security companies. Attacks, even if they are not new, are more and more elaborate and intense, though their typology has not changed radically in 2013.
There is the human factor, which can always be the weak link. For a given information system the threat will always be mixed, included in an attack chain adapted to the environment. These will almost always exploit classic vulnerabilities and are avoidable with some simple behavioral hygiene. Only 5% of the attacks come out of this category and are precisely targeted, requiring a lot of development resources by specialized teams.

Concerning thresholds that trigger a response and political power, Deputy Rihan Cypel was invited to clarify the French political position on October 8th, 2013 at the symposium "Law and ethics in the face of cyberconflict challenges,"[5] and he called on CREC organizers to provide some elements of the talk.

According to S.A Baker, the law is a machine to block the military, an increasingly dense normative framework hindering action. However, according to Didier Danet, it is in fact a lever for action from the moment it is used to support actions, and it is a legitimate recourse to cyberattacks. In regards to this, Harold Koh, Legal Advisor of the U.S. State Department, clearly defined the U.S. position on this issue at Fort Meade on September 15th, 2012. He stated that international law applies to cyberspace, which in fact is not a lawless space. Technology now makes it possible to identify perpetrators of attacks and he asserts that they should be prosecuted, that States should be held responsible "for activities undertaken through 'proxy actors,' who act on the State's instructions or under its direction or control."[6] He goes even further by stating that a cyberattack can be considered an armed attack if it produces comparable effects to those of a conventional weapon (damage to persons or property), that a response can be preventative in the event of an imminent threat, and that the idea of a threshold should remain vague (the important question being whether the response is necessary and proportionate). In turn, Léon Panetta postulates that if a crippling attack is launched, the American people will be protected by the orders given by the President, which offer a rather wide political margin for maneuvering.

Hence, it appears that the position of the United States on this issue, through their legal declarations and assumptions, clearly shows a desire to act as they see fit, without precisely defining response thresholds in order to keep many options for action open. This is done through an expanded interpretation of self-defense justifications in the aftermath of the September 11, 2001 attacks. Thus the U.S. carries out military operations in situations where the justification of the use of armed force is not necessarily evident with regards to the Charter of the United Nations. This brings up the question of France's political position on these same issues, and on the private sector policy that supports it, and more precisely on the sovereign interests that our country wishes to protect.

<u>Threats as seen through specific cases:</u>

[5] "Le droit et l'éthique face aux défis de la Cyberconflictualité"
[6] http://www.state.gov/s/l/releases/remarks/197924.htm

Today the threats are real: from taking control of a car, to the tracking system of a boat, or to an airplane through non-secure control protocols. There are many threats to systems and logistic flows. Attacks can be carried out through the digitalization of systems, their interconnection, or through the military's use of unadapted civilian technologies. Added to this is the growing complexity of software, with an exploding number of lines of code in systems, which come in response to the need for more reliable and more efficient software. It should be noted, however, that taking control of a system requires access to something integrated in the network, that is, a legitimate and authorized "on-air" connection to access the core of a system. Consequently, the belief that it is possible to take of control of a system by simply sending signals is, according to our technical knowledge, false. This only allows it to interfere with a system but not to take control of it.

In addition, attacks are mostly unintentional, with ¾ being encouraged by human neglect. Added to this is the fact that 80% of data leaks originate from the actions of an individual with legitimate and authorized access. Both cases show that humans are a primary weakness in a system. Deterrence, controls and pedagogy are therefore solutions to be implemented and integrated into a comprehensive approach to security. Despite this, geographic outsourcing of data storage (offshoring) decreases control in critical areas; this is difficult to avoid for many small or moderately sized entities for obvious cost reasons.

In order to contain these risks within the Defense environment, DIRISI manages the largest French network with tens of thousands of servers and hundreds of thousands of computers, and with an increasing interconnection of systems. The physical and logical compartmentalisation of the different levels of confidentiality is still compulsory, but it makes management more complex. The pressure for greater simplicity sometimes means making choices that can generate risks (ex: Intradef and the internet on the same workstation). Moreover, these traditionally separated networks must increasingly communicate, such as about procedures regarding exporting weapons systems, where parts with a higher level of classification must be able to communicate with lower levels in order to be efficient.

The DIRISI doctrine relies on a similarity between urban warfare and the world of cyberconflict: the enemy is there, present, but invisible or blended into the masses and can come out at any moment. It is no longer a question of taking refuge behind a wall and defending against the enemy outside, but rather using thorough defense procedures connected with reactive actions (the latter being implemented by CALID).

A large and often forgotten consideration in cyberdefense is intelligence, which is important as one moves toward active defense (which replaces the old doctrine of protection). It is indeed necessary to identify the origin of attacks and to assess the capabilities of the adversary (for these two missions good intelligence is necessary). This amounts to integrating RIC (Renseignements d'Intérêt Cyber) or cyber intelligence of interest and ROC (Renseignement d'Origine Cyber) or intelligence from the cyber domain. Both are complementary while they are different in nature. The RIC, like defense intelligence, aims to use any type of tool to identify cyber-threats, integrating the conventional means of gathering open and closed information. The ROC, on the other hand, focuses on the open sources of information in the cyber domain, such as the information collected by NSA (PRISM). They are confronted with the opposite problem, information overload (sometimes linked with disinformation) that requires extensive processing work. Using these two types of intelligence does not disrupt the analyst's job, who then has his or her sources and tools augmented. As a result, intelligence, as a mechanism for direction, research, processing, exploitation and dissemination remains unchanged. Cyberdefense is in fact integrated into the classic work methods of an analyst. In this way, RIC is not derived from ROC but both are used in the assessment of threats.

Cyber education within the Forces:

The training of the armed forces is at the center of Defense concerns. Plentiful and specialized expertise is demanded within the Forces to meet the demands of the cyber domain. It is therefore necessary to adapt military training or to recruit people with technical profiles for short-term careers in order to have a staff that is continuously trained in the latest innovations in the field. However, this last solution may not be suitable for ensuring resilience in times of crisis, but institutional history within the forces can guarantee resilience. Someone with a cyber-career would thus find a place within the cyberdefense system. As the ability to think in terms of the long-term is critical in management, this person would know his subordinates (from a soldier to an officer) and would in fact be more responsive particularly in crisis management. Added to the need to retain cyber-trained personnel is the need to avoid the "désert des tartars" syndrome, even if no cyber military attack has taken place, they must still regularly provide training on new risks (like other professions confronted with these changes).

Initial training at military schools includes a cyber dimension in the education of officer cadets. From the core curriculum, to the more specialized options, one notices that the cyber domain becomes an educational opportunity for teaching computer science, with cyberconflict exercises integrating the defensive (LID) and offensive (LIO) elements.

These ideas are deeply inter-linked and, in accordance with the recommendations of the Livre Blanc, no part of the French Armed Forces is missing a program in this field in terms of research and the training of personnel. For example, the Gendarmerie has already included cybercrime in the training of its officers, a domain deeply intertwined with cyberdefense. It is a necessity, pushed by the fact that most of the interconnected objects of tomorrow will be traceable and therefore protected. The military police of tomorrow will need to be able to track these objects in cyberspace through the use of Big Data or directly, which will require a metamorphosis or a rapid adaptation of the education provided.

For the jobs of tomorrow, it will be necessary to attract people with cyber competencies adapted to the military world, and to make these professions attractive with room for progression over time. It is therefore necessary to think about cyber career paths and adapted flexible education, integrating technical, ethical and legal dimensions with specific types of trainings, from simple cyber hygiene to crisis management. The jobs are yet to be specified, but they will need to cover the whole spectrum of military missions in the theaters of operation (LID officer, protection of locally deployed SICs, intelligence and LIO accompanying military action). The ultimate challenge is to have continuously trained and high-level staff, who will be able to understand a threat and relay it in simple terms to decision-makers, and to rely on a rather centralized model supporting synergies. Maintaining the quality of trainers is also essential and will prepare them, in the medium and long-term, in terms of the capacity of the institutions to train professionals to be adapted to these new threats.

Some overview elements that are complementary to this seminar:

A. It appears that the interconnection of networks is an element of weakness in digital networks used. While the interconnection of military networks with the civilian world (the internet in particular) is known, the interconnection with inter-ally networks is problematic, as control capacities are faced with issues of confidence and technological control.

B. The political will to protect national interests in cyberspace needs to be clearly and explicitly explained by the political authorities. First to define the framework of our cyberdefense and the threshold levels for responses to attacks on our interests, but also to determine the private sector policy which supports it (sovereignty over critical components (OS), software, or networks).

C. In terms of the citizen and operational reserves, today the effort is focused on raising awareness among French companies about cyber-threats, an awareness for which the citizens' reserve is in support. Though GIRs are the spearheads of CALID, operational experts are rare and difficult to find. It therefore seems necessary to develop an operational reserve based on a pool of technical experts in companies and to train them in possible interventions for the Defense.

D. Most of the time, human error (or weakness) is the cause of many malicious acts. In the cybersecurity domain, banks and insurance companies have developed a standard of training and risk management that commensurate with risks they take. With the support of these professionals, a workshop on this and the issue of personnel training in cybersecurity could be envisaged for the Armed Forces.

Gérard de Boisboissel
CREC Saint-Cyr

CHAIRE DE
CYBERDÉFENSE ET
CYBERSECURITÉ