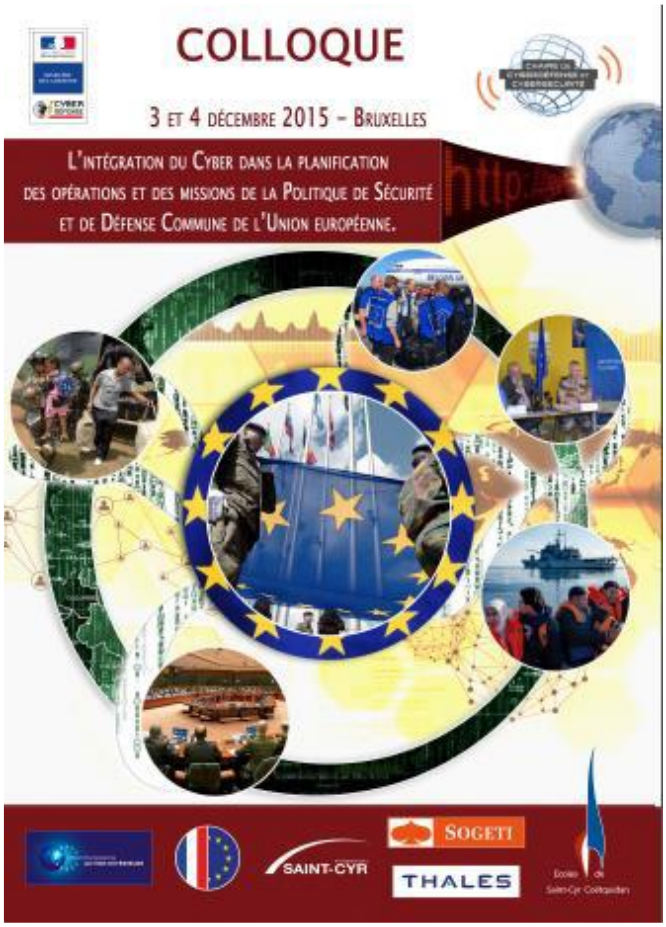
Integrating “cyber” into the planning of operations and missions of the Common Security and Defense Policy of the European Union.

Summary report of the symposium of December 3rd and 4th, 2015 in Brussels,
organized by the Chair of Cyberdefense and Cybersecurity
Saint-Cyr / Sogeti / Thales
held at the Représentation Militaire Française



The idea of having a security and defense policy is not new to the European Union. The will to have common defense was introduced in 1992 in the Maastricht Treaty (Treaty on European Union - TEU) in Article 17.

The omnipresence of automated information processing systems and their widespread use has resulted in the defense policy of the European Union being strengthened. This is present in national daily activities and during external operations. European defense is based on collective action (CSDP: Common Security and Defense Policy).

The CSDP of the EU must tackle the threats posed by the expansion of the digital space, such as cyberattacks and cybercrime. It must adapt and develop new tools against these threats. On November 17th and 18th, 2014 the European Council adopted the "EU Cyber Defense Policy Framework," detailing the priorities for integrating the cyber dimension into the European Union mechanisms for cooperation, training and crisis management.

The colloquium on December 3rd and 4th, 2015 aimed to cover the experiences of national armies in the planning and conduct of operations as well as the reasoning behind technological and organizational solutions from civil and industry partners.

With this in mind, a hypothetical scenario was developed and presented that involved planning an EU intervention outside its borders. The scenario presents the issue of a defensive reaction to a possible cyberattack in retaliation to a security action in the fictitious country of SURINIA, which is in conflict with the extremist rebel forces of CELEGO. This scenario was preceded by an introduction to the symposium on the strategy and integration of the cyber domain into European cyberdefense policy by Philippe Setton, Ambassador and Permanent Representative of France on the EU Political and Security Committee (PSC). He was followed by Francois Rivasseau the head of space and digital security at EEAS (European External Action Service), who reminded us that the will of Europe should not be below that of the Member States for cybersecurity and cyberdefense issues.

One will remember from this symposium the willingness to organize, perfect and finance European cybersecurity from the point of view of the private sector, public, military and European political representatives.

Though this may seem difficult in the EU, where 28 States with unequal technical and technological capacities have to cooperate, it has been emphasized that cybersecurity must never be achieved at the cost of economic efficiency (François Rivasseau), for which the EU was born and expanded. While opinions may diverge from the historical idea of common defense (the rejection of the European Defense Community, EDC, in 1949), and although "it would take European defense before European cyberdefense,"[1] it is not necessary to bury this idea which is taken increasingly seriously, as the symposium showed.

Philippe Setton began the meeting on a good note when he announced that the EU was in the early stages of cyber operational cooperation. He pointed out that in November 2014 the community decided to integrate cyber tools into the European defense efforts, "a recent phenomenon which will continue to develop." He then referred to the responsibilities of the States and defined their strategies, their capacities to act and thus more accurately defined the responsibilities of the EU in terms of cybersecurity.

Phase 0

The first phase will develop the case for military intervention by a European country. The French example, in particular the integration of cyber in the planning of military operations (where Lieutenant-Colonel Victor Le Bihan, "officier anticipation," Defense Staff of the Armed Forces, CYBER cell,[2] presents the different steps involved), shows that cyber operations planning follows the same cycle as kinetic operations.

Phase 1

It is time for cyber (in the planning of EU military operations) to be developed beginning with the inclusion of cyberdefense issues in the planning of CSDP operations, that is, according to Lieutenant-Colonel Gernot Schwierz, developing the architecture and structure to be adapted

[1] Admiral Arnaud Coustillère

[2] "Lieutenant-colonel Victor Le Bihan, officier anticipation, état-major des armées, cellule CYBER "

to military, technical, technological and legal challenges. Importance is given to the assessment of threats using risk assessment and cyberawareness, which use intelligence to facilitate protection, regulations and procedures (prevention), technical training (detection), and political and military cooperation (reaction). Planning is thus what makes it possible to design a response through developing reaction tools, adapted upstream of the crisis. Colonel Heinrich Krispler had previously mentioned that cyberdefense is not only protection and reaction, but anticipation and preparation, with a spectrum that covers a wider field than simple physical security of networks such as organization and training, etc.

From a legal point of view, Captain Pascal Brangetto points out that pre-emptive defense is allowed under international law, otherwise known as the "last window of opportunity," which allows for an attack before the opponent can do so. The idea of preventive defense remains more difficult to codify in cyberdefense.

Phase 2

The place of cyber in the planning of EU civilian missions.

A representative of the EU CERT, Emilien Le Jamtel, explains what CERTs are. They are divided into 65 organizations for 13 research sectors (finance, administration, security, etc.), have cybernetic technique expert groups that provide solutions to the EU to combat threats (spear phishing, infection of sites etc.), and counter attacks by groups such as APT28, 29, or SNAKE. It therefore involves the sharing of information to assess the origin and gravity of the threat and the possible solutions.

The legal perspective is also laid out, starting with a general presentation on the legal framework for external civilian missions presented by Eric Chaboureau, who said that contract staff could be posted to cyber-protection of civilian missions.

This was followed by a talk by Attorney Cécile Doutriaux (DOUTRIAUX-VILAR et Associés), who asserts that the fight against cybercrime, particularly attacks on critical infrastructures both at the national and international level, requires cooperation between lawyers and computer experts, between police officers and military police, and even between States that need a subpoena for data that involves "courtesy" agreements. Cooperation can prove to be complex since information exchanges may be denied by Member States, which sometimes interfere with each other. As a reminder, Europol (European police) and Eurojust (European justice) work, in a limited capacity, to expand these cooperations. Moreover, France is ahead in terms of accountability of internet giants and operators. It prevents the spread of cyber-caliphate propaganda and in other cases holds some accountable for major technical problems. Cybersecurity is thus built in the same way legally. The European resolutions have to satisfy the greatest number of States but “jeopardizes the credibility of the EU” because they are not binding directives.

The actors in cyberspace

The symposium then addressed the issue of the role of cyberspace actors in the EU’s external operations and missions. Michael Sieber, Head of Information Superiority at the European Defense Agency (EDA), spoke about the role of the EDA. It involves the collection of military intelligence and the protection of forces in theaters of operation through, among other things, cyber-awareness.

Grégoire Germain then spoke about the role of THALES in monitoring networks that involve repair teams dealing with intrusions and detection solutions particularly through the behavioral study of attackers and researching in open source technology. This allows them to analyze and to identify the types of aggressors and their usual techniques in order to improve cyber-resilience (ability to reset a network).

Andrus Padar (chief of the Estonian Defense League’s cyber defense unit) spoke about the possibility of using experienced volunteers (even a cyber-reserve) for use in the digital space for additional security assistance (reaction, support and prevention objectives).

However, he specifies the limits because not everyone can be involved, such the group Anonymous (trust is required).

Stéphane Taillat and Admiral Coustillère conclude the first day. Stéphane Taillat details the principle of active defense in cyberspace, where it is possible to refer to ancient doctrines such as that of Clausewitz. This shows that any strategy remains possible despite the variety and increasing rapidity of attacks across a continuum of strategic positions (possibility of deterring, blocking, using "deception" or deceit, etc.), and that the whole of the Defense is only a series of skillful blows against the attack of the adversary. However, in cyberdefense it is also possible to lure the enemy in nets in order to surround and destroy them. Admiral Coustillère recalls in his capacity as general cyber officer that the digital space is indeed a space of confrontation and combat (at the center of other spaces) and that it requires a global approach, requiring the integration of trained people in complex operations at the center of this space.

Training

December 4th was a day to explore the issues of training, the needs and opportunities. Indeed cyber experts prove to be a scarce resource and the interoperability of networks of experts remains imperfect.

Colonel Nurenberg (President of EUMCWG/HTF) asserts the importance of operational excellence through the organization of a large European market for the training of cyber experts. The ultimate goal is cyber-sovereignty (ideally reliable and credible).

Commander Jeff Vandromme, of the strategy department of the Belgian Defense Ministry, is planning a Belgian cyber-strategy, which already includes partnerships between European cyber actors (AED, EU CERT, CSED, etc.). It is a cybersecurity strategy consisting of three poles: cyberdefense, cyberintelligence, and cyber-counter-offense. It allows for the possibility of a mixed cyber military-civilian organization.

Symeon Zambas (from the European Security and Defense College - ESDC) showed that training in ESDC is recognized by all EU states. He described the partnerships (AED, ENISA, etc.) and the components, including the exchange of military students and cadets as part of a “military Erasmus.”

LCL Pierre-Arnaud Borrelly concluded the first part of the seminar dedicated to cyber-training needs in a talk covering how France has gone from the design phase to operational capacity and that J5 already integrated by France in the planning mechanisms will be at the European level soon.

This was followed by a session dedicated to the existing and proposed cyber-training possibilities in Europe. The presentation by Olivier Bartheye (teacher and researcher at CREC Saint-Cyr)[3] covered the increasing adaptation of models to address more and less serious and developed types of attacks (more technical part).

Hannes Möllits spoke about the training program offered by the Baltic Defense College on cyberdefense in English, including the different levels of training open to civilians and military personnel, and the need to create synergy between the cyber experts of the world and operational planning implementers.

Lieutenant-Colonel Paulo Nunes (MNCDE&T Project Manager) developed a curriculum in cyber-training through studying cyber-users (individuals), cyber law (cyber lawyers), cyber leaders (operational), cybersecurity (specialists) and cyberdefense (cyber-warriors).

Didier Danet returned to conclude the seminar by questioning the value of diplomas, training, strategies and strategies for the training of current and future cyber actors. He brought up the growing gap between experts and the military, where language misunderstandings become apparent as missions become more and more technical (hence the necessity for greater synergy in training). Lastly, Danet questions the strategies when faced with choices surrounding preparation for crisis management (which are currently quite conventional) when the crisis is, by definition, unconventional. This opens up vast strategic possibilities for cyber action planning (such as the choice of accepted intrusion if it is controlled or action in a contaminated environment). Future generations of experts in operations will need to make their own decisions.

Officer Candidates (élèves officiers) Barthélemy Canal, Rémi Deydier, Nicky Dorval, Gautier Grailou,
of the 2nd Battalion of the Ecole Spéciale Militaire de Saint-Cyr,
On December 9th, 2015.

[3] "Olivier Bartheye (enseignant chercheur au CREC Saint-Cyr)"