Cyberconflicts and ground forces: is the environment relevant?

Memo on the Cyberconflict and ground forces conference, Rennes, February 12th, 2013.

Gérard de Boisboissel & Didier Danet
CREC Saint-Cyr, Pôle Action globale et forces terrestres

May 2013. Article n°5.1

One of the specificities most often stressed with cyberconflicts is the existence of a threat continuum, with the same assailants using the same instruments to carry out hostile actions against any civilian or military entity, with a single modus operandi. No frontier could be drawn within cyberspace between actors, intervention fields, action modes… This would result in a necessarily global response from the powers that should, on the policy level as well as on the level of institutional organization for cyberdefense, be "inter-everything": inter-armies, inter-department, civilian/military and international.

The hypothesis of a completely silo-less cyberspace in which threats could globally deploy without being influenced in any way by the specificities of a local environment seems nonetheless somewhat unlikely.

Even if the idea of a threat remains globally the same (hamper the actions of civilian or military organizations by damaging their interconnected systems), its implementation, its potential effects and the counter-measures which could be opposed will likely change in many ways, some marginal, some essential. To stick to the exclusive subject of cyber-threats aimed at military forces, characteristics of Army cyberspace are not the same as the Navy's or the Air Force's. By nature, the Army is deployed over a geographically vast territory, hardly predictable, heterogenic, more or less fenced, where the various units will be scattered and where wire interconnections, for instance, have no place nor meaning. Land forces often operate within the population,

thereby inducing a greater vulnerability facing hostile actions on local communication infrastructures, as well as a greater risk of popular uprisings with crowds being every more interconnected through social networks, where information isn't easily monitored, and its spreading is hard to control. The environment is obviously completely different for a Navy vessel or a fighter squadron.

The mindset should therefore not be, it appears, placed at the highest level (inter-) and it should include the specific characteristics of each of the considered environments: companies and administrations, armed forces, naval or air forces… How do the specific characteristics of organizations, digital information management systems and interconnections influence the forms of cyberconflicts? To what extent can the characteristics of the physical environment in which the interconnected entity operates induce specific forms of cyberconflict? Should threats be assessed globally or should they be taken individually, according to the local environments in which they might materialize? Is the right level for cyberconflict organizations necessarily the highest, in the "inter" level? Will the counter-measures presented to cyber-threats be all the more efficient if they are conceived globally?

The conference of the Cybersecurity and Cyberdefense Chair (Saint-Cyr, Sogeti, Thales), which was organized by the Global Action and Ground Forces department from the Ecoles de Saint-Cyr Coëtquidan, aimed precisely at brushing a state of the art in cyberconflict management, considered under the angle of differentiating the environments in which ground forces evolve. This conference should be obviously followed up to pursue the methodical study of ground-level specificities, on the one hand, and to compare with conclusions come to by the Navy and the Air Force.

From this reflection conference, a first conclusion came out, relative to the necessity to prepare all of the ground forces, and not only specialists, to the matters of cyberconflicts. But general awareness within the Army personnel of the stakes and forms of cyberconflicts does involve developing appropriate training modules, which would be made comprehensible by not basing them on a too technical angle, and hinging on prior knowledge of information systems. Three levels of training could be considered. The first would aim at giving basic keys of cyberdefence to all Army personnel and would serve as a common background for everyone. It could be implemented by exercises which would ascertain the proper learning of reflexes, in the event of an attack. The second level would be a first level of technical expertise, enabling the personnel to defend the existing networks. The third level would lead

to a high expertise level, without the accurate positioning of these experts within the defense network being defined.

Stands the question of the citizen's cyber-reserve which could be created, in order to supply armed forces with a constantly-updated expertise pool, in touch with the evolutions of threats and protection counter-measures against cyber-attacks. The citizen's cyber-reserve would provide for an financially advantageous alternative, while guaranteeing a high level of expertise within the considered fields.

One general question must be asked regarding the nature and scale of the necessary adaptations to the current organization of forces, due to the development of the cyberdimension to modern conflicts. In many countries, cyber chains of command have been set up, which complicates the previous organization. In particular, the question of the creation of a specific cybercommand must be asked, given the pre-existing Signals Corps, an old branch of the army which has an obvious know-how in terms of electronic warfare and network protection. In practice, the global action of land forces will necessary involve a cyber-dimension within the mission preparation, and in its carrying out on the field. Each regiment will have to be trained to carry out cyber-conflicts, notably in the sense of protecting digital equipment and information management systems, the tasks of expertise and specific actions being reserved to specialized units within the Army, or in inter-army services. Does the appearance of cyberspace necessarily involve the creation of a specific chain of command? In such a case, might it provoke the shattering of commanding authority and deprive field officers from the positive effects linked to the principle of subsidiaries?

Because any effort which would be made in favor of cyber-conflicts would have to be made with the same personnel volume, it is necessary to accurately assess the economic cost of the priority which it is liable to receive, while keeping in mind the sacrifices which will have to be made on resources allocated to other operational functions. Increasing the resilience of military systems and of those who operate them seems a sound objective. However, taking into account this resilience within the global organization of military systems involves accepting an extra cost to train personnel and, also, securing systems so that they may still function in degraded mode. The question of operating in degraded mode also raises the question of its relevance and feasibility. Is it possible to consider a double training level which would systematically involve a normal functioning mode and a more or less degraded one? The question stands, particularly, in the case of the military environment which could

never accept the paralysis of its actions and of its weapons systems in the event of a cyber attack or of any other cause of interruption of its digital components (malfunction, digital war maneuver, bug...)

The question of the costs of these protection steps must be considered in relation with the fact that cyber-threats looms on all of the civilian and military systems, and the latter cannot be considered specific and totally protected by their relative independence from traditional digital networks. But, on the one hand, military systems are fitted with a more or less large share of components stemming from the civilian world and, on the other hand, the independence of these networks seldom reaching a complete separation (maintenance operations, for instance), protection systems are indispensable to avoid the danger of a false sense of security.

The doctrine of use, for cyberdefense, raises questions, both practical and theoretical. It is commonly admitted that the lack of control on the effects of a cyber-attack keeps countries such as France from considering carrying them out and concentrate on protecting their systems, in a network defense strategy. But once this principle generally established, the defining of limits between cyber-attack and cyber-defense doesn't go without its share of problems. For instance, should a defense system be limited to the neutralization of the threat or does the attack authorize the defender to reply by attacking the author or vector of the said attack? Can we go further and consider preventive attacks against potential or ascertained enemies? Likewise, cyberdefense cannot be designed in an isolated way and must be articulated with the other fields which are connected or complementary (electronic warfare, information, counter-information...)

This day enables us to measure the interest of a reflection for each environment, complementary to the analysis which is traditionally dominant and which places cyber-conflicts under inter-department and inter-army aspects. It raises many theoretical and practical questions pertaining to the organization of cyber defense, its doctrine, its implementation within the forces, the training of personnel... The Global Action and Land Forces center therefore wishes to pursue this reflection. It will organize, in June 2013 and during the next years a series of events, open to the public. If needed, it will organize specific workshops for specialized military personnel.