Strategy and networks in the conduct of military operations

Captain Djamel Metmati

December 2014 - Article V.2

The convergence of human and technical networks has an impact on the conception, the planning and the execution of a military operation. As most of the armies of the world are based on intervention models, their deployment is based on principles relating to the characteristics of the networks. Their engagements require the control of the spreading out in order to ensure the coordination of the units and a temporary control of the cyber-space face with potential adversaries. This operation craft, which can be the result of a controlled strategy, determines the capacity of an army to manoeuvre in a context where the network reaches the lowest tactical levels.

The military operations express a strategy based upon architecture, capacities, and an army format. Established with a war target, they are the reflection of a combination of this set in an area in a given time. In this deployment, the role of technical and human networks has taken a new dimension in order to establish the conditions of a favourable engagement.

As usual, the capacity to generate ad hoc alliances [1] in order to support the action seems essential. In 2003, the United States got involved in Iraq searching for allies. To result in force generation, the implementation of technical and human networks is necessary. This need is not a prerogative of times of war, and begins in times of peace. The stake is linked to the collecting and processing useful information for military operation. Displayed as data and transported by physical supports, the information has become both a means and a stake. It conditions the military manoeuvre operation and has the characteristics of a weapon which can weaken the opponent's will. It is applicable on the whole range of current operations.

From coercion to irregular war, including peacekeeping, it is at the centre of a battle for detection against discretion, and interception for destruction. Each opponent tries, depending on circumstances, to control these four steps at one point in the military action. In this context, the relative distance of the current battlefields creates major lengths in the transmission of information for the armies. This phenomenon, increased tenfold by the constitution of very mobile armies capable of eliminating space constraints, leads to the control of the system of networks.

Though the conduct of the war introduces networks into the strategic and operative action, it also introduces innovative processes applicable to the different phases of the launching of an operation.

1 Theoretical tactics, Colonel Michel Yakovleff, Economica, 2006.

I - The novelty of networks in the conducting of war

A source of wealth and power, the convergence of human and technical networks give military operations a rhythm enabling strategic and tactical surprise.

1.1. The role of innovation in strategic superiority

Though innovation is a chance to reshuffle the cards and change the ground rules, it is very difficult to anticipate. What's more, in war, the first thing to do is to make sure of the conditions which make it possible in an operation. It is expressed as much by the methods as by the means, by giving new efficiency to a manoeuvre or an operation.
During World War 1, a commander in chief had to have artillery capacities in order to lead efficient offensives. In 1940, the air force [2] in support of the armoured vehicles seemed particularly important in order to accomplish this kind of operation.
But, since 1945, the evolution of the art of war needs rather more a capacity to combine all of the classical means with the help of networks. This practice isn't new. The Roman and Mongol armies based their superiority on their capacity to master their movements from the technical and human aspects of their networks [3].
However, today's technology makes it possible to give the military operations another form and contributes to conducting the war in a different way in the conception, planning, implementation and execution phases. The emerging army models include the capacity to fight in a world of networks called cyber-space.
The military consequence of these dynamics implies that a combined effect of the electronic war and of the information and communication systems has an influence on the manoeuvring of an army. The Air Force and the Navy are currently at the forefront of the integration of networks in the conduct of their operations, making their jobs precious in crisis management, urgent engagement in protection and intervention.
The land forces and specific units strictly acting in cyber-space are barely beginning to integrate this particularity into their operating modes and their operating procedures. Working on the assumption that the concepts exist, the consequences in strategy and tactics open new perspectives in the rhythm of the combined and joint operations manoeuvres. An army which is constrained by its framework and its resources can move in this direction in order to strike hard and fast by using these more powerful means at a chosen time, whilst focusing on the manoeuvre [4]. Thus, the network technologies spur innovation in the application of military action.

1.2. The importance of armies built as systems

Maréchal Foch established three great principles which define the course of action for any commander in chief [5], the ex-post analysis of the historical battles show that the conscious application of freedom of action, focusing efforts, economy of means, leads to victory or defeat depending on circumstances.
This characteristic is at its most acute in the coalition wars and those where the balance of power is not in favour of one of the parties [6]. These features show how an army set up as a

2 The development of Colonel Von Richthofen's stuka was, for example, a milestone in the German breakthrough in May 1940.
3 The Roman army, Catherine Wolf, CNRS, éditions Paris 2012.
4 The myth of flash-war, the campaign of the West of 1940, Karl-Heinz Frieser, Paris, Belin, 2003.
5 The principle of war, Maréchal Foch, Economica, 2007. These principles are freedom of action, focusing efforts, economy of means.
6 The historical examples are numerous. One can quote the Napoleon Empire wars and the Arab-Israeli conflicts between 1948 and 1973

system associated with the manoeuvrability of the troops and the commanders in chief can reverse a disadvantageous situation. Even if an army which has a large staff has greater regeneration abilities over time, it can be beaten by an opponent who is more intelligent and more apt at manoeuvring. And as the orders of battle are subject to the nature of the weapons, the construction of the units is also a reflection of the lethality of the technologies nowadays. Thus the fight to close the gap between the technique and its integration in the armies still creates archaic behaviour, which is partly visible in the war.
The network technology adapted to strategy and tactics generates a discrepancy with the sociological acceptance of the new concepts it generates. It supposes a controlling of the dynamics produced by the cybernetics effects in each army through each technical aspect added to the human tasks. By encouraging integrated operation, cybernetics format an army system which is demanding in method and organisation. The manner for the integration and the comprehension of this innovation linked to networks is the key to conducting operations in a new style.

1.2. The adaptation of networks to war

Weaponry does not determine the outcome of the battles; it conditions their form and changes the combination between weapons and armies. This is why; the art of war must reinvent itself at times when technology redistributes the factors contributing to victory. Especially since operational superiority factors for an urgent engagement in protection and intervention imply prior conditions. The ability to create networks at short notice out of strong coordination set the level of power of the engagement. It is transversal because it affects logistics, supports, and the fight. It also deals with adverse attacks that try to limit, destroy or disrupt deployment.
The networks therefore generate deep consequences in the political and social systems. They change the organisations in their operation and their capacity for action. They increase the ability to surprise an opponent by making possibilities for brutal action on long distances [7] available to the military leader. The demonstration made by the American army during the first Gulf war [8] set this new conditions for any operation.
This is why the adaptation of networks to war consists in winning the battle for information [9] in the largest sense attributed to cyber-space [10]. An operation conducted with no controlling of the networks is condemned to follow its opponent's rhythm. The base of this power originates from a powerful digital economy supported by a state system which itself is organised as a network [11].
This aspect changes military operations which, in order to survive, have to adapt to this context. Though there are two possibilities to counter the flaws in an organisation – the coordination of individuals throughout human networks, and the personalities' own ability-, this motion pushes military leaders to constantly transform their forces into systems. In this framework, though Foch's principles remain relevant, the networks generate new ones in combat processes.

7 Conducted in the form of cyber-operations in the networks.
8 Especially in the case of the air weapon.
9 War and manoeuvre, under the direction of Christian Malis, Economica, fondation Saint-Cyr, 2009.
10 Anything that transits in the form of data.
11 The information theory, Aurélien Bellanger, Gallimard, 2012.

II – New combat processes

Three processes can thus be identified: poly-centrality, dispersion, protection. The latter are not intended for distance, but rather more a convergence of efforts. The aim being to apply the violence of war in rapid style without there being any indication of offensive movement from the initial positioning of the units.

2.1. Poly-centrality

Poly-centrality makes it possible to create network nodes which can extend the spreading out of the operations up to thousands of kilometres. They are connected with the network backbones meshing the territories, and with the satellite systems for the richer nations.
This means that the military power of a country is supported by an ability to mesh the physical geography of places in communication networks and roads. The national operators and a large concentration of data-centres supply the basis for this poly-centrality. By capturing data in a place at a specific time from digital factories, the nations produce added value for their actions which are specific to the defence of their interests. During an operation, this system from times of peace contributes to facilitate rapid position changes of the forces on a given field by using architecture of modular communication and information systems.
Likewise, poly-centrality is conducive to the expression of the firepower in a new style. As the ratio between firepower and number of units keeps increasing with technology, the battlefield becomes a threatening vacuum in which an attack rises and recedes depending on the goals. An army without poly-centrality factors could not engage in mobile combat without the risk of being destructed before movement [12]. Hence anything conveying information multiplies the chance of good coordination of complex spaces [13] at higher levels of combination.

2.2 Dispersion

Dispersion also becomes a process. When a military operation has a force capable of creating networks, its units can be far apart. This trend can maintain the fog of war for the enemy [14]. It does not perceive the main effort and the potential combinations likely to hit him. The German armies used this principle at the beginning of the 1940 campaign by preventing the French government from knowing the main effort. Conversely, an army which cannot disperse will try to initially be concentrated, and will therefore be more vulnerable to strikes during these manoeuvres [15]. From then on, a double fight starts between detection/discretion and interception/destruction. This fight is supported by communication and information systems that are used by entities other than the usual commandment posts. Thus, a soldier, just like a service, can be a sensor or a broadcaster.

12 The Iraqi army during the 1991 Gulf war.
13. The development of air and land combat drones also makes it possible to transform them into mobile relay antennas for the armed forces.
14 In order to deal with this problem during the first Gulf war, the Iraqi purposely set fires around their armoured vehicles in order to avoid being hit by air strikes when the coalition found an opportunity.
15 Operation desert storm from 1991 show how the Air Force covered the land making the Iraqi forces to go underground and disband.

Other problems are arising from the dispersion process. It dilutes responsibilities and tactical opportunities if the networks are not built according to a hierarchical approach based on a discipline of use at the army-staff and units level. The isolation which is specific to dispersion implies superior decision-making and leading qualities. The autonomy which must be apparent and the vision of the moment will determine the result of the manoeuvre. This fact appears in the decision process. Being able to see in dispersion a strike capability in relation with a tactical opportunity supposes reasoning that integrates sparse and partial information from the remote units, in an equation where networks restrict or increase the combinations for the managers.

2.3. Protection

Protection is the last combat process. It makes it possible for the States and their armed forces to keep their freedom of action with regards to other countries, but also with regards to non-state groups with digital power [16].

In order to asphyxiate its opponent before it even gets a chance to get into motion, the tempo induces continuity and disaster recovery plans for the military and state networks. They are an answer to the possible strategic and tactical cyber-attacks.

Each creation of territory generates a fight for its possession; cyber-space is no exception to this rule. It reproduces international tensions under other forms. In other words, an opponent will try to act in the numeric field at more or less technical levels in order to break the rhythm of the operation. The goal of these plans is to limit the effects of an offensive on national networks.

Regarded as much as a place for exchange and confrontation [17], cyber-space, unlike physical spaces, is not controllable because the interconnections are such that they leave two possibilities of control to the States. Either they proceed with a black-out of the networks, which seems rather unrealistic if one takes into account the role of the networks in the economy. Or they try to filter, regulate and formalise networks which is not easy to do, even by the greater cyber-powers.

Protection therefore has two opponents: the States and non-state organisations. In both cases, military action is faced with the quantum features of the movements. They generate brutal changes in situation status due notably to the number of connections associated to their scope. This shifting terrain leads to vulnerabilities used by the attackers. The experimentation of drone X47B partly reflects this problem. By having a drone capable of catapulting itself from an aircraft carrier, the Navy has a greater spreading out possibility in order to strike targets in the case of an attack on Taiwan, whilst keeping its Air-Navy group out of reach. On the tactical level, this notion of protection implies the defence of the physical integrity of the supports and access points of the national networks.

Faced with non-state organisations, the networks foster dissent, the emerging of parallel networks and attacks combining direct and indirect style. Protection implies fighting against their offensive actions by using the same methods, whilst being on the same level of engagement. They are as much about strategy as they are about tactical conducting. In strategy, they unsettle the States. During the Uzbeen ambush, the Taliban lead a media campaign strongly relayed by the networks. They made politicians consider the question of the relevance of the French engagement in Afghanistan.

16 For example Hezbollah, Anonymous, the Blacks blocks.
17 Cyber-strategy the art of the digital war, Bertrand Boyer, Nuvis, 2012.

In contrast, the Kenyan forces largely used Twitter to communicate in real time during the hostage taking in Nairobi in 2013, while at the same time preventing the traditional media to take the initiative of information. This overall assessment of combat processes related to networks transforms the operations which appear as a means to apply an original strategy [18].

III – Adapting the strategic phases

A military operation is composed of several phases: conception, planning and execution: each of these phases needs to take into account an approach through networks [19].

3.1. Conception

The conception of an operation is the result of a combination of goal-oriented available means, within the framework of a limited environment. It is inspired from a war plan transformed in an operations plan, and leads to the creation and the projection of a force in faraway and limited areas.
The plans aim to control the creation of a temporary autonomous area which is structured around communication and information systems. The force deployed is structured on this device, enabling the combining of services. By deploying a diversified range of military satellites during the first Gulf war, the Americans had freedom of action in the use of the air force in a coalition broadened to several countries. It should be pointed out that there are two dimensions to take into account for the conception of an operation. First, the networks enable a geographical spread of the alliances with a narrowing of the geo-political action. As a State cannot oppose another one without having first compiled a community of interests, original network strategies are established in order to establish coalitions.Very distant countries can converge around common interests in a given situation. This principle was already prevailing in the past, be it for the opening and the consolidation of trade routes or for technologies such as the telegraph and radio. Nowadays, this trend brings the parties more closely together, which makes it more reversible in time. Then, no planning can be limited to purely military problems, since it must systematically include the media dimension without losing sight of the political goals.

3.2. Planning

Planning consists in defining the necessary steps to achieve the war objectives. It aims at articulating a force made consistent by a "network bubble" in order to enable the autonomous or combined engagement of an army.
National networks which are controlled from beginning to end give power to the operation. The more a nation is capable of combining a strong spreading out with data transmission speed necessary to lead units, the more its armies are able to concentrate, disband and recombine on very short notice and greater distances. What's more, the new perspective given by cyber-space adds another dimension to this principle by enabling the use of cyber-operations in adverse civilian and military networks [20].

18 As for example the cyber-attacks lead against Iran in order to slow down its nuclear program.
19 The network war in the XXIst century, Jean Pierre Maulny, éditions du Félin, 2006.
20 « Integrated and network warfare », Major Général Dai Qingnim, China military science, 2007.

The development of mobile terminals such as smart phones, tablets and computers shows the hold of the problem of networks in operations. The Marine Corps integrates cyber-space in its combat actions, and within the military staff, electronic war cells act against adverse networks on the operation field, but also against the infrastructures of the enemy country [21].
In fact, military operations are a part of a flow logic induced by the pervasiveness of networks, the commander needing to constantly take into account the detection, discretion, interception and destruction fields during the action.
This network logic does not place leaders in the background, quite the opposite; it necessitates forward management in which the commander is at the centre of an information node. It can be temporary yet be crucial for the act of war. In fact, the leader directs the movement of his units, and seizing the crucial moment which most great war leader can feel becomes possible. In order to attain this target, the network is a means to regain control over its units despite distance. It increases the capacity of units to communicate and share on the basis of the initiatives from the subordinate levels.
As a result, the networks suggest thinking about the military operations of today according to the spreading out capabilities rather than the focusing of the means. By maintaining distant links without interrupting the exchanges, an army can then concentrate according to needs.
This specificity is enhanced by a militarisation context of the cyber-space where military operations can be engaged directly through networks by non-conventional means. It implies the emerging of new types of soldiers such as were the gunners, aviators, submariners. And it suggests the understanding and the mapping of the communication infrastructures through a digital geographic atlas of the data centres and other friend or enemy transmission nodes. The consequences on the conducting of operations necessitate the sanctuarisation of the electromagnetic environment by using cyber-intelligence [22]. Inadequacy in mastering this phase prevents the execution of large-scale operations.

3.3. Execution

The execution process includes the managing and the processing of the information in the operations. These two processes imply more coordination and formal discipline in the transfer of information [23], and also modify the form of military organisations.
Nowadays, the armies of the world make different choices on tactical reference levels. Some keep the division whereas others move towards the notion of pooling concentrated services within reinforced units. Integrating networks gives the group a mobility which is superior to that of a traditional division level, whilst increasing the speed/power ratio in the manoeuvre.
This effect is observed at the level of the basic units by adding a deputy managing the information flow at the company commander level. This need is de facto broadened up to the operation theatre where the network deputies have the responsibility of the military databases related to the crucial interests of the countries. From then on, in the manoeuvre, the technical infrastructure providers become strategic players because they identify the information routes with the physical and digital universes partially identifying the framework of the military operation.
During World War I, General Ferrié used a French post camouflaged as a German centre which communicated journey modifications to the Zeppelins: they would bring the airships above the aviation camps and the French batteries.
What's more, the technical infrastructures are nowadays set according to the intensity of the traffic and the priorities. The main artery, commonly referred to as the *Backbone*, links the major centres where domain names are verified, addresses authenticated, communications redistributed.

21 Chinese and American network warfare, Timothy L.Thomas, 2005.
22 It is more general than signals intelligence
23 The Psychology of battle, Karpov and Jean-François Phélizon, Economica, 2004.

The generalisation of data centres associated with cloud-based solutions become strategic targets for the air weapon and missiles. Then, the networks can be subjected to deception manoeuvres by increasing the traditional fog of war by the alteration, the paralysis or the destruction of the information. The military operations can then be supported by digital actions. As shown by the third law of Newton which states that for every action there is an equal and opposite reaction, they generate cyber-operations in cyber-space from the tactical principles of traditional war. They aim at paralysis [24], intelligence [25], destruction. By targeting specific aims that integrate system weaknesses which are unknown by the opponent, with their effect increased by the network in which they have to manoeuvre, the cyber-weapons have a potential for destruction. In 2012 for example, the Shamoon virus infected the Saudi petrol company Aramco and resulted in the destruction of 35 000 computers.

This status brings very closely together the conception, the planning and the conducting of military operations. Though this phenomenon has existed since the introduction of the radio in military operations, it has been accelerating with the denser network introduced by cyber-space. For the first time during the First World War, an army could use the wireless signal in order to lead and intercept adverse communications. The Second World War strengthened this trend by supplying radio systems to the units.

Nowadays, the feedback on the wartime experiences disturbs this phasing by the immediate effect of the network. The proliferation of sensors and the arrival of the Internet into war change the strategic and tactical approach of a military operation.

Conclusion

The converging of strategy and networks in military operations stems from cyber-geopolitics. An operation will have only have value if the cyber-space is controlled in its broadest definition at a given moment. What's more, the armies don't only move on their territories or their immediate neighbours' territory, they engage in interventions which require a different combination of force.
In this framework, the digital economy becomes a sovereignty stake. Its development generates military power through the densification of networks, and their use.
The goal is to maintain some control of the physical territory through the control of its digital space. For this purpose, it is better to think in terms of entry points rather than in terms of border defence. China and Israel understand this principle, and are unique examples of original civilian and military strategies, while building a digital sovereignty which is based in the case of China on its own norms and a volume of Web users exceeding that of the other States, and as a result the programmed opening of its networks to the rest of the world would make this country the leading digital world power.

24. Saturated bandwidth
25Operation Newcaster, Thierry Berthier

Fondation Saint-Cyr, Ecole militaire, 1 place Joffre, 75007 Paris
Telephone: 01-45-55-43-56 - email: contact@chaire-cyber.fr; SIRET N° 497 802 645 000 18
The Chair thanks its partners