

Old wine in new bottles: deception in modern warfare

A persistent enabler of victory in information-age warfare



RUSI brief: In an information age of constant and persistent ISR, is military deception still possible?

Major JAY Stéphane

Major EPHRITIKHINE Nicolas

Old wine in new bottles: deception in modern warfare

A persistent enabler of victory in information-age warfare

War is uncertain, and surprise – accidental or deliberate – plays a vital role in tactics. The recent exponential growth of information and communication technologies (ICT) has highlighted the idea of a ‘transparent battlefield’ within the framework of constant and persistent Intelligence, surveillance, reconnaissance (ISR). This could both make surprise irrelevant and weaken the ability to deceive an enemy tactically, leading to a military stalemate. Yet this has not been the case.

History shows that the concept of deception has not been of constant interest. Sometimes deception has been at the forefront of symmetric wars or when tactics are blocked; sometimes it was in the background for Western states, when they have held the advantage in a conflict or for cultural reasons. Deception used to be (and is still) a critical enabler of surprise at the operational and tactical levels and an (undisputed) advantage when trying to seize the initiative.

Modern armies now operate in a more and more contested environments against potentially high-intensity threats, where they lack mass and where concentrating forces is dangerous. Deception will multiply the effects of new doctrines (Scorpion in France, MdB in the US, Strike in the UK) and allow more effective actions in new environments such as influence and cyber.

Whether we consider war only in a scientific way or more in its human dimension, our understanding of what is deception may have to change. War is an Art in which deception is a masterstroke.

Remembering that war is above all a duel of will in a Clausewitzian sense allows new perspectives for deception in the information age. *Technological advances not only continue to support deception as a critical enabler for achieving operational surprise and seizing the advantage, they reinforce it.*

This paper will discuss how with new tactics and means (new bottles) we can wage deception operations, adapting already known tricks used for centuries (old wine) in a new environment.

Table of contents

Table of contents3

- I. Military Deception (the old wine)4
 - A. Military Deception: various definitions and their implication4
 - B. Common principles and criteria5
 - C. Deception and technological perspectives (XXI-century bottle)8
 - D. To go further: constraints and prospects for land operations11
- II. New perspectives for deception in future warfare (old wine, new wineries)14
 - A. Cognitive bias in HQ's decision-making process allows deception14
 - B. Deception in MDB15
 - C. Deception in Scorpion and non-linear warfare perspective17
- III. Creating uncertainty through cyber (old wine, new bottles, new delivery systems)19
 - A. AI and countering enemy deception19
 - B. Deception in cyberspace, kingdom of the assailant20
 - C. Cyber-deception actions: wasting time23
- IV. Influence (adapting the label, storing the bottles)23
 - A. Influence as a way to reduce effectiveness in military operations24
 - B. Democracies: tempting targets.25
 - C. Democracies must be able to use these weapons26
- V. Conclusion: to go further28
- VI. Appendix 1: Scenario OLD THREAT, NEW MEANS29

I. Military Deception (the old wine)

The concept of deception does not enjoy a common understanding throughout military organisations. Moreover, it does not apply in the same way at the strategic, operational or tactical level. In this study, we will focus on the *operative and tactical levels* and not consider socio-cultural, economic or political areas and their necessary multi-domain coordination.

A. Military Deception: various definitions and their implication

French definition: « Effect resulting from measures intended to deceive the adversary in leading them to a false interpretation of the friendly attitudes, in order to encourage them into responding in a way that is detrimental to their own interests, and reduce their response capability. Deception includes concealment, diversion and intoxication. »¹

US definition: “Military deception (MILDEC) is actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.”²

UK definition: “measures designed to mislead the enemy by manipulation, distortion or falsification of evidence to induce him to react in a manner prejudicial to its interests.”

While the French definition emphasises the effects on the enemy, the US definition refers to friendly actions. The American definition intends to be operational. Their Jominian approach, rational and scientific, confines deception to a mission subordinated to the friendly operation – to the same tempo and the same objectives. This scientific approach to deception allows its integration in the range of military effects and above all gives it a pivotal place in planning and conducting operations. The study of FM 3-13.4 "Army support for military deception" gives clues to managing difficulties related to allocation of military means.

A more Clausewitzian approach, the French definition stresses the human duel in war and insists on an effects-based approach, which assumes that the enemy is unpredictable and can only be influenced, not directed. Concentrating on the adversary allows more freedom of action in time and space for, and greater effectiveness of deception, over time and at different levels. It also allows focusing on the efficiency of measures releasable to the enemy. It integrates the uncertainty inherent in perception and differentiates the action of deception from the rest of an operation. Yet deception does not answer *how to* integrate uncertainty in the planning process nor how to allow military resources. Therefore, it seems less operational.

The British definition appears to be quite similar to the French. Nevertheless, variations in courses of action seem to focus more on perceptions than on physical actions on the ground.

¹ EMP 60.641, Glossaire français-anglais de l'Armée de Terre, CDEF, janvier 2013, p182.

² US Joint Publication 3-13.4 : Military deception

In all three definitions, deception is regarded as a multiplier of the friendly action. **Deception has only one purpose: to maintain our freedom of action, either by reducing the adversary's grip or pressure or by depriving him of his own freedom of action by making him take measures contrary to his interests.**

While building on this convergence of views, it now seems essential to draw up a more concrete *typology of what is meant by deception and of possible courses of action to achieve it; are there common principles?*

B. Common principles and criteria

Conducting a deception operation requires first a study of the main principles to be respected. Even if these are relatively obvious, it is certain that several operations have failed because they have not been respected.

1. PRINCIPLES

a. Aim at the opposing leader

Deception aims at the opposing leaders and only them, the chief at my level or of the level that will undertake the manoeuvre that I want them to engage in. Knowledge of the personality of the chiefs and their entourage, doctrine, the functioning and the organization of its intelligence systems, the time-frame of its decisions, is therefore essential.

You must not miss the objective and try to fool someone else in the organisation. For example, the British had observed in Burma that it was impossible to lure the Japanese command as Japanese generals held their intelligence officers in such low esteem: intelligence officers could be fooled but generals did not change their intentions.

b. Only hide what can be hidden:

What you want to hide or mask is usually the goal or the point of application of the effort. Meanwhile, it is unnecessary and expensive to try to hide the evidence. Deception will therefore start from a healthy assessment of what the adversary cannot reasonably ignore since it is on what the adversary knows or believes that his decision will be built.

Too often, staffs classify as "essential friendly information" (those whose secrecy must be kept at all costs) information that no one can ignore or that everyone already knows. A clear SECOPS policy must be built during the planning process, involving not only J2 but all the branches so as to avoid such an "overly-secret" tendency of Hqs.

c. Subscribe to the enemy's assumptions:

It is easier to make the opponent believe in something he already believes in, or that he hopes to have prepared for, than to get him to change everything.

In May 1940, Manstein rightly believed that the Franco-British expect a repeat of the Schlieffen plan. By self-suggestion alone, the French command refused until 13 May to believe the information reported by the air force on armoured columns in the Ardennes.

Franchet d'Esperey in Macedonia in September 1918 put his main effort on the Serb side which the Germans considered to be neutralized. The French general reinforced the Serbs with two divisions and French artillery (while the Germans could not imagine him putting a single soldier under the orders of such "backward" leaders). He then carried the effort in the Moglena (a naturally impregnable mountain triangle closed by two rivers without bridges) while the German command could only await an attack in the Pelagonian plain or the Vardar valley where he concentrated their artillery and deployed his reserves. The conviction of the German generals was so strong that no intelligence reported by Bulgarian commanders on the astonishing preparation works they could observed in front of them could convince them. A bit of concealment (secrecy, camouflage of work, night movements and deployments), a bit of intoxication manipulation (organized leaks on secret landings of tanks in Salonika which obviously could not support a mountain attack) did the rest.³



³ Max Schiavon, Tallandier, 2014, « Le front d'Orient: du désastre des Dardanelles à la victoire finale, 1915-1918 »

d. Develop unpredictability in the manoeuvre:

Staffs have a universal flaw: they are predictable. However, deceiving or surprising requires being unpredictable. There are two options for the military leader:

- acting on Liddle-Hart's famous "least waiting line" by systematically choosing the course of action that the opposing staff will understand as less probable because unworkable, refuse the average and agreed solution, cross where the geographical cell tells you that the terrain is no-go and avoid its avenues of approach;
- give flexibility by choosing a course of action that offers many branches, leading in each phase to targets that open up several possible directions of action.

e. consistency, redundancy, convergence:

Deception cannot work if the clues produced in the various functions or different levels or parts of the command are not coherent and convergent, and if their abundance does not counteract the effects of what will be impossible to hide. At the very least, one needs to maintain uncertainty and doubt (which is, for example, the object of all "display manoeuvres grouped under the code Fortitude"). As a result, a decoy manoeuvre must be coordinated closely in all its parts.

However, and this is a paradox, one must be careful not to push the line or exaggerate the number and nature of clues to prevent the opponent from finally not taking the bait.

TOPOLOGY OF DECEPTION ACTIONS

A deception operation relies on two families of processes: cover-up and simulation.

a. The cover-up

It involves fighting the adversary's intelligence capabilities, passively by acting out of their reach or actively by attacking them.

Passive ways:

- Hide the manoeuvre using terrain, weather, darkness and the environment. Even if in the information age all this seems irrelevant, these military fundamentals affect the security of one's forces. Non-compliance can be fatal at the tactical level.
- Exploit special conditions that favour surprise):
 - o Doctrinal: historical examples of the unexpected use of force are winter combat, divisional combat, night combat and more recently combined and joint cooperation; in the future, "non-linearity" could result from this doctrinal surprise (will be developed in part 2).
 - o Technical: Increasing range of strike with the rifle and artillery, the tank or combat gases, digitization, and collaborative combat are typical technical advances that make technical surprise possible, and they can only be fully effective after a doctrinal translation.

- Camouflage and physical concealment
- Intoxication
- Secret: classification and limited dissemination of documents and information (Franchet Esperey ordered that only three copies of his plan be made, considering that "there was a lot of talk on the terraces of Salonika cafes"; Turenne used to keep his intentions to himself...). As mentioned in the principles, the level of secrecy must be controlled and limited or it could obstruct the manoeuvre and be counterproductive.

Active ways:

- Counter-intelligence or operations aimed at destroying, neutralizing, blinding, the means of enemy intelligence
- Security, secondary manoeuvres to mimicry or conceal the main manoeuvre

b. Simulation

Symmetrically, simulation exploits the enemy's intelligence assets. This assumes that these are effective enough to see what we want to show them and interpret it in the way we want, yet not enough to crack the ploys we employ. Simulation and cover-up require skilful handling, but the analysis of many battles shows that the simplest manoeuvres are often the most effective.

Passive ways:

Intoxication: Spreading false clues and fake news; it is also part of the cover-up.

Active ways /Manoeuvre:

- Simple manoeuvre "on the line of least waiting"
- "random manoeuvre ": multiple objectives, multiple manoeuvre options.
- Feint: simple manoeuvre on the most expected line
- Demonstration
- Diversion

C. Deception and technological perspectives (XXI-century bottle)

We can now measure the relevance of these processes of deception in light of likely technological and organisational developments in (future) warfare.

At the tactical and operational level, future warfare must be characterized by a struggle between detection and simulation capabilities. With developments in detection, it seems increasingly difficult to surprise the enemy. Five trends reflect this difficulty:

- the *proliferation* of sensors (air, marine, autonomous ground, cyber, space): the battlefield is now observed by a very wide spectrum of sensors that allow information to be cross-checked and clarified;

- a *wider variety* of signals: this gives a less piecemeal and more complete view of the battlefield;
- The *persistence* of observation: mainly because of drones, this trend may be accentuated by the use and proliferation of new aerial or satellite vectors;
- Increased sensor *accuracy*: the launch of the CSO2 satellite, and soon the CSO3 in low orbit, allows us to move from detection to reliable identification. Spectral cameras multiply infrared observation;
- *Added Capabilities*. Crossing IR bands, radar and visible observations significantly improve the detection of camouflaged vehicles;
- The near-real-time transmission of information to military and political decision-makers.

These technological developments obviously undermine the ability to cover one's battlespace assets. However, they also offer a greater grip on the opponent, which strengthens the intoxication and the simulation processes.

"Getting a perfect knowledge of his enemy is dependent on a stupid enemy unable to keep pace with relevant countermeasures. Such enemies are rare"⁴

Combining thermal, infrared and even radar signatures by incorporating conductive fabrics to complement the visual aspect, the latest-generation decoys should be particularly effective. Their use in the recent conflict in Nagorno Karabach is striking⁵. In the Western armies, their use was hampered by the lack of a doctrine such as the American *Multispectral Close Combat Decoys*.⁶ As part of its hybrid approach however, the Russian military are showing a real interest in decoys.

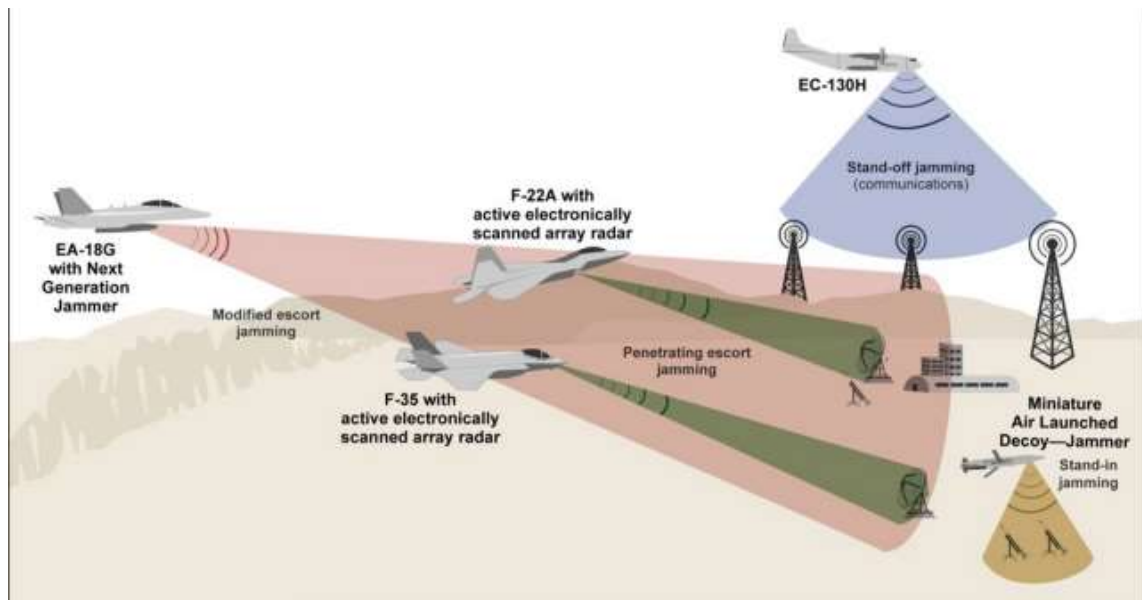


⁴ D.Betz, *Carnage and connectivity*, Londres, Hurst, 2015

⁵ uasvision.com, « Azerbaijan Used Unmanned Antonov Decoys to Reveal Russian S-300s »

⁶ US Field Manual 90-2, *Battlefield deception*, ch.5

In electronic warfare, it is possible to consider the creation of fake digital units. The use of drone swarms would simulate flights of larger aircraft. Making old aircraft into ad-hoc UAVs triggered the Azerbaijani air defences, which enabled Armenian counter-batteries to target them more effectively. The prospects of holography could lead to the further development of convincing decoys as their ability and resolution is improved.



Concealment is equally still possible thanks to technological developments. Next-generation camouflage, radar wave-absorbing coatings and paints already exist. Thermo-reactive tiles to mask thermal footprint are the beginning of a multispectral camouflage. The use of fumigants, and by extension suspended sub-micronic particles, are part of the technologies available to disrupt or prevent optical and infrared detection.

The U.S. military has integrated all these processes into a broader electromagnetic and cyber approach in its 20-40 concept.

Electronic and cyber deception developed later in this study is part of a comprehensive approach aiming to create uncertainty.

The development and democratization of autonomous robotics and drones will inevitably change the use of armies on future battlefields. Within a decade or so, autonomous units could be established. In particular, they would respond to the lack of numerous units and would allow the development of genuine disappointment ops. The development of robotized swarms offers multiple tactical possibilities that open the way to new processes of simulation (in tactical manoeuvre, modification of the electromagnetic environment) and concealment (jamming, saturation).

⁷ Gentleseas.blogspot.com, Australian Growler Jamming Aircraft to work with Australian F35s, March 2017, Peter Coates



8

The main weakness of western armies lies in their lack of doctrines that integrate both the current means and foreseeable technological perspectives. It seems essential to consider doctrinal and operational developments to develop a mentality capable of "blurring one's tracks" in an increasingly transparent environment.

D. To go further: constraints and prospects for land operations

Before considering the modalities of implementation of deception, it seems necessary to open the subject to broader considerations relating to the means for, and the key moment of a deception operation. The aim here is to open up some general avenues of reflection that could be the subject of further research.

1. Operating deception in coalition

At a time when coalition engagements have become the norm, with allies of equal rank or in support of a partner in difficulty, the development of deception manoeuvres poses two problems that cannot be solved generically.

The first issue is that of dedicated resources. It is hardly possible to propose an increase in the force deployed for deception. Thus an Operation Commander will from the start have to allocate some forces to this manoeuvre. This will potentially reduce the commander's balance of forces and this additional risk will have to be weighed against the benefits of deception. In a coalition, this difficulty is increased by the existence of CAVEATS and potentially by the

8

natofoundation.org

political reluctance of states to take this additional risk. The prospect of robotic and autonomous units to eventually provide the necessary mass could relieve this constraint of having to find and commit troops.

The second issue concerns the differences in doctrinal approach already mentioned, but also the level at which a deception operation can be undertaken. In the Western world (notably the US), the division seems to be the first level of a multi-domain deception operation. However, the latter remains at tactical level and its deception action can only be understood within a wider manoeuvre at the operational and strategic level. It is therefore a "Russian doll" operation, for which the tactical effects would be defined by a division while being integrated into a broader approach. Thus, beyond the level of the key element is coordination, which goes far beyond the current framework of "parallel planning".

2. Deception in defensive phases

Deception is commonly found in an offensive operation. It is much easier and makes more sense to dedicate means and to widen the operational spectrum when we possess the initiative. However, deception could be an essential part of recovering initiative in a defensive operation.

Taking back the initiative is conditioned by several factors, including the restoration of a favourable balance of power. In this perspective, a deception operation could make the enemy's manoeuvre more predictable and would help establish the conditions for resuming the initiative. Such a deception can be achieved by using technological means to simulate positions and to attract the enemy, but it could also be based on an indirect manoeuvre. Examples of such a manoeuvre are disrupting the enemy's rear by targeting his logistics and C2, and disorganising the enemy by reducing the tempo of his operation.

3. Time vs tempo: when deception is the most efficient

Whether in an offensive or defensive operation, the planning and decision-making process is not continuous. It alternates between phases of effort and phases of re-articulation or even restoration of combat potential. At the tactical level, these variations in tempo provide key moments favourable to employing deception.

A deception operation is above all an operative or tactical effect multiplier. As such, and in the same way as logistics, its tempo is different from the rest of the operation. The tempo effects must be combined with the effort of the manoeuvre. In order to produce these effects, the deception operation must be conducted prior to the action. Ideally, it is necessary to measure the first effects before launching the operation and to adapt the manoeuvre so as to best exploit the opportunities offered by a successful deception operation.

In addition to being integrated alternatively with kinetic operations, deception operations can be aimed at medium or even long-term operational objectives. Deception operations should therefore be considered on different time scales but always in advance of launching major actions.

The planning of a deception operation is therefore more in keeping with the J5 rhythm or even with influence operations.

As we have just seen, there are indeed non-concordant key moments for deception operations depending on the level envisaged (tactical, operative, strategic). For this reason, the operative level seems to be the most appropriate for coordinating the whole. The creation of a dedicated function integrating competencies such as Cyber, InfoOPS, J3 and J35 representatives could generate the necessary deception effects.

II. New perspectives for deception in future warfare (old wine, new wineries)

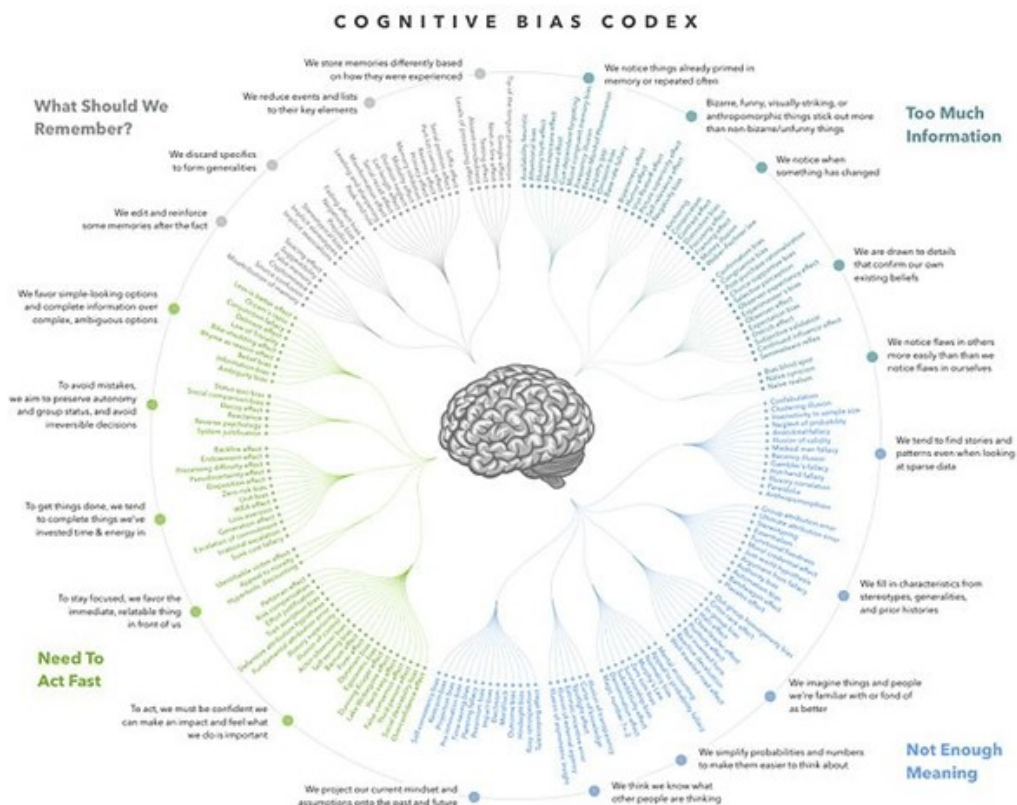
As we saw, deception is an effect-multiplier in modern warfare. More than just a passive means (hiding, SECOPS...) it can have direct action on the military decision-making process through various weaknesses we need to define. It may also influence changes in the way we manoeuvre.

A. Cognitive bias in HQ's decision-making process allows deception

On 6 October 1973, a coalition led by Egypt and Syria launched a surprise attack on territories occupied by Israel in what would be called the Yom Kippur War. The Egyptians in particular took advantage of one of their exercises near the border to intoxicate the Israeli military intelligence services and prepare their attack. The Israelis refused to take into account all the clues related to the impending attack, which brought them very close to total defeat before turning the situation around.

The Israeli military intelligence services had been the victims of a well-known cognitive bias, the *confirmation bias*: only information that confirms the initial assumptions and the dominant thesis are retained. At best, the divergences are considered negligible, at worst as results of errors or questionable elements.

All organizations are victims of cognitive bias, especially in the operating procedures of an organization – what armies call doctrine.



In the field of intelligence, cognitive biases are also expressed in the way one considers one's enemy. Several errors exist in this approach, the most well-known certainly being the *projection bias*. This is to project one's intentions and way of fighting on to the enemy to make it a double of oneself and to consider its capacity for initiative and reflection as null and void.

This projection bias also applies to the way materials are used in combat. While the battlefield has always been a place for resourceful DIY, conventional armaments are sometimes diverted from their conventional uses causing real surprises in battle. This illustrates the law: "Professionals are predictable, but the world is full of dangerous amateurs."

Sometimes simple hierarchical pressure is sufficient to create a climate conducive to setting up intellectual blinkers. So-called *compliance bias* – adopting the dominant thinking of one's organization – is all the more powerful as the chain tends to exclude non-aligned individuals.

While a doctrine is essential to combined and joint operations and allows a relative subsidiarity, it also makes our behaviour and intentions more readable for the enemy. He will no doubt use this knowledge to circumvent our effects and even intoxicate us relying on the cognitive biases evoked.

To guard against this risk, modern armies have set up "red teams". However, their use is often perverted into an "enhanced J2" when the objective should be to "think out of the box" and to question the leader.

The Russian and Chinese armies have clearly identified this doctrinal risk and propose complex doctrines that are incomprehensible to their public. The existence of varied cognitive biases, and the varying sensitivity of the Chief and his staff to them, is one of the most interesting keys in how they implement successful deception. The British army makes no mistake when it deploys permanent partnership teams to countries of interest. The knowledge gained should allow them to practice deception well in advance of conflicts and thus to exploit the flaws or trends observed in the partners' staffs.

B. Deception in MDB

The U.S. Army published functional concepts for the future 2020-2040, the Multi-domain Battle (MDB). The multi-domain battle is based on a simple but difficult idea of execution: inter-domain integration (land, air, sea, cyber and space) at the lowest levels and as soon as possible. The goal is to achieve an amplification of the desired effects. Its definition as concepts allows a more concrete understanding of this vision in organizational, doctrinal and technological terms.

In a contested, complex environment with increased lethality, and in which our operational superiority will be contested, ground forces will have to rely on a more agile C2. Operations will require extreme mobility to maintain freedom of action and to generate temporary bubbles of operational superiority. Soldiers and materials will have to be resilient under the increasingly harder blows of the enemy. The fight will **extend to** the field of perceptions. Interoperability with allies will allow the ability to create uncertainty and dilemmas in joint

operations. In an expeditionary context, a force will have to be tough to sustain lengthy operations, but will also need to be able to scale up its efforts to operate at the regional level.

Functional concepts aim to answer the following questions:

1/ How to decide quickly and better?

Decision-making capability relies upon two pillars: the best possible understanding of the environment, and the philosophy of "mission command" as a critical ability of commanding officers down to the lowest level.

The intelligence function aims at reducing the barriers (both horizontal and vertical) to ensure optimal information sharing. Horizontality corresponds to the trans-domain approach of multi-domain battle. Verticality is defined as the disconnection between the strategic, operational and tactical levels and of all these with the governmental level. From a strategic point of view, it is less about "winning the war" than about "winning the peace". This change in mentality is marked by the placing of the population as the centre of gravity of the theatre, but also by the desire to develop a certain subsidiarity in the "mission command": "The chiefs convey a clear intention and give the means for subordinates to take disciplined initiatives."

This resolutely subsidiarity-oriented approach to command with intent, coupled with fluid information sharing, will create uncertainty about tactical actions. An action of deception may be voluntary or involuntary intended at any level of command. The primacy of the human in decision-making and his appreciation of the spirit of orders with "variable geometry" generates an uncertainty that cannot be compensated by technology.

The declassifying information will also help to coordinate the effects of the disappointment of the tactical level at the strategic level and in the sphere of perceptions, without the need to make a plan *per se*.

2/ How to adopt a more agile manoeuvre?

The agility of the future manoeuvre (in perpetual motion, dispersed, with precise and massive fires, whose effects will converge) is based on complementary concepts gathered into the "cross-domain" manoeuvre. The combination by the Army of lethal or non-lethal capabilities in the five domains (land, air, sea, cyber, space) to place themselves in a position of superiority, presents multiple dilemmas to the adversary and offers strength, freedom of movement and action to friends.

The concept proposes combining decentralized linear and non-linear manoeuvres, in order to force the enemy to defend itself against multiple directions and domains. The tactical level envisaged to operate semi-independently is the Brigade Combat Team (BCT) and no longer the battalion. Coupled with deception and misinformation, dispersal is an effective tactic for the preparatory phases, as it maintains doubts among the enemy about the location of the main attack. Dispersal does not mean that renouncing the principle of concentration of effort. What is sought is an alternating manoeuvre dilations and contractions, combining dispersion,

infiltration and rapid concentration on the decisive points. To do this, armoured units will still play a major role.

The pace of operations must be sustained so that the adversary cannot keep up with it. Surprise is highlighted. The goal is to avoid a battle of attrition by obtaining the dislocation of the enemy.

The manoeuvre's concept describes some of the necessary capacities:

- hyper-mobile, rustic, light combat vehicles with efficient energy sources;
- an inter-domain "obscuration" capacity: avoiding detection by a form of "Evolved camouflage". This integrates conventional capacities, electromagnetic and cyber, which degrade the enemy's sensors or outnumber their ability to discern targets;
- increasing logistical autonomy;

These capabilities are enhanced by technological developments such as swarming and using AI to accelerate C2..

The fire-support function appears to be key. The American concept advocates a hyper-centralized command of fires across the theatre, encompassing all kind of means. It affects the strategic, operational and tactical levels, the joint forces, and is transversal in several operational functions (intelligence, fire support, influence, cyber, space, etc.).

The manoeuvre in MdB generates uncertainty and reconciles vulnerability in a visible space with surprise by proposing a dispersion of resources while allowing a concentration of effects. Deception is integrated "by-design" into the manoeuvre and can be the subject of initiatives at all levels to meet opportunities that arise.

C. Deception in Scorpion and non-linear warfare perspective

Without going back on the technological perspectives (info-valued combat) and organizational (new format of the BTG, integration of logistics, etc.) promised by the Scorpion program, it is necessary to look here at the manoeuvring perspectives it offers.

Scorpion should allow us to consider non-linear combat. Given the relative transparency of the battlefield, it seems risky to concentrate our forces during the "initial contact" phase. In the concept of non-linearity, this concentration of forces is replaced by a concentration of effects, notably thanks to remote fires and the info-valued use of vectors. Deception will aim to provoke the opponent to push himself to concentrate.



The split between a discovery and an assault echelon compensates for the loss of some of the contact intelligence with better dissemination of information collected at the lowest levels. The infiltration into the depth of this discovery echelon, taking advantage of gaps, will allow the concentration of effects by the fires envisaged previously.

A more fluid organization could also allow an irregular tempo and thus create a time-lag that will disrupt the enemy's decision-making. Surprise coupled with deception could also be achieved throughout manoeuvre, and not just in the initial phase.

Culturally, Western armies adopt axial manoeuvres with two objectives: maintain the coherence of their forces to concentrate them and so dislocate the coherence of the enemy. In a more transparent world, it will be complicated to scramble or blind the enemy. Thus, a less linear manoeuvre should be adopted, leading an offensive from multiple directions. Swarming is the beginning of this type of combat, quickly grouping units of different sizes and natures on a lens in three dimensions and by divergent pathways.

The decentralization of the means of command and communication and the tactical use of robots should generate surprise. At the tactical level, this non-linear dispersion, coupled with great autonomy, allows commanders to generate uncertainty, to vary the tempo, to take advantage of opportunities and thus to propose a form of permanent deception in the field.

The last line of thought allowed by this non-linear manoeuvre would be to incorporate into planning an "idea of manoeuvre of deception". The divisional level seems to be right for allocating sufficient resources to such a manoeuvre.

III. Creating uncertainty through cyber (old wine, new bottles, new delivery systems)

Intelligence and observation capabilities suggest that the battlefield will become increasingly transparent. The new templates being developed in many countries are already considering this, and include surprise and deception as key elements of their tactics. These new capabilities of observation, detection but also of concealment are based on an undeniable technological edge provided by the IC technologies that feed cyberspace (defined as the set of networked computers connected via the internet or not).

This technology, from which technologically advanced countries are taking their strength, is gradually becoming their new center of gravity. The main interest is its ability to save a considerable amount of time in data processing. Increasingly restrictive measures are implemented to protect this CoG and avoid exposure to attack. Nevertheless, attacks are still to be expected. The main issue regarding deception in cyberspace is precisely how to exploit these flaws in order to be able to conceal one's intentions. The purpose is not to hide (which could be particularly difficult) but to cause the enemy to waste as much time as possible before he can grasp the reality of what is happening. Cyber will maintain sufficient doubt and reinforce actions in the physical world.

A. AI and countering enemy deception

Developed nations are taking advantage from their technological advances to acquire an overall view of the area of operations. As a result, they are optimizing the technical capabilities of their networks. This in turn multiplies the effects of existing sensors. Jacques BLAMONT¹⁰ detailed this approach through "CYBERWAR" (which he opposes to NETWAR, to be discussed later). This use of digital technology aims at increasing the pace of decision-making through an ever-increasing interconnection between close-to battle-units and the staffs that command them. The gap in an enemy's speed of information processing is assumed to be capable of creating a lag in how fast they can produce orders, therefore giving a substantial edge to the "fastest minds" – which are ours.

The steady and exponential increase in data processing capabilities of servers suggests a comparable rise in computational and analysis capabilities in the years to come. This is particularly so in information management. While current computational systems are able to sort data and to reproduce simple actions, they are not yet able to process the resulting information in its entirety and with discrimination. The analysis and then the release of subsequent intelligence to the appropriate person are still left to humans. With the rise of artificial intelligence (machine learning and perhaps one day, deep learning), the information will be processed much faster, again diminishing the enemy's ability to conceal.

¹⁰ Blamont, *Introduction au siècle des menaces*.

The interconnection of networks should enable the quick detection of deception actions by highlighting inconsistencies in concealment and misinformation actions. They could enable the detection of enemy units and the understanding of their intentions by cross-referencing information from conventional sensors; the increase in computational capacity can detect inconsistencies among such information. The construction of fake news by big data analysis is the main advantage of networking many systems. In both cases, an increase in computing power will reduce the risk of being surprised and will consequently decrease the effect of the enemy deception. The other side of the coin is a continuous increase of data and a risk of rapid saturation of processing capabilities. Paradoxically, the increase in intelligence-gathering capabilities could lead to info-obesity. Any machine (let alone any operator) could not handle such a tremendous amount of data quickly enough to be exploitable at tactical or even at operational level.

Intelligence linked with cyber could take two complementary patterns: Cyber Threat Intelligence (CTI) and Cyber Intelligence (CI). The CTI aims at collecting and processing vast amounts of information on cyber defense; it does not necessarily come from cyberspace but will have an impact on the conduct of cyber operations. An example is the detection of new cyber actors (teams coming from cyber units, teams of cyber privateers or internet influence teams) who might have a marginal impact on waging an operation but could upset the cyber approach (protection of computer networks, adaptation of communication strategy).

The purpose of CI is very different. Its role is to detect pieces of information within cyberspace (usually open-source), process and cross-referenced, they will to improve tactical and operational situation awareness.

B. Deception in cyberspace, kingdom of the assailant

An operation in cyberspace cannot be improvised. Therefore an attack can only be built as a prepared action within the long-term planning process. A paradox the cyber planner has to face is the gap between the time needed for cyber infiltration and political life. The first tempo requires months if not years to be effective, while the political planning for a military intervention rarely exceeds six months (at most one year). Failing to have traditional or long-standing enemy, cyber planners have to think about attacking a very large array of targets in many countries based on the probability and nature of a future conflict. This point is very sensitive for democracies that have neither (officially) designated enemies. The Axis of evil¹¹ or the Iranian “Grand Satan” when speaking about the United States are exceptions and not the rule. It is also difficult for military planners to target large numbers of potential future enemies: in addition to a legitimacy issue, the ethical framework is also at stake when speaking about targeting civilian or dual targets. Despite its importance, cyber targeting will not be

¹¹ During the state of the Union speech, on January 29th, 2002, Georges W BUSH designated North Korea, Iran and Iraq as an Axis of Evil supporting terrorism, thus preparing the population to the military intervention of 2003.

discussed in this document which focuses more on how to deceive once the enemy has been designated.

As concealment of a cyber-attack is key to its success, it is essential to conceal its preparation for as long as possible. Several kinds of concealment actions can be integrated into deception operations at operational or even tactical level.

Cyber-attacks are regarded by NATO as acts of war that may trigger Chapter 5 of the Atlantic Alliance Treaty¹². Concealment of an adversary's actions has therefore been put to the fore. The main challenge in cyberspace remains the ability to attribute attacks with near certainty; it seems unthinkable to launch a war based upon highly probable but unproven allegations.

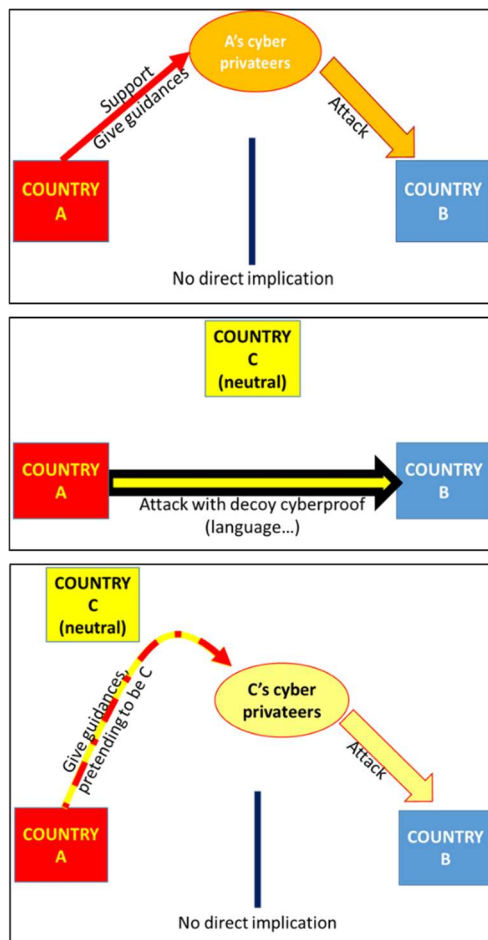
Deception in cyberspace could take many forms. To avoid attribution, an assailant may first seek to support teams of national volunteers (or pro-state factions) in their own territory or seek for support abroad to build the attack. These "cyber privateers" that fight for the cause of a foreign state but not visibly on its side protect the sponsor. The second kind will deliberately leave a computer "fingerprint" suggesting that the attack was perpetrated by another nation. This attack under a false banner is all the more difficult to detect since proving attribution requires several actions: first to define which state is suspected of being the attacker, then to find out who is the real sponsor. A third kind is a "proxy cover-up", where State A recruits cyber privateers in a State B while impersonating representatives of State B to carry out actions against the ultimate target, State C. Like a physical-world operation, the more discreet a cyberspace action is, the more effective it is. The protection offered by an attribution default provides sufficient time-lapses to conduct operations in other parts of the battlespace.

Western computer networks and intelligence assets are major if not the-main centers of gravity of modern armies, and are prime targets. It seems unlikely that a cyber-attack with a military purpose could permanently knock out an operational or even tactical-level command post. Nevertheless, a denial-of-service attack on institutional servers or an attack via the use of Advanced Persistent Threat¹³ could neutralize entire computer networks for several hours. The services will eventually be restored, but losing the initiative for several hours would allow the enemy to carry out vital physical actions. Meanwhile the targeted staff -- blind, deaf and dumb -- would be unable to react. Georgian government services were the subject of systematic attacks simultaneously with the combined Russian invasion of August 2008.¹⁴ Such actions and cyber preparations (similar to artillery preparations during the First World War) could divert attention to one field of operations, leaving an enemy free to conduct its main action.

¹² JENS STOLTENBERG, « NATO will defend itself ».

¹³ Malicious code triggering on orders that can be implanted voluntarily or by accident by a user.

¹⁴ Captain Paulo Shakarian, « The 2008 Russian Cyber-Campaign Against Georgia ».



Cyberspace can also offer concealment in itself, as Jacques BLAMONT explains¹⁵. The NETWAR he describes can be understood as the use of the internet as *common goods*. The use of civilian communications allows the perpetrator not to rely upon rigid hierarchical chains that are easily detectable. Not to mention the facilities offered by darknet, the use of mail, blog or even online gaming sites to communicate clandestinely.

Another use of a computer network is its ability to *simulate an activity*. The DONBAS conflict in 2014 highlighted the ability to pinpoint the location of individuals through their presence on social networks.¹⁶ While no Russian soldiers were officially deployed there, several geolocated photos in UKRAINE were released on the social networks VKONTAKTE and Instagram. Another kind of cyber location occurred in 2014. The FANCY BEAR malware allowed separatists to locate Ukrainian 2S30 batteries, allowing pre-emptory counter-battery firing¹⁷. In the near future, such locating is likely to be common. But it may also be possible to simulate such actions:

creating fake geolocations prior to the mission, "connecting" units to social networks in places where they are not deployed.

The increase in computing power will make fake information more and more convincing. Created images may not correspond at all to reality and may constitute first-class misinformation. These *deep fakes* already involve entire interviews, altering not only what is said live on-air but also who is saying it. It may soon be possible to lure the enemy on the location and identity of displayed units. *Spam dexing* (or BLACK HAT CEO) is another technique that can be implemented with greater computing capabilities. The action of numerous ghost accounts relegates messages, articles or unfavorable comments to the bottom of the search index.¹⁸ The more consulted pages are on the first page of the browser; relegating a link to the second page or lower drowns the information under other content.

Cyber-attacks will most of the time exploit software flaws and can only be a single-shot weapon: once known, the flaws are corrected. Furthermore, if the flaws are discovered and corrected (within, for instance, normal software updates), the entire prepared attack will not

¹⁵ Blamont, *Introduction au siècle des menaces*.

¹⁶ Myriam LEBRET, « Ukraine : les soldats russes trop bavards sur les réseaux sociaux »

¹⁷ CROWDSTRIKE GLOBAL INTELLIGENCE TEAM, « USE OF FANCY BEAR ANDROID MALWARE IN TRACKING OF UKRAINIAN FIELD ARTILLERY UNITS ».

¹⁸ Captain Paulo Shakarian, « The 2008 Russian Cyber-Campaign Against Georgia ».

be effective. It is therefore essential not to rely only on technically-based cyber-attacks. Cyber has to be regarded as a combat support tool. The success of an operation, even one centred on a deception, one cannot rely upon the success of a single actor.

C. Cyber-deception actions: wasting time

New technology will ensure that at the end of the day, a deception action will be detected. The whole point of deception in cyberspace is not to get the enemy to change tactics but to slow down their decision-making. This creates a gap and classic deception actions can then resume, making the opponent hesitate even longer. Cyber may be regarded as a classic amplifier of deception actions.

The main outcome of cyberspace attacks is the wasted time (and therefore money). As Thomas Rid pointed out¹⁹, services will be restored after an attack targeting servers; similarly, a fake news will have its veracity disputed and then invalidated. However, the time to deal with these difficulties creates difficulties and uncertainty. In military operations this doubt restores the fog of war -- once dissipated by ISR capabilities -- by altering the situation-assessment within headquarters and slowing the decision-making process. The effect of concealment and intoxication actions will be reinforced by the waste of time due to remaining doubt about the very veracity of each information received.

In addition, once one warring party has used a modified image, the other side will be compelled to devote time to checking each of the following images. This false information, that can be created a long time before the operation, could be disseminated at the very beginning of an offensive (along with the artillery preparation mentioned above) and could saturate the processing capabilities and consequently, the targeted command-and-control capabilities. In addition to having doubts about the enemy's intentions, the targeted force will then have to deal with this new and plausible information -- while also having to deny the messages propagated by the opposing actions.

IV. Influence (adapting the label, storing the bottles)

"Facts are the great enemy of truth", Cervantes in *Don Quixote*

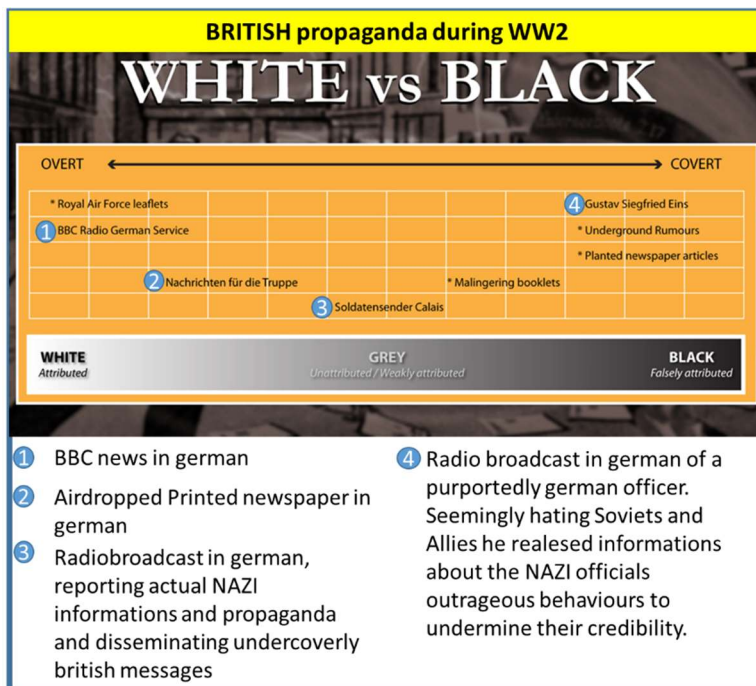
The quest to exercise effective influence is constant in military art. Without mentioning the GALLIC WARS (a self-serving rewrite by Julius Caesar of his campaign), all sides have an interest in presenting themselves as the camp of good. And the opponent will systematically be portrayed as less civilized and fighting for an unjust cause. The message conveyed by military and political authorities will therefore have a major impact on the way operations will be waged. Absolute truth does not objectively exist in communication; the art of influence will be either to present the truth in an directed way or to deliberately lie. Democracies seem to

¹⁹ Rid, *Cyber War Will Not Take Place*. Rid,

be at a disadvantage: the imperative of truth both structures them and seems to be a disadvantageous constraint.

However, solutions exist to disseminate the desired informations and focusing on the perspective one wants to stress. While the deception action permitted by influence may have little impact on tactical operations, its intoxication action will play a very important place at operational level, raising doubts about the intentions of stakeholders.

A. Influence as a way to reduce effectiveness in military operations



Influence actions can take up the common classification of propaganda actions described by François Bernard HUYGHES²⁰. Propaganda is structured into three types of actions: white, grey and black. All of them can carry out relevant actions in terms of military deception.

White propaganda encompasses all official discourses. Facts will systematically be real. Instead of seeking to influence the opposite side, it aims to protect the effectiveness of an operation, emphasizing the benefits for the population. It plays a key role

against misinformation or, as a bottom line, at countering the actions of adverse influence. It is consequently oriented toward *deceiving the enemy*. White propaganda supports the image of the military operation and removes doubts that may remain not only about the enemy's course of action but also about public opinion (local and domestic). The action is not focused on the military. Nevertheless, its impact on the outcome of a campaign is decisive. Allowing the enemy's denigration and intoxication will undermine their legitimacy and morale. Furthermore, white propaganda seeks to bolster an already well-established idea. This functions by recalling the economic and social progress permitted by the presence of the military force and by scanning in detail past operations.

Grey propaganda by contrast does not respond to an official discourse. The media spreading it present themselves as fully independent, yet are most of the time guided from abroad with editorial lines clearly defined by the sponsoring country. Notwithstanding the fact that the information released might systematically be true and the facts they put to the fore may not

²⁰ Huyghe, *La désinformation*.

be attacked, the angle from which the idea is presented is systematically biased. The main purpose is to *guide opinion*. Using altered images or images taken out of their original context (reworking the frame, colours, reuse of old images, etc) can provoke and intoxicate the population, thus forcing the target to change his attitude in dealing with the crisis (regarding the use of force, for instance).

Last but not least, there is *lying outrageously to create doubt*. This **black propaganda** will usually mask its sources. By spreading deliberately false messages it aims to undermine morale or cause indignation, even if temporary. During the fighting in DEBALTSEVE in 2015,²¹ Ukrainian soldiers received numerous text messages urging them to surrender and explaining that the city was surrounded or that the ceasefire was not being respected. This decoy action even when carried out on ordinary enemy soldiers, can have a decisive impact on the probable success of an operation. François Bernard HUYGHES sums up this idea: "If the fake holds up until the victory, the revelation of the tricks does not matter"²².

B. Democracies: tempting targets.

Freedom of speech is a touchstone of western societies. It entails also a systematic doubt about any proposal. Western media try to adopt a critical position on disseminated information so as not to be accused of bias. It is precisely this strength that can become a weakness. The whole point of influence actions will be to turn the population against an operation, undermining its legitimacy while allowing simulation actions to be carried out.

It is possible to fool the most official and independent media. The use of local freelancers (cheaper than actual journalists) is widespread. These "journalists of fortune" can be easily influenced or given prepared arguments or images. The proliferation of continuous news channels and the rivalry between them also create a follow-the-leader effect. Once published an information is almost immediately taken up before being verified. The more spectacular or surprising an image is, the more effective it will be, at least initially. The possibilities of manipulation are endless, from disinformation to the full spectrum of simulation actions. These communications can then be picked up and amplified by social networks. The means of relaying information online are developing, from the multiplication of BOT networks to the creation of dedicated teams on social networks. All these actions aim at generating doubt. Shallow fakes are a good example. These coarse lies²³ are sufficiently elaborated to initially look credible and to create a "reasonable doubt" which then has to be combated. We all believe in images (let alone the videos), and it takes a substantial effort not only to realize the deception but also to erase the idea propagated in the message.

Freedom of speech means that for the sake of impartiality, all opinions may be presented, including the most heterodox or subversive. Newspapers will provide an equal forum for proponents and opponents of an argument. Disinformation actions are all the more

²¹ Myriam LEBRET, 'Des soldats ukrainiens ont reçu un SMS qui prouve que la paix est encore loin« ».

²² Huyghe, *La désinformation*.

²³ KARIN VON HIPPEL & JONATHAN EYAL, « When Misinformation reigns ».

achievable as civilians in Western countries experience widespread skepticism (or even paranoia) about official information. The messages do not even need to target the entire population (abuses, however simulated, will inevitably attract the attention of human rights advocates). Once the target (or part of it) has been convinced of the idea, it will relay the information as possibly true to its like-minded relations. Step by step, this information will acquire a widening audience, becoming all the more difficult to tackle. This 'sleeper' effect is reinforced not only by various cognitive biases but also by the algorithms of social networks that will create a phenomenon of information self-validation. The purpose of these messages is not properly speaking military, it has no kinetic effect, but it has implications for the conduct of operations. Any emotion that is provoked could force a military leader to modify his manoeuvre or, at a minimum, will force the staffs to justify their actions in terms of communication. The purpose of these actions is not to conceal units but to create rumour and increase doubt in the minds of the enemy population and ultimately among their military.

C. Democracies must be able to use these weapons

The generalization of doubt in democracies does not mean that they are condemned only to suffer the actions of influence and narrative spun by adversaries. They can equally invest these fields actively for the vast opportunities they offer for military deception.

The first step will be to defend against the actions of the enemy. This comes mainly from protecting one's own credibility. It will be necessary not to lie, at any price, and to communicate only real facts. If necessary, one must clarify actions taken and review those which have caused criticism. Agreeing to recognize collateral losses (even if this means having to revise them upwards) is undoubtedly temporarily damaging; however, it will prove profitable in the long run. Recognizing proven changes of situation makes it possible to be more readable in acute crises. An organization known for its transparency is more likely to be listened to.

However, defense should not be built solely on alleged facts (where, as we have seen, doubt will inevitably arise once the idea has been set). If a re-information action is essential to restore the truth, it is all the more important when counterattacking the enemy's communications, their contradictions and questionable actions. The targets could be also those principles that distance the opponent from the targeted population. The aim is not only to discredit them immediately but also their future messages. Eventually, the goal is to reduce the impact of the enemy's future attacks by reducing his credibility now.

It is also important not to leave the initiative to an opponent but to lead deception and influence operations. The challenge for our message is never to be seen as propaganda. While it is essential not to lie, it is not mandatory to clarify the whole truth. Showing an image or footage without context and letting the enemy come to its own conclusions is not a lie. During the first Gulf War, the U.S. military released several images of fighter jets in Saudi Arabia.²⁴ The

²⁴ Macdonald, *Propaganda and Information Warfare in the Twenty-First Century Altered Images and Deception Operations*.

facts were indisputable: aircraft were displayed. Yet no logistics units or combat service support appeared on images. The communication was accurate in so far that the planes were there - but they were not combat ready. Halfway between a decoy and demonstration, this action allowed the opponent to reach his own conclusions, guided by the U.S.

More broadly, we must seek to bolster shared values among our forces and the targeted population. If the adversary is not going to be presented as the source of all evil, force must be seen as the only possible way to peace. Fear can be used with positive effect. Without stressing that the enemy is responsible for the suffering (easily refutable), one can play on the distress of the people and show how the use of force could end it. These messages will be all the more credible if they are disseminated in the vernacular and by locals. In general, the broadcasted messages should never look like propaganda (or they risk being quickly rejected). Simple messages must be included in a broader media landscape that emphasizes what culturally brings the force closer to the rest of the targeted population. Once again, the interest of such an action is to preserve credibility and ensure that it can effectively tackle the future intoxication actions of the adversary.

V. Conclusion: to go further

"In the conduct of operations, (...) it is recommended to use cunning and subterfuge of all kinds, if only to sow uncertainty in the spirit of the enemy command, to make him hold back, to hesitate (...)." ²⁵

Deception is an old concept. It is inherent to the art of war. Although its principles appear to be permanent, the implementation of its processes requires adapting to the evolving forms of conflictuality, integrating contemporary technological and organizational developments and extending deception to the new places of war.

The panorama and analysis proposed by this study is intended to demonstrate the relevance of deception, which has become even more so in the so-called "transparent battlefield" of the modern, IT-led ISR environment.

What does this mean?

Current technological and organisational conditions, and the complexity of the operating environment marked by a wide spectrum of forms of warfare, should push us to integrate deception in our operational planning and to establish a principle of surprise in all our operations. Even so, the modalities of its implementation within a force will remain problematic when every resource is being counted.

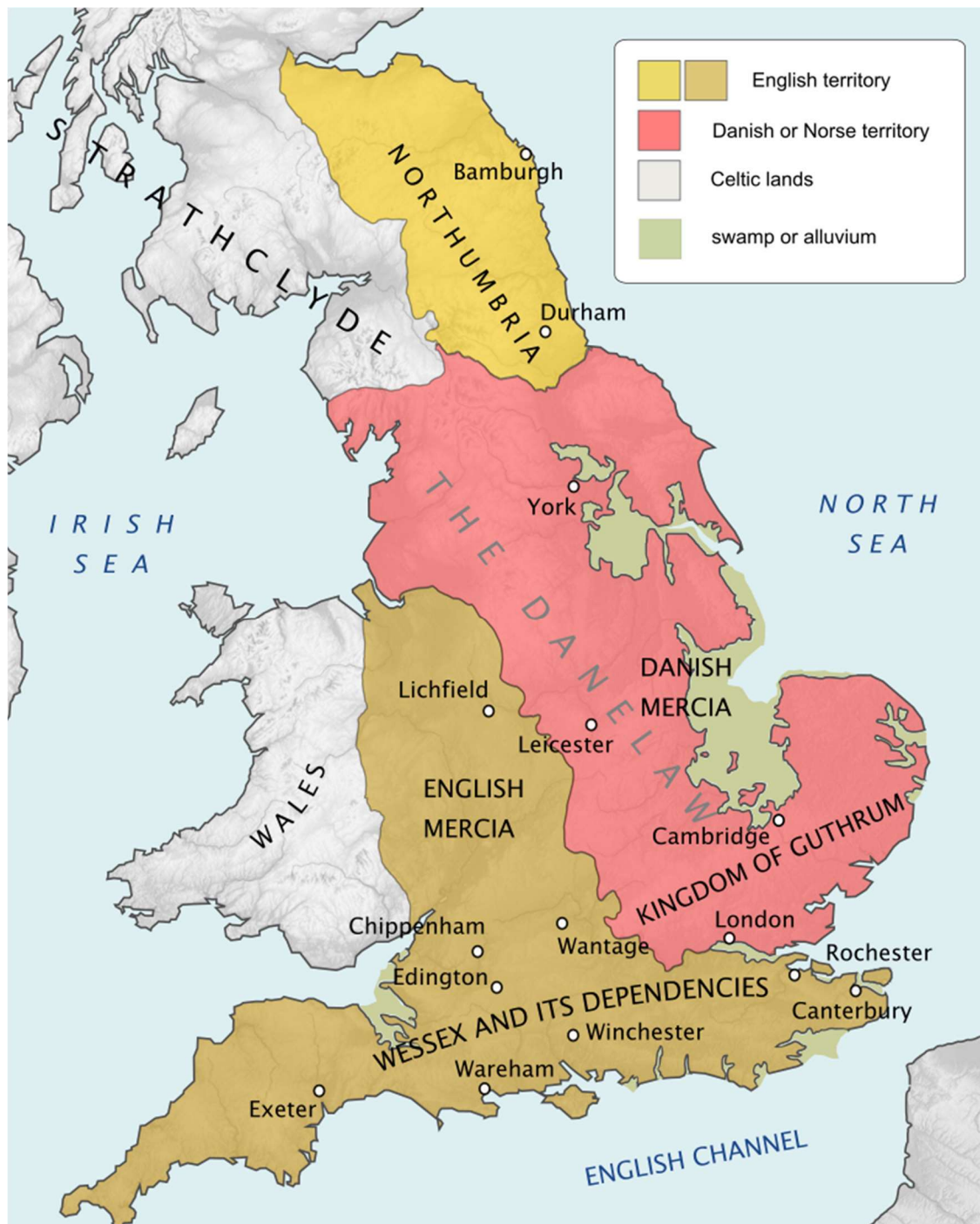
The operations of deception and the articulation of effects in the different fields necessarily have an influence on the tempo of operations. They can also deter the enemy before the engagement. In order to lead the way, we present a possible course of action with the scenario in the Appendix.

²⁵ Field Marshal Erwin Rommel, *Rules of War in the Desert*.

VI. Appendix 1: Scenario OLD THREAT, NEW MEANS

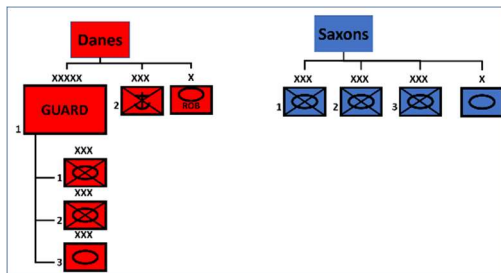
During the 9th century, in the central part of what will one day become England, the Danes were trying to establish their rule over the rich Saxon kingdoms of the south. In 861, the Danes succeeded in luring the king of Wessex, Æthelberht by fooling him about the direction of advance of their army. Being deceived, the Saxon king focused his war effort elsewhere, leaving its capital WINCHESTER open to the Nordic army.

How could we reproduce such a prowess with modern technologies?



DANELAW (an authoritarian country allied to NORTHUMBRIA) decides to invade the **Saxon** Mercia (democratic country allied to WESSEX, with Chippenham as their common capital) the day after the presidential elections. The other countries are neutral. **Danes** and **Saxons** have been hereditary enemies for decades. They fought three wars during the last century. The last one saw the victory of the **Saxons** and their annexation of the LICHFELD industrial area to **Mercia**. So there is no mystery about the will of the **Danes** to avenge the latest defeat. This outcome will depend on general disruption around the presidential election, itself influenced by a military campaign that hinges on a full range of deception actions.

"J" is the day following the **Saxon** presidential elections and the beginning of the **Danish** offensive.



The **Danish** armed forces are made up from 1st Army of the Guard (two mechanized and one armored divisions), the 2nd Rifle Amphibious Division (RAD), and a full Robotic Brigade. The **Saxon** army has around three mechanized divisions in the south of the country and an infantry brigade in the vicinity of LICHFIELD. The two countries have effectively the same level of technology and the

confrontation can be regarded as symmetric. Contrary to the Saxons, **DANELAW** conducts actions of disappointment. **Saxons** have strong ISR means.

PREPARATION

J-500:

- **Danish** cyber recognitions on government and institutional websites are launched to detect software vulnerabilities; a specific malware is developed. Then infiltration is carried out on targeted networks (fishing campaign - purchase of flaws on the darknet - voluntary or involuntary introduction of malware via a USB stick).
- On the stock exchange, the **Saxon's** GPS supplier is bought by a holding company secretly owned by Danish oligarchs (resident in Denmark).
- The **Danish** cyber command designs a malware (or buying on the shelf) to lure GPS.
- A campaign to discredit the **Saxon** political class is launched in **Saxon** media financed by **Danish** funds.

J-300:

- All targeted computer networks are infected with the malware, but no cyber-attack is launched: a cyber "recognition" is conducted. This aims to neutralize a small part of the network, causing little consequences, to check the effectiveness of the infection.
- The malware designed for GPS is progressively deployed, via an official software update, throughout the **Saxon** army.
- On **Saxon** social networks, the most virulent ideas from political opponents are put to the fore (these groups are silently supported by the **Danes**).
- The number of web pages touting the action of the **Danish** authorities for the benefit of developing countries is increasing as fast as those highlighting the growing debt and mismanagement of the **Wessex** national budget.

- The most rational pages begin to disappear and only appear on the 2nd and then 3rd page of most browsers, due to the action of **Danish** cyberprivateers.
- In the vicinity of York, the first BESERKER exercise unfolds. This Northumbrian/**Danish** exercise gathers for an entire month the most modern units of the two armies, air force and navies, including the **Danish** 1st Army of the Guard and the Robotic Brigade.

J-150:

- The denigration campaign against the **Saxon** political class carries on.
- STRATHCLYDE (Scotland) media released images of **Danish** soldiers committing abuses during a humanitarian operation in Wales. The footages triggered a political and popular outcry in **Saxon** MERCIA.
- The **Danish** air force made several overflights of the **Saxon** border. These "Accidental" infringements occurred near LICHFIELD, WANTAGE AND CANTERBURY.
- Another BESERKER exercise took place in the DURHAM area. This time a wide media coverage is made on the **Danish** side. The event is broadcast as factual among the **Saxons**.

J-120:

- **Danish** air incursions are more and more numerous, especially in the mouth of the River Thames.
- Having fueled heated debates about the legitimacy of the army and the government's ability to conduct a military operation ethically, the images broadcast at J-150 proved to be fake. However, **Saxon** critics continue to question the official thesis, finding a "surprisingly" effective echo on social networks.
- Claiming for equality of treatment with the **Saxon**, **Danish** minorities demonstrate in ROCHESTER, calling for a higher degree of autonomy.

J-15:

- The third BESERKER exercise began in the WHITBY region allowing a strong media presence. Several interviews of the main **Danish** generals are made. They all clearly show the insignia of the 1st Army of the Guard. The footages show detachments of corresponding units, allowing observers to distinguish the markings of specific units on some vehicles. Inflatable decoy units capable of returning appropriate thermal signatures are secretly deployed during the exercise and are moved regularly. These movements are coordinated with the vertical passage of the **Danish** observation satellites so that at each pass, the vehicles move; **Saxon** observers regard those units as real.
- The mobile phones of the entire Guard are confiscated
- While being theoretically engaged in the BESERKER exercise, the 1st army of the Guard gathers in the utmost secrecy (night travel, radio silence, GPS off) near LEICESTER.
- A large number of phones belonging to soldiers of the 1st Army are activated in the vicinity of WHITBY and broadcast on social networks. These display real photos of exercise BESERKER 3, as well as others dating back from BESERKER 1 to increase the number of units.

- A large-scale exercise involving naval forces and amphibious units take place off the coast of COLCHESTER. Decoy and inflatable units simulate the presence of the 2nd RAD. Similar concealment and technical ruses as deployed by the 1st Army of the Guard are implemented.
- Meanwhile, the bulk of the 2nd RAD rallies in the Bedford Region.
- Numerous highly visible decoys appear in the regions of MANCHESTER, DERBY, LEICESTER (effort), BEDFORD, NORTHAMPTON and LONDON. These elements are detected by the Saxons and regarded as preparing an action. The Saxon army's level of readiness is increased.
- Some modern decoys are carried out along the entire Danish border. A particular effort is put on the northern shores of the River THAMES.
- The Saxons misinterpret this decoy concentration as real.
- On Saxon media criticism is raging against the ineptitude of government policies.
- Shallow fake videos featuring pseudo-Saxon soldiers abusing Welsh civilians appear on the internet. This ignites controversy over the behaviour of the armies. The Saxon Ministry of Defence introduces much stricter ROE.
- Facing the purportedly absence of consideration, the separatists in ROCHESTER launch violent riots. the Danish government calls on the Saxon government to protect minorities.

J-5

- The interview of the general commanding the 1st Army of the Guard, live from YORK, is widely broadcast among the Danish media and is seen as factual among the Saxons.
- The boarding of some units belonging to the 2nd RAD is filmed by the media in COLCHESTER.
- The Danes maintain continued but discreet support to opponents of the political class in the Saxon media.

ELECTION DAY AND AFTER

J-1, Election Day

- Social unrest continues in COLCHESTER.
- The Danes move (empty) ships from COLCHESTER to the southern shores of the THAMES .
- The Saxons detect concentrations of troops near LEICESTER. However, the Danish influence strategy in Saxon MERCA has reinforced the bias established within the staff there of an imminent Danish intervention at COLCHESTER. Despite the initial reluctance of the Saxon red team in the face of the obvious, it did/does not dare to contradict their CHOD (known for its assertive character) when it felt that Colchester could only be a diversion. For him, the Danes would only be going to support minorities there.
- Elections bring to power an anti-system opponent with no real experience, with an aim to unbalance the Saxon political class.
- Large-scale troubles occurred as soon as the results are announced, Saxon security forces are widely deployed; the military are on high alert and some units are marching to the capital CHIPPENHAM to support the overwhelmed security forces.
- The 1st Army of the Guard and the 2nd RAD commanders discreetly come back at the command of their respective units.

J, H-12

- **Danish** naval artillery shells Saxon positions near COLCHESTER to simulate support for the separatists.
- The cyber-attack is launched. All institutional computer networks are affected by denial-of-service attacks and by deletion of official websites. Saxon MERCIA is cut off, unable to use its computer and telephone networks for the next 24 hours.
- The **Saxon** army moves a mechanized brigade from the 1st DIV to the region of COLCHESTER to face the **Danish** fleet.

H-6:

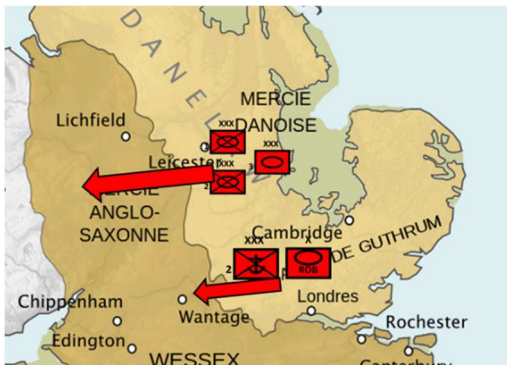
- The deliberately limited offensive of the 2nd RAD is made possible by the reinforcement of the autonomous Robotic Brigade on the axis BEDFORD- WANTAGE. These attacks suggest a **Danish** main effort towards the Saxon capital CHIPPENHAM.
- Without political order, **Saxon** armed forces are limited to basic defensive reaction. Their HQ remain focused on the formerly received orders: support the security forces in the capital and defend COLCHESTER.

H:

- The offensive of the 2nd RAD has progressed 20km and the **Saxons** are moving the two remaining brigades of the 1st **Saxon** division to tackle their advance.
- **Saxon** observation satellites are illuminated by the **Danes**, and their space ISR is no longer available.
- The virus introduced into **Saxon** GPS gives false positions, provoking friendly artillery fire on Saxon positions. At the same time, the communication clocks are staggered, making any tactical communication impossible using frequency hopping: all radio communications are over a fixed frequency and are easily intercepted by the Danes.
- Thanks to the location of **Saxon** gunners' cell phones, Danish counterbattery fire destroys the **Saxon** field artillery at WANTAGE.

H+4:

- **Danish** observers detect the commitment of the 3rd Saxon mechanized division to protect the capital. To reinforce this belief the **Danes** launch a carpet dropping of leaflets that urge the population of the **Saxon** capital to stop fighting and open the city.
-



- The first echelon of the 1st Army of the Guard cross the border and advance westward, leaving doubts about its effort aims: attacking the capital to the South or the industrial regions to the North? Two divisions at the front and the last on in second echelon.

- An air interdiction campaign directly supports the attack, blinding the Saxons.

- As soon as the border is crossed, an APT is released on the Saxon military servers; their computer system can run

for the next 6 hours (time to reconfigure them). Without specific orders, Saxon troops continue their effort against the 2nd RAD.

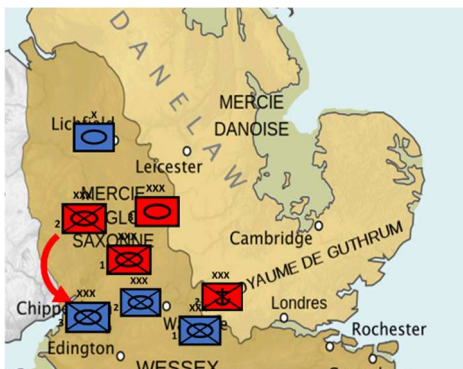
H+6:

- The 2nd RAD is fixed, the Robotic Brigade discreetly retreats to Danish territory and comes to fit into the device of the 1st Army of the Guard.
- The 1st Army of the Guard continues its advance westward.

H+10:

- The 1st Army has advanced 100 km from the border without any serious resistance. The effort of the Saxons is still not based on a proper analysis of the whole situation.
- With the computer systems finally restored, the 2nd Saxon division receives orders to stop the advance of the 1st Army of the Guard. Saxon forces encounter the southern flank of the Danish army and fix an entire division.
- Without frequency hopping, the locations of Saxon HQs are quickly located and destroyed by Danish artillery.

H+12:



- Supported by the Robotic Brigade, the northern division of the 1st Army of the Guard launch an envelopment attack, changing direction and advancing towards the capital. The Saxons, considering a coordinated attack with the 2nd RAD order their last division, that had been held back to defend the capital, to hastily counterattack. The envelopment attack is tackled, the Danes (and the Saxons) are fixed.

H+14:

- The **Danish** 2nd echelon scorpionnized division, adopts a non-linear attack. Based on information, the force identifies the location of the command structures and regiments of the LICHFELD brigade. Considering its slightly favorable balance of strength, it refuses to engage in a linear manner and employs her discovery detachment to go destroy the PC of the LICHFELD brigade. The latter is then no longer able to regroup its forces which will be fixed simultaneously by the dispersed assault echelon of the 3rd **Danish** division.

END STATE

D+3:

- The LICHFIELD industrial area is seized. The **DANISH** units stop their advance and the front freezes on the initial axis of progression of the 1st Army of the Guard.
- The three **Saxon** divisions have been fixed, the brigade to the north is tactically neutralized (without having suffered a significant attrition). The **Danes** are in a strong position to call for the LICHFELD industrial area to be re-attached to DANELAW.