Cyber and Military Action in the Air and in Space

Didier TISSEYRE

| Général de brigade aérienne, Deputy chief of cyber defence.

Globalisation and the digital transformation of society have led to the creation of a space in which almost all human activity can be seen: cyber space. Its characteristics offer great chances—economic, scientific and cultural in particular—since they increase trade, in turn favouring progress and the creation of wealth. And yet precisely because it potentially reaches all who connect to it and all deployed systems, it is also a world that attracts envy, and is favourable to crime, espionage, influence, sabotage and destabilisation. It is therefore an environment of conflict, which means that security and defence are at stake.

Interactions between cyber space and the other spaces (ie land, maritime, air and space) are many and on several levels. Cyber is therefore a transverse space, able to reach all the others. Like the ground and maritime spaces, air and space are highly computerised, thus contributing to the efficiency of military action in those environments. That computerisation then itself becomes a new source of vulnerability. Are we then condemned to suffer, when faced with sure risks and proven threats (*Winter is coming*, as in *Game of Thrones*!), just hoping that our defences hold out? Is there not a strategy for better management of these risks and for countering these threats? Could we not turn these vulnerabilities to our advantage to preserve our freedom of action and independence, and to contest those of our adversaries?

To counter the risks that stem from cyber space and which could limit military action in the air and in space we need on one hand for our systems to have genuine, operational cyber defence that relies upon a permanent cyber defence posture, and on the other to have the capability to plan and conduct defensive and offensive military operations in cyber space, both in external theatres of operation and in the defence of the forces' digitised systems. And though seeming a contradiction in this environment of hyper-technology, it is the intrinsic qualities of the human being, when set to work within the framework of that new technology, that will drive our response to the challenges posed.

To back up these analyses and proposals let us look at the characteristics of cyber space and the vulnerabilities induced into military action in the air and in space, then at the capabilities we have to develop for our defence and to enable us to conduct operations in cyber space.

Benefits of digitisation and dangers of cyber-space

Mass digitisation of information, the exponential development of calculating power, the interconnection of networks and the falling cost of the associated technologies have led to the transformation of all human activity. Computerisation of processes optimises activities and new uses see the light of day, freeing us from traditional prescriptive, regulatory frameworks. States, administrations and historical players in certain sectors are therefore disappearing, to be replaced by direct relationships between users and suppliers of services. Digitisation increases opportunities and contributes to the development of progress. Internet is the symbolic example of this worldwide web, connected by cable or waves, and plugged into by numerous private and public networks. Initially limited to information and communication systems, digitisation has been broadly extended to remote control of automated systems through Supervisory Control And Data Acquisition (SCADA) and, in the field of defence, to command and control (C2) systems and hence to almost all weapon systems.

Worldwide interconnection of digitised systems has created a completely artificial cyber 'space' in which everyone can potentially interact with everything. In view of the profound transformation of society that accompanies its deployment, we could say that it amounts to the digitisation of physical spaces (land, sea, air and space) in a rather philosophical, conceptual sense. It is a higher-level space since it penetrates all the others and can act in them. In another universe we might argue that it is a space, like Tolkein's ring, to rule and control everyone. Although sometimes seen as a single entity, cyber space is far from homogeneous and is often described as three layers on top of each other—physical, logical and semantic (or cognitive, or social). The first is made of computer materials and components and the networks that link them, which could be cables, fibre-optics or electromagnetic waves. The second is the collection of digital data, its handling processes and flows of data being exchanged, which are activated in the physical layer. The third layer brings together that which is exchanged in cyber space between humans—ideas and sentiments for example—in particular via avatars (digital identities) set up by users. These three layers are interdependent and any action on one of them could have consequences on the others. It is possible to hide a user's real identity and traces in order to remain anonymous and/or furtive.

Our companies and administrative bodies make massive use of cyber space in support of their activities and are becoming dependent on it. At the same time its boundaries and structure continue to evolve. Other than its physical aspects it has no real limits, geographical characteristics or political or legal boundaries that would connect it to states and thereby define notions of territoriality or sovereignty. Because states are in essence absent from cyber space it is difficult for them to play any stabilising role. The real influence, on both economic and social levels, comes from the major companies associated with the digital world, such as the GAFAM,(1) BATX(2) and NATU(3) groups. Others are revolutionising entire areas of activity: Elon Musk, for

(1) Google, Amazon, Facebook, Apple and Microsoft.
(2) Baidu, Alibaba, Tencent and Xiaomi.
(3) Netflix, Airbnb, Tesla and Uber.

example, with New Space and SpaceX. Clearly it is no longer states that are initiating or supporting the development of technologies, among which those essential to aerospace activities, nor are they controlling their availability: that all now lies in the hands of private interests.

On Internet everyone, whatever his motivation, can potentially transmit information or software almost instantaneously to a great mass of addressees or in a more targeted fashion. Tools exist to protect against malware but few, if any, protect against broadcasting of false information—fake news—aimed at manipulating opinion.

Vulnerabilities impacting military action in air and space

A major constraint on cyber space is the frequent need for updating of hardware and software owing to their rapid obsolescence. Because of the reliance on open architectures, mechanisms need to be added to ensure confidentiality, availability, integrity and the traceability of data and its handling. The complexity of development and parametering of the hardware and software associated with those mechanisms means that vulnerabilities can be discovered, which once in the public domain lead to distribution of corrective patches that are not always installed as quickly as they should be. Therein lie opportunities for the attackers, some of whom even set traps in those patches in order to infect the machines. Indeed, some manufacturers are accused of deliberate infection of the material or software that they sell, to the advantage of the state to which they belong—the debates over Kaspersky and Huawei being examples.

The worst scenarios see attacks on the digital systems of civil or military vehicles in flight (aircraft, helicopters, drones and missiles, for example) or of spacecraft (satellites and rockets). With no need to have anyone on board it is possible for pirates to take over control remotely to make the vehicles crash, collide in flight or be used as flying projectiles as in the terrorist attacks of 11 September 2001. In other scenarios there is some form of intrusion into an air traffic control system to disrupt it by masking, adding or moving tracks. Up to now the few successful attacks that have been made public concern flight reservations systems or handling of customers' accounts and their only impact has been financial or on company image.

Because of interoperability and interdependency, risks to civil activity inevitably weigh on military activity too. Everything that is connected to or within the aircraft physically or by radio, or even asynchronously by a removable device, could be used as an entry channel for a cyber attack. New generation systems for air traffic management in the context of single European or American skies are based on satellite links and interconnection of systems that assemble information relating to the aircraft and its environment and are therefore a greater source of cyber vulnerability. Robustness and resilience in the face of an attack on a system are major challenges for all public and private organisations, such as airlines, airports, air forces and the missile, launching and satellite sectors.

Cyber attacks affect military action in the air and in space even more so: on one hand the Air Force's missions of defence of airspace and surveillance of exo-atmospheric

space, and on the other, defence of its own air and space capabilities. It is therefore essential to analyse these risks and threats very well, especially to evaluate their possible impact on our systems since these are now 'systems of systems' that rely on complex architectures. They integrate many constituent digital elements, airborne or on the ground, including data links and various sensors. The C4ISTAR (Command, Control, Communications, Computers, Intelligence, Surveillance, Target Acquisition) concept well illustrates the operational gain afforded by the digital technology that allows these functions to be brought together, something unimaginable back in the days of manual and analogue information handling. Tactical data links are another major advance for the coordination of combat and optimum allocation of targets. For France, these advances are being implemented in collaborative or connected combat, part of the major Future combat air system project (FCAS, *Système de combat aérien du futur*—SCAF), which brings together sixth generation aircraft and a wide range of interconnected and interoperable elements such as drones. And yet this very interconnection facilitates penetration by an attacker. The same goes for the entire range of satellite systems used by military bodies (for observation, listening, communications and positioning and navigation, for example), all of whose components and functions are potentially vulnerable to attack even via their ground segments. Their cyber security is a major issue since today there is no military operation that does not requires the support of space assets.

Cyber-defence operations and military action in air and space

Whilst cyber 'weapons' hardly revolutionise the principles of war, by the same concentration of effort and economy in use of assets they open up new perspectives for states and armed groups through their unconventional and hybrid use alongside traditional weapons and action. The Internet allows anyone to overcome issues of time, distance and borders to destabilise a state by targeted or wider broadcasting of information or transmission of malware. Globalisation, which offers easier access to high technology, and the dependence of Western society on information technology lead to counter effects in cyber space. The use of cyber space adds to the difficulty states have in creating an appropriate response in an environment in which the boundaries between peace, crisis and war are less clear than they once were. There is no internationally recognised definition that clarifies whether a cyber attack can be considered 'armed aggression', which would entitle legitimate defence under the terms of Article 51 of the UN Charter, or collective defence under NATO's Article 5. Cyber attacks and strategies of influence on social networks therefore bring a level of asymmetry that profoundly modifies the framework of international relationships.

Quite apart from the technical impact, proliferation of threats, the variety of modes of action—often furtive and difficult to attribute to an originator, and the multitude of possible targets, the ability of cyber attacks to produce worldwide effects from limited resources lead to serious operational challenges. They involve the freedom of action of armed forces and national sovereignty. Our adversaries are in a position to put credible attack strategies into effect against our forces and defence industry. Organisational measures and local protection techniques are no longer sufficient and

need to be complemented by a form of overall reactive and dynamic cyber defence that forms part of a permanent cyber defence posture. It would be structured on an operational chain of command with specialised human and technical assets. We must anticipate adverse modes of action, detect and define them, assess their likely impact and react in order to preserve as best we can our operational advantage. It is a cycle comparable with that of air defence, though adapted to cyber space. Since a cyber attack could be wide ranging and arrive via indirect channels, it is essential that all players share the same operational picture so they can respond collectively to crises.

Within the Ministry for the armed forces the Cyber defence command (*Comcyber*) is responsible for conducting operations in the Defensive information battle (*Lutte informatique defensive*—LID) according to a policy of end-to-end coordination based on a principle of subsidiarity. Each major body in the Ministry—forces, directorates and services, for example—establishes LID arrangements within its area of responsibility, overseen by a technical and operational structure, one of a number of Security Operations Centres (SOC). The LID analysis centre (CALID) a sub-unit of *Comcyber*, ensures wide-ranging technical oversight and assembles and shares information on the cyber pictures produced by all the SOCs or by its own assets. *Comcyber* is at the head of the LID chain and has an operations centre which directs the work of the CALID and the SOCs to ensure broad operational oversight. Comcyber receives complementary information from national and international cyber security, cyber defence and intelligence partners, and is party to the cyber threat state and to newly-discovered vulnerabilities so it can ensure best effectiveness of the chain.

Actions in cyber space should now be considered as genuine operations, and their design and conduct need to follow the same types of process as traditional military operations. They draw on C2 assets to ensure coherence and effectiveness of manoeuvres. Whilst they can be conducted independently following their own objectives, the advantages of cyber operations are often greater when they are combined with traditional operations such as assisting an in-depth air attack by masking it from radars more discretely than would be the case with jamming.

Offensive operations can also allow paralysis of the adversary to avoid or limit combat. This possibility is well illustrated by the theory well known in aviation circles of the American John A. Warden, who describes the enemy as a system of five rings.(4) The rings—fielded military, population, infrastructure, system essentials and leadership—can be attacked individually or collectively through cyber space. Additionally, through the use of influence operations on social networks, the population ring becomes the target of choice for acting indirectly against the leadership ring.

France considers that the military Offensive information battle (*Lutte information offensive*—LIO) broadens the palette of military options. It can be combined with or take the place of other military capabilities and contributes to acquiring and

(4) WARDEN John, *Air Theory for the 21st century*, in SCHNEIDER Barry R. and GRINTER Lawrence E., *Battlefield of the Future, 21st Century Warfare Issues*, Air War College, Studies in National Security n° 3, p. 103-124 (www.airuniversity.af.edu/Portals/10/CSDS/Books/battlefield_future2.pdf).

retaining military superiority in the defence of our interests and preservation of our sovereignty. Its peculiarities generate constraints for its use, however. Its use must be controlled and involves political, legal and military risks. As with any weapon of war, LIO is subject to the principles and rules of international law, particularly humanitarian law regarding proportionality, distinction and discrimination, as well as to national laws and regulations. It is therefore only used in cases where the rules of engagement (ROE) are very restrictive, and any risk of compromise, abuse, collateral damage or fratricide must be avoided.

The development of military cyber defence advances hand-in-hand with new skills that are specific to cyber matters such as threat analysis or *Threat Intel*, a strategy for detection of attacks on IT, cyber patrolling and hunting on networks, digital forensic investigation, reverse engineering of codes, management of cyber crises, mass data analysis, the laws of armed conflict and those controlling the digital world. A cyber combatant is neither a specialist in IT, nor in communications nor intelligence nor even a social engineer or a pure 'soldier'. He is a combination of all of these, which means ever more focused training that is continuous, modular and alternating in partnership with the civilian academic and industrial world to ensure improved competence appropriate to the profession. Yet in addition to the knowledge required, there needs to be a mentality particular to work in cyber space. This means a preference for those born in the digital world—digital natives, as it were—with the minds of hackers (ethical ones, of course!) and a strong ability for self-learning, able to 'play' with their computers in order to meet the challenges with passion. Indeed, some among the self-taught are the best performers. Recruitment and retention of qualified personnel are essential to the performance of military cyber defence.

⁂

The air and space, like other environments, benefit from what digitisation brings them, but they suffer equally from the vulnerabilities associated with the cyber environment. To control the major risks and counter the known threats it is essential to have a highly operational approach to cyber space and to establish a permanent cyber defence posture to defend our weapon and information systems. We also need to know how to seize the opportunities offered by cyber space within a strictly controlled framework in order to conduct offensive operations. Such operations might be conducted alone or combined with other forms of action since they bring a significant operational advantage to both strategic and tactical levels, which mean that balances of forces can be reversed and the adversary paralysed. The human remains very much at the centre of such an organisation because his capacity for adaptation, his reactivity and diversity of thought, together with his sense of commitment make the difference when facing up to the rapid developments now taking place in cyber space. ◆