the cyber, a new space of conflict

National Defence and Armed Forces Committee

Général de division aérienne Didier Tisseyre

Published on 08/05/2020

Sciences & technologies

Thank you very much for inviting me to speak about cyberspace, this area of conflict, and to discuss its issues with you, particularly for the defence of our country. In my opening remarks, I propose three parts, which I will illustrate with a number of examples. The first part will lead me to talk about this conflictuality associated with cyberspace and what characterizes it. I will then explain how this conflictuality affects security and defence issues. Finally, I will deal more specifically with the command of cyber defence: its dynamics, its action, its responsibilities.

Conflictuality in cyberspace is linked to the digital, which is everywhere, in all human activities, and which supports all professions - whether private or public - and individuals. At the base, of course, the aim is to create progress, to connect people, to facilitate these activities. These technical mechanisms that make it possible to link one another - and in quantity: one person to a multitude - to contract space and time in the transmission of information and to share a huge number of elements are an opportunity but also a risk. Some have clearly identified this risk and the value of personal data, for example, which some may be too carelessly put on the Internet. They have seen that they can benefit from these links between individuals, from everything that can pass through cyberspace. Cyberspace attracts all kinds of lust, all kinds of cybercrime. This of course facilitates espionage, and then by widening, influence, sabotage and destabilization... These words have existed for a very long time, but they take on a whole new dimension because of the very characteristics of cyberspace.

It is important to understand that cyberspace is totally man-made. Compared to air, land, sea and even space, it is the only one that has been built by man, and it is constantly evolving. This evolution makes it difficult to identify its contours, both present and future. Initially, it is rather based on technical governance, in which States are not necessarily present. Today, however, the question arises as to the presence of States and all the operators that can be found there. Cyberspace is thus like other spaces, other media: a

field for the expression of rivalries between States, between groups, between companies, and a field of action for a certain number of criminals. All those who wish to use it for their own benefit to impose their will take advantage of the difficulties and fragilities in terms of organization and technology, but also sometimes of the lack of knowledge on the part of its users. As you can see, such conflicts present security and defence challenges.

I will take two examples. In the summer of 2019, within a structured framework, the Pentagon in the United States asked a number of hackers -hackers in the rather sympathetic sense of "hacker "-totest systems and their security. Within 48 hours, these hackers managed to get their hands on the digital systems deployed in an F-15 aircraft. You can see what this can do to operations using these very modern means equipped with deadly weapons... Even on very expensive equipment.Even on very sophisticated, highly advanced hardware - even if the F-15 is not the latest generation of fighter aircraft - there are vulnerabilities. These weapons systems were designed ten or even twenty years ago, at a time when cyber defence was not the main focus of attention.I'm more concerned than I am today, and there was not yet the knowledge of the vulnerabilities associated with cyberspace. There is a catching-up to be done, and it is sometimes complicated.

Another rather emblematic example of what can be done in terms of offensive actions in cyberspace is the famous Stuxnet virus, which was used a number of years ago to slow down the deployment and operation of centrifuges in Iran. One can imagine that in order to reach these centrifuges - in fact the computer systems that control them - it took a great deal of intelligence, knowledge and ingenuity to get this software to work over long distances. Extremely careful coordination and planning of the operation made it possible for it to have a real effect in slowing down a country's capabilities.

We can see that any balance of power must incorporate this notion of cybersecurity, of cyberaction: those who do not do so at a disadvantage compared with those who do and who do not apply the same ethical rules as we do. We must therefore anticipate these risks and be resilient in order to protect everything that is essential in the national territory. This is the will of the Ministry of the Armed Forces.

I could take other examples from the army or the navy but, as an aviator, I am obviously very sensitive to the deployment of air power and air fire. The appearance of the air force was, in good French, a game changer, which gave us a capacity to act beyond enemy lines, a capacity to strike logistics, to acquire information, to obtain intelligence, to better calibrate artillery fire. Yes, whoever had those capabilities had an advantage over the others. In all joint operations, the acquisition of air superiority, whether continuous or ad hoc, is an indispensable prerequisite. The one without air superiority will be in a much more difficult situation and will have to deal with the adversary's intelligence, deep strike or front-line capability.

There is a clear link with this new capability related to digital and cyber defence: whoever masters cyberspace will have an advantage, not only to protect himself, but also to ensure his operational superiority. This is what the Ministry of the Armed Forces is doing in our theatres of operations, in the Levant, in the Sahel. Our cyber defence capabilities are the result of years of work and are being used to preserve our capabilities and our highly digitized weapons systems. They enable collaborative combat, real-time information

exchange, and thus combined, nested, integrated but also highly efficient operations.They also enable us to block the adversary, in particular - this is what was done against Daech - from its propaganda and the preparation of its operations against our forces deployed on operations.

These mechanisms of military strategy and their application have a long history. According to the Chinese strategist Sun Tzu, "the best skill is not to win a hundred victories in a hundred battles, but rather to defeat the enemy without fighting. With cyber and systemic attacks, some people imagine bringing down an entire system. Let's take the example of the American F-15s, potentially vulnerable to attack: if you prevent them from taking off, you necessarily have a significant advantage and, in the end, even before you've triggered them, you've won the battles, you've won the war.

Today, another strategist, American this time and from the 20th century, John A. Warden III, sees institutions, structures and the enemy as a system of many circles. He described these circles. You obviously have the military forces deployed for protection and action; you have the populations; you have the infrastructures that are important today - like medical, energy, in addition to roads, ports, airports - and which are targeted by some; in the fourth circle, there are essential organic functions - energy production, fuel supply, food supply; and in the last circle, the functions of command, state, regalian, governance and very senior management. In the conflict between armies and between states, one always finds the application of these principles to whether one is going to target deployed military forces or directly the place where decisions are made, to paralyse or prevent those decisions. In the 20th century, one or the other of these circles was targeted. With the cyber, you can target the totality and take a combined action against the armed forces, the populations, the critical infrastructure of the country, but also against decision-making systems. This dual action is also exerted on the populations: on their daily lives, on all their information systems, but also on their positioning, through social networks. It is therefore a real existential risk that weighs on our societies, faced with those who know how to use cyberspace to block our systems and impose their will.

The impacts can be very strong. Today, actions in cyberspace are divided into several issues. First, who can attack us? A state? A group potentially attached to a state, but not necessarily officially or in uniform? Its individuals? Second, what techniques, tactics and procedures are being used? Let's make a comparison with burglars: they have their tricks, their strategy. Some will go through rooftops, some through windows, some through doors. Cyber attackers also have their own strategies. These strategies are characteristic of a number of groups, and it is important to be familiar with them in order to know how to react, whether to protect roofs, basements or windows. In cyberspace, you have to protect everything, you have to be able to defend everything, because all you need is for the attacker to find a way into your system. With the answers to "who's attacking us" and "how", the question of impact and effects then arises. These effects are of three types. It can be a hindrance effect, a disruption in the functioning of a system: I was talking about a plane being prevented from taking off. But you can also block a power plant to destabilize and impede the enemy's manoeuvre. The second possible action is to capture data; because we're doing economic espionage, we recover the other person's order of battle so that we can pre-position ourselves. The third purpose is to change the perception of the other, to lure him or her and influence his or her vision. These are the three objectives targeted by cyber attacks.

In our operations, we integrate these three dimensions. We also pay particular attention to our information and systems. We are trying - and for the time being we are succeeding - to ensure the confidentiality of this data, which is essential to our manoeuvring and our business, but also its integrity. I mentioned the risk of modification: their integrity is essential. And, as we sometimes tend to forget, we make sure that the data is available. The integrity of the processing is also essential. For the cyberdefender, these are elements that must be integrated and for which security mechanisms must be deployed.

We can have the impression that the attacker does whatever he wants, that we are powerless against him. There is, however, a framework, which is becoming more and more precise. International law applies to cyberspace. However, it is difficult to know the precise modalities of its application. Do states or groups recognize these principles? How do they apply them? Do they feel concerned and committed to these principles? At one time, a reference manual - the Tallinn manual - was produced by a multinational working group to explain how to understand these notions of cyberspace. Now, two working groups are considering this within the UN framework, one chaired by the Americans and the other by the Russians. At the national level, on the initiative of the Ministry of the Armed Forces, a report on the application of international law to cyber operations describes the mechanisms by which France perceives cyber attacks on its territory against its systems. Who is attacking us? How can we react? What are the principles of self-defence, the principles of digital sovereignty - it is very detailed - but also the principles applicable to cyber operations in theatres of operations: what is their framework? How are they regulated? What are the principles of proportionality, availability and discrimination?

When we talk about cyber operations, we can imagine Tom Cruise parachuting with a laptop computer that allows him to communicate directly and trigger a lot of things to fulfil his "mission impossible". In reality, at the risk of disappointing you, a cyber operation is prepared well in advance. Its effects can be immediate: all you need to do is to trigger what has been pre-positioned to have an immediate and far-reaching effect. But to achieve this effect, it must be prepared well in advance. You have to have a very precise knowledge of the target's IT infrastructure to identify how to reach it. You have to pre-position your equipment to carry out the action you want to carry out: the planning and intelligence phases are therefore very important.

A distinction is sometimes made between times of peace, crisis and war. I can assure you that in cyberspace - I think you know this - we are not in a time of peace: there are many crises, and in some ways cyber warfare has already begun. Some people are deploying their tools and pre-positioning themselves so that on D-Day, when they press the "Enter" key, they canimmediately trigger the elements. But once you're paralyzed, it's too late to react.

Within the Ministry of the Armed Forces, how is the cyber defence command, which I have had the honour of commanding since last September and of which I had previously been number two for two years, positioned? Created in 2017, this entity is in fact the result of ten years of build-up, which takes us back to 2007 and the cyber attack on Estonia by a neighbour who wanted to react to the removal of a statue. This event marked an international awareness: if someone has cyber capabilities and wants to use them, it can have a very strong impact on a state. Many countries became concerned about these

cyber threats and developed elements of defence.

There is a political will to achieve and develop the capability that we have today within the ministry and that the commander of cyber defence has. The means allocated by the Military Programming Law have made it possible to commit the budgets and human resources needed to develop these capabilities.

Specific doctrine documents - including elements that have been made public on doctrine, on offensive cyber warfare operations for military purposes - have also set the framework and objectives for our action. The missions of the Cyber Defence Command are therefore the protection and defence of the capabilities of the Ministry of the Armed Forces, and also include possibilities for action in cyberspace in theatres of operation. I am the operational controller of all operations in cyberspace: defensive operations for the benefit of the Ministry of the Armed Forces and offensive operations for the benefit of the nation, depending on the political choices that are made. In the chain of responsibility, the President of the Republic, as head of the armed forces, decides on cyber action in the same way as he decides on military action.

We are in the continuity of the field. For example, we have carried out coalition offensive actions against Daech in theatres of operations, just as actions have been carried out in a more traditional manner with these same coalitions, to reduce the size and scope of Daech's actions. In cyberspace, we targeted their entire propaganda apparatus, identified where the servers were located, penetrated those servers, erased data, and blocked those servers so that propaganda could no longer be disseminated. All of this was carried out as part of a more global approach to identifying terrorist content with the support of the Ministry's Pharos platform (Platform for harmonizing, analyzing, cross-checking and directing alerts).s Ministry of the Interior - the administrative authority for Internet operators - to derefer a certain number of terrorist propaganda contents.

We are facing technological challenges, as you can imagine, but also challenges in terms of capturing innovation. In a rapidly changing cyber space, we need to be able to capture this innovation with rapid procedures and processes. We are doing this in particular through a Cyber Defence Factory in Rennes. Above all, we need to meet the challenge of human resources. Cyber fighters are not only people with five years of higher education in computer science - you need them, of course - but also technicians, people with a very analytical, geopolitical mind, to understand this cyberspace. They are also psychologists and sociologists to understand this cognitive layer: I mentioned social networks earlier, which is obviously essential. In fact, the best team of cyber-fighters is a mixed, versatile, obviously feminized team. This too is essential: we have a 15% feminisation rate in the COMCYBER, which is noteworthy in a very technical field. We also rely heavily on operational reservists.

I will conclude by saying that the human element is fundamental. One gets the impression that cyberspace is just technology, but in fact it is the human being, through his involvement, through regular training throughout his contract and his career, who makes it possible to respond in this very evolving field.

Title : Général de division aérienne Didier Tisseyre

Author (s) : Général de division aérienne Didier Tisseyre

Release date 08/05/2020

FIND OUT MORE