Towards a cybernetic deterrent?

military-Earth thinking notebook

Chef d'escadron PRETEUX

Published on 21/10/2018

Sciences & technologies

At a time when artificial intelligence, big data and connected objects are giving the exchange of information an unprecedented scale in the history of humanity, the virtual world has taken on considerable importance, particularly for armies. The power of cyber means is such that many journalists and observers in the military world wonder about the parallel that could be drawn between nuclear deterrence and cyber deterrence.

The creation, but above all the expansion and use of the Internet have radically changed the life, habits and customs, and methods of reflection of societies. They are considerably changing the relationship to knowledge and information of each citizen. The Internet has therefore become a privileged vector, an "effector", no longer potential but unavoidable, for anyone wishing to achieve a particular objective. Beyond the Internet, it is in fact the whole of what can be called the cybernetic sphere (see Box) that has become a major challenge for States. The description of the cyberthreat, which first appeared in the 2008 White Paper on Defence and National Security and was taken up and reinforced in the 2013 White Paper, clearly shows that this new space is being taken into account. The LBDSN of 2013 places cyber attacks in third place in order of importance (after aggression against national territory and terrorist attacks), while the Americans, for their part, place them in first place, even before terrorist attacks. Cyberspace is described as the "fourth dimension", after land, air and sea. Even more recently, in his speech on the occasion of the visit to the Directorate General for Armaments and Information Management, the Minister for Defence, Mr. Klaus Kolchak, said that the United States was the first country in the world to have taken the first steps in the fight against terrorism, even before terrorist attacks.fense Minister Jean-Yves Le Drian advocates increasing the resources, both human and financial and material, allocated to the control of this new space. Thus described and considered, the cyber domain could only be supported by a strong and ambitious policy, in order to enable France to hold its place in it as much as in the physical world. To achieve this, it has chosen three complementary lines of action:

- effective intelligence, which is the first of all missions and which contributes to the successful completion of all subsequent missions;
- a robust defensive posture, capable of protecting not only the Ministry of Defence's cybernetic infrastructures and systems, but also, in conjunction with the ANSSI, all structures of strategic interest;
- a range of offensive capabilities, from Internet intelligence to destructive capabilities, which France reserves the right to use at any time by decision of the President of the Republic.

This complementarity between a defensive scheme and a full spectrum of perfectly mastered capabilities is not unlike the physical world and the broad spectrum of its capabilities. Thus, we shall see that even if it is tempting to push the analogy further and imagine a cybernetic deterrent that would make it possible to achieve, by other means, the preAs the Minister of Defence pointed out in his speech, the semantic field of deterrence must remain limited to nuclear weapons.

First of all, it is therefore necessary to ask what deterrence is all about.

Dissuade: To make someone renounce his intention to do something (Larousse).

Diplomatically, deterrence consists of preventing an actor from taking action against the state (its territory, its vital interests) by persuading it that its action will have an unacceptable cost, far greater than any gains it might receive[1].

1] The elements that constitute nuclear deterrence can be seen here.

First of all, deterrence is based on the willingness of the actors to prevent any action from taking place. In order to do so, therefore, these actors must be identified. The possessors of nuclear capabilities are known, whether they are known legitimately or in fact. But they are generally known or at least suspected [2]. The ability to attribute an attack is therefore indispensable for deterrence in order to be able to target the possible response.

Finally, deterrence, as noted above, is based on unacceptable costs that far outweigh the gains. This implies the credibility of possible retaliatory actions. The credibility of nuclear weapons is based in particular on history (Hiroshima, Nagasaki) and on the nuclear tests carried out by certain countries. Everyone knows what a nuclear bomb can do. The loss of (very) many human lives, the destruction of any structure for miles around, the perennial irradiation of the "fallout" up to 25 km awayare all unacceptable consequences, at least at the present time.

French cyber capabilities

France has the full spectrum of cybernetic capabilities, both in terms of offensive and defensive actions. Actions in cyberspace have been defined as being of four types: defensive actions, offensive actions, counter-narrative actions and intelligence.

Defensive actions consist of putting in place the necessary means (physical, software and human) to prevent at best and limit at worst any type of attack on French strategic points of interest and, in particular, on the Ministry of Defence's networks. The possible attacks are of very varied types and can be committed by a wide variety of actors. From young

geeks who "hack" for fun to attacks by organised states, via "hacktivists" and large-scale banditry, the multiple forms that these attacks can take make it necessary to maintain a constant technological watch as well as tools dedicated to this work. CALID[3], within the Ministry of Defence, co-located with ANSSI[4], brings together about a hundred experts in the field whose mission is to ensure this protection.

Offensive actions consist in striking, in different ways, a particular point in order to obtain the desired effect. These actions can take several forms, phishing , spamming, DOS[5], worms, viruses, Trojan horses. They can be destructive or not, targeted or not. France is able to implement all of these capabilities if necessary.

Counter-narrative actions: a particular aspect has emerged from the expansion of the Internet over the last ten years, which is the importance of social networks. They have become a powerful vector for propaganda, information and disinformation, but also for planning and publicising illegal actions. The purpose of counter-narrative actions is to monitor social networks, to identify suspicious and/or potentially dangerous content and to act on them either by tracking down the various players or by carrying out counter-propaganda and information actions. This particular area of cyberspace overlaps with the social layer of cyberspace mentioned above, and its scope is growing.

Finally, intelligence, as in the physical field, is a priority, since one can only act well when one is properly informed. France's cyber-intelligence resources are defined by the Military Programming Act and make it possible to gather the necessary intelligence, in particular by exploiting open sources and Big Data.

Exclusion of a cyber deterrent

In view of these capabilities, it would indeed be tempting to draw a parallel between the physical and cyber worlds, particularly with regard to deterrence. Journalist Eric Mettout does not hesitate to draw this parallel in his article "Russia - United States: the cyber-war has begun" in the newspaper L'Express in December 2016.

However, while the analogy is interesting, cybernetic deterrence is not technically feasible at present. Indeed, for it to be effective, a possible cyber deterrent would have to be credible and display a particularly high destructive power. France does indeed have destructive offensive capabilities whose consequences could prove unacceptable (destruction or control of energy networks, for example). But what is missing for this credibility is a "Cybernetic Hiroshima" that would make it possible (beyond the films we have seen) to realize the disastrous consequences that such an action could have. The applications would however be multiple:

- taking control of a country's energy flows (especially electricity);
- cutting off all communication networks;
- cutting off a cooling system leading to an explosion;
- shutting down data centres in financial centres, resetting all global financial data to zero.

However, the non-directly lethal but highly demonstrative aspect of these capabilities makes such actions acceptable. Current events, both recent and ancient, are full of examples of more or less destructive direct or indirect actions. From the STUXNET worm, responsible for a twenty-year delay (according to experts) for the Iranians in their nuclear programme, to the suspicions of Russian interference in the 2016 American elections, cybernetic actions are a type of strategic action in their own right. Until recently, the ability

of an attack to directly target a state was demonstrated by the Botnet Mirai 14 [6], which saturated the single internet entry point of an entire state, Liberia. If the consequences of this attack were minimal due to the low density of population connected to the Internet, the strategic capabilities of a cyber attack are obvious here!

Moreover, one of the principles of deterrence is to know who you are dealing with. This attribution of the first potential attack is therefore necessary to be able to talk about cyber deterrence. However, attributing a cyber attack with certainty is something that is rather poorly controlled. There are many clues that allow suspicions to be raised about active groups, and only in-depth speculation, but never proven, can analysts imagine the responsibility of a state entity. An official response, in the framework of a dissuasive programme, then becomes unthinkable because it is difficult to justify in the light of the law of war and the morals commonly accepted in the world diplomatic game.

Finally, and moving away from technical and feasibility considerations, deterrence must retain its strictly nuclear character. Indeed, when one of the international actors establishes a policy of cyber deterrence, the diplomatic game would imply an escalation of means, and many States could thus equip themselves with a "cyber deterrent", since the means to be implemented would certainly be complicated, but much more affordable than a nuclear deterrent, from both the technical and financial points of view. It would also greatly upset the balance of power and change the relationship between states. The permanent members of the United Nations Security Council have in common that they are the official masters of the nuclear deterrent game. Countries that have wanted to join this very closed "club" of nuclear powers have done so at great expense, as this type of programme is exorbitant, both in terms of research and implementation. By contrast, an advanced cyber defence programme requires much less investment.

This relative accessibility to a possible cyber deterrent also stems from the great difference between the physical and virtual worlds in terms of standards, control and, from a more philosophical point of view, morality. While the physical world has many treaties, laws, regulations and conventions that can regulate nuclear weapons proliferation more or less effectively, the cyber world does not. In this regard, the Minister of Defence considered that international law applied to the cyber world[7]. [7] Yet the cyber world is considered by most protagonists to be virgin, neutral and free territory, making it very difficult to control. Thus, it is estimated that the Internet as we know it, the web, represents only 5% of the total Internet, with the deepweb and the darkwebsharing the remaining 95%. In these two "territories", no state law has a hold, which allows the different groups to flourish and launch their targeted actions. Thus, a coherent cyber deterrent can never be achieved as long as the Internet as a whole, or at least the vast majority of it, is not regulated by states.

However, the unacceptability of a cyber action could be accepted in the case of a takeover of a nuclear reactor or an opposing nuclear arsenal. This could argue in favour of a cyber deterrent. But the problem must be seen in a different light. The French nuclear deterrent had three components, land, air and sea, reduced to the two air and sea components in the 1990s. It might then be interesting to consider a third component, this time cybernetic, capable of attacking and taking control of nuclear infrastructures around the world. This would not be a cybernetic deterrent, but still a nuclear deterrent, implemented by its cybernetic component only towards those entities with access to the atom.

Thus, even if it is necessary never to underestimate the destructive or harmful capabilities of the cyber capabilities of active small groups or nation states, at present the semantic field of deterrence must remain restricted to nuclear strike forces. For, first of all, the

technological means of a possible cyber deterrent are not yet ready (attribution, demonstration of effects), and secondly, and above all, there is a risk that this would call into question and redesign the forces and interactions between international actors and make the global diplomatic game even more complex, thus upsetting the already fragile balance between these actors. However, it is essential to continue to think and reflect on the notion of cyber deterrence as a possibility in order to prepare for any eventuality.

1] Wikipedia article on French nuclear deterrence. https://fr. m.wikipedia.org/wiki/Dissuasion_nucléaire

https://fr.m.wikipedia.org/wiki/Force_de_dissuasion_nucléaire_française

2] Article "Nuclear weapons in the world" by Damien Hypolite du Figaro, 12 April 2010.

http://www.lefigaro.fr/international/2010/04/12/01003-20100412ARTFIG00537-les-armes-nucleaires-dans-le-monde-.php

[3] Defensive Computer Warfare Analysis Center.

4] National Agency for Information Systems Security.

[5] Deny of service. A denial of service attack consists in sending a very large number of requests to a server in order to saturate it and thus neutralize it for a certain period of time.

6] Article "A Botnet Mirai brings Internet access in Liberia to its knees" by the editorial staff of the zdnet.fr website.

http://www.zdnet.fr/actualites/un-botnet-mirai-met-a-genoux-l-acces-internet-au-liberia-39844240.html

7] Speech by the Minister of Defence on the occasion of the visit to the DGA/MI on 12 December 2016.

http://www.defense.gouv.fr/ministre/prises-de-parole-du-ministre/prises-de-parole-de-m.-jean-yves-le-drian/cyberdefense-discours-de-jean-yves-le-drian-lundi-12-decembre-2016

Saint-cyrien of the promotion "General Vambremeersch" (2001-2004), Squadron Leader PRETEUX first served in the train weapon within the 121st regiment du train as a platoon leader, in the medical regiment as a unit commander and then in the logistics brigade before joining the War School in 2015. Passionate about new technologies and in particular those related to information systems, he is currently studying for a specialized master's degree at École Centrale Paris.

Title : Chef d'escadron PRETEUX

Author (s) : Chef d'escadron PRETEUX

Release date 12/02/2021