Can digital capabilities contribute to deterrence?

military-Earth thinking notebook

Chef de bataillon Frédéric GERLINGER

Published on 26/10/2018

Sciences & technologies

The increasing number of attacks in cyberspace in recent years, particularly involving major powers, raises questions about the role that digital capabilities could play in future in deterrence. The aim of this article is to briefly recall the foundations of nuclear deterrence, to study the potential of digital technology in the field of deterrence, before analysing whether digital capabilities could play a role in the future.It is possible to envisage the implementation of cyber-deterrence in the face of cyber-attacks or, more generally, possibly as a complement to nuclear deterrence.

The development of digital technology is creating new opportunities for the United States today. Indeed, the relative anonymity of cyberspace actors is a major obstacle to the development of digital technology.[1] once again makes it possible to envisage offensive operations while limiting the risk of reprisals. This paradigm shift could thus be compared to that which occurred with the appearance of nuclear weapons in the early days of the cold war. Initially envisaged for offensive operations, nuclear weapons gradually emerged as a deterrent tool, making it possible to avoid direct conflicts between the nuclear powers and to limit peripheral confrontations not in number but in intensity. The increase in recent years of attacks in cyberspace, involving precisely these major powers, raises questions about the role that digital capabilities could play in deterrence in the future. Some states have announced the development of cyber defence capabilities to strengthen their deterrence. This is the case in particular of the United Kingdom, which considers the Internet to be an integral part of the "battlefield" and, as such, has demanded, through the intermediary of the United Kingdom, that the Internet be used as a tool of deterrence.diary of its Minister of Defence in 2011 for the creation of a cyber deterrent force capable of protecting the country's strategic installations against terrorist attacks.[2]. In France, the armed forces have also taken the measure of future challenges by recently creating a cyber operations command and developing synergies with the civilian sector. At the same time, the Ministry of Defence must carry out a massive recruitment of "digital combatants" to reach a strength of 2,600 in 2019, to which will be added 600 specialists from the DGA.[3] and 4,400 reservists[4] of cyber defense. However,

the French Minister of Defence, Jean-Yves Le Drian, declared on 12 December 2016[5]I do not see how, indeed, the cyber weapon would have the very specific restraint or deterrent effect that we see and maintain with nuclear deterrence. And the way nuclear deterrence works is profoundly different from cyber battles. That is why I am more inclined, in our modes of reasoning, to link cyber issues to conventional ones".

The objective of this article is to briefly recall the foundations of nuclear deterrence, to study the potential of digital technology in the field of deterrence, before analysing the role of digital technology in the field of deterrence.It is possible to envisage the implementation of cyber-deterrence in the face of cyber-attacks or, more generally, possibly as a complement to nuclear deterrence.

What is deterrence? What is it based on?

It seems necessary first of all to return to the definition of deterrence before studying its fundamentals. In the specific case of France, the Joint Centre for Operational Doctrines and Lessons Learned recalls that "deterrence is exercised for the defence of the interests of the people and the environment".France's vital interests by threatening to provoke, through the use of all or part of its nuclear weapons, damage of any kind, out of proportion to the interests at stake and, as a result, unacceptable to any adversary wishing to harm them". [6]. Two different forms of deterrence can thus be distinguished: either by prohibition, by putting in place all possible measures to prevent and convince an adversary that it will not be able to achieve its objectives, or by retaliation through the threat of nuclear capabilities to an adversary seeking to harm the vital interests of the nation.

Deterrence, therefore, depends first and foremost on credible military capabilities. As such, deterrence requires concrete elements that aim to persuade a potential aggressor that it will with certainty receive a nuclear response in the event of an attack. Nuclear capabilities thus have a twofold requirement: they must be visible and conspicuous through tests (nuclear or not), training or exercises. [7] (in France this is one of the roles of the strategic air forces), and be discreet to ensure the permanence of the nuclear threat (this is in particular the role of the strategic oceanic force). But the credibility of this deterrent also depends on the expression of political will through clear signals, in particular the coherence of budgets, operational strategy and means strategy. Indeed, doctrine, public strategies of deterrence and statements by political leaders make it possible to show the will of a state and thus to strengthen the credibility of its deterrence.

Despite the difficulty of knowing the effectiveness of deterrence or the role of nuclear weapons in restraint among the major powers, most of them consider that their vital interests are better defended by its existence than by its absence or gradual elimination. [8]. Nuclear deterrence, however, remains the preserve of a limited number of powers. The democratisation of cybernetic capabilities seems to be able to offer some countries deterrent capabilities hitherto unattainable.

Cyber-dissuasion, an interesting potential?

The development by some countries of digital capabilities with a view to integrating them into a deterrence strategy shows that this theory is not entirely illusory. Indeed, the emergence of new tools points to the possible use of these means in the field of deterrence. Some operations, such as Operation Olympic Game [9] attacks on Iranian uranium enrichment centrifuges or the recent disruptions to the Ukrainian power grid

show that computer attacks can cause serious damage to an industrial system. As such, these weapons can now be assimilated to weapons of mass destruction and have a real deterrent effect. Moreover, the consequences of such attacks can be multiplied tenfold when they are directed against highly digitised countries, as was the case in Estonia.[10] in 2007. While these examples did not result in any damage comparable to a nuclear response, they prove that, without some restraint on the part of the sponsors, the consequences could have been catastrophic. In addition, cyberspace can provide a better gradation of responses to an attack. It allows both for broadening the scope of deterrence from only the most serious attacks to warnings prior to a larger response.

Moreover, while nuclear deterrence is regularly called into question because of the considerable financial effort it requires, cyber-deterrence seems much more affordable. First of all, from an economic point of view, the investment needed to develop cyber defence capabilities is in no way comparable with the budgetary effort required by the nuclear deterrent. By way of example, France currently spends about 3 to 4 billion euros per year on its deterrent tool, whereas it has announced that it will invest about one billion euros over the period of the 2014-2019 military programming law within the framework of the cyber defence pact'. From an industrial and technical point of view, mastery of cybernetic means requires neither the same requirements nor the same level of expertise as nuclear weapons. Finally, while human resources remain critical in many countries, digital capabilities are not dependent on any supply of raw materials and can therefore be difficult to control or limited.

Finally, from a normative point of view, there is currently no treaty on the non-proliferation of cyberweapons. Their development is not regulated by international law and, as such, a state can develop its own capabilities to implement a strategy of cyber-dissuasion without fear of economic or diplomatic sanctions.

Thus, cyber capabilities appear to be able to be integrated into a deterrence strategy and facilitate their appropriation by new actors that have hitherto been excluded. However, the real potential of cyber-deterrence today still seems uncertain.

Is it possible to envisage a global cyber-deterrent?

However, major challenges remain in implementing a comprehensive cyber-deterrence strategy. Firstly, there is no absolute cyberweapon today that can be used against an unannounced target at short notice. Indeed, an effective digital weapon, comparable to the one used during Operation Olympic Game and capable of inflicting significant damage, requires a long preparation. Like a conventional military operation, a complex computer attack requires careful planning, exhaustive intelligence gathering on the target and its technical and human environment, and finally the development of a specific weapon that must then be developed and tested to demonstrate its effectiveness. Each target therefore has its own mode of action and weapon. It is therefore difficult to anticipate the development of this type of tool. However, it can be planned in advance by identifying potential enemies and high value-added targets. However, these weapons rely on and exploit "zero day" vulnerabilities and loopholes.[11] which can be discovered and corrected, thus making the chosen mode of action against a given target random or even ineffective. Digital means cannot therefore guarantee a political leader the ability to inflict unacceptable damage with certainty, at any time and on short notice to any potential aggressor.

To be effective, deterrence must furthermore persuade an enemy that he or she faces disproportionate retaliation if the vital interests of a nation are threatened. The

effectiveness of digital capabilities relies, among other things, on the preservation of secrecy, including the means and modes of action chosen to attack a target. This requirement therefore seems to be at odds with the credibility of deterrence, which requires ostentatious demonstration of its capacity for retaliation. Moreover, cybernetic weapons are not as frightening as nuclear weapons, at least for the time being. Indeed, there is to date no example of a "cyber Pearl Harbor" or a "cyber 9/11" as prophesied by former US Secretary of Defense Leon Panetta in 2012. As such, cyber-dissuasion will not be credible until an actor in cyberspace has demonstrated concrete proof of its existence.the destruction capabilities of a cybernetic weapon, as was done on 6 and 9 August 1945 for nuclear weapons.

Finally, even if complex digital weapons are shaped to act against a particular target, the risk of collateral damage cannot be excluded. The Stuxnet worm has infiltrated thousands of computers around the world. However, the interconnection of networks and the dependence of our modern societies on digital technology require a careful and limited use of cyberweapons. A state cannot afford to retaliate against an aggressor and cause equivalent damage to an ally or partner. Difficulties in controlling the spread of a digital attack - and thus limiting collateral damage - therefore seem to be a further impediment to the development of global cyber-dissuasion.

Digital capabilities therefore do not seem to be able to meet the various requirements and fundamentals of deterrence. As such, nuclear weapons still appear to be the most effective and secure means of deterring a state aggressor from threatening a country's vital interests. However, the feasibility of implementing effective cyber-deterrence to prevent destructive cyber-attacks can be explored.

Can cyber-deterrence be used to prevent large-scale digital attacks?

In this last section we will distinguish between two types of deterrence: prohibition and retaliation. First of all, let us recall that cyber-deterrence must prevent sophisticated attacks capable of threatening the vital interests of a nation. Such attacks today benefit from the relative anonymity of digital space and the difficulties in establishing the origin and attribution of such attacks. Indeed, even if the number of actors with the technical, financial and human capacities required to implement complex APT-type attacks is limited, it is still difficult to establish the origin of these attacks.[12] remains limited, the attribution[13] is a long process with uncertain outcomes. Evidence accumulated during investigations rarely leads to formal attribution, leaving a degree of uncertainty. Moreover, the evidence gathered cannot always be communicated, at the risk of revealing sensitive capabilities. The attribution process is ultimately a political decision, based on a number of assumptions and may therefore suffer from a lack of legitimacy in the international arena.

Cyberspace has also shaken up the game of traditional alliances, as certain revelations have shown, particularly during the Snowden affair. Confidence in yesterday's allies is now being called into question. The number of players to be deterred is thus multiplied. However, unlike nuclear deterrence, the preparation of a digital deterrent weapon requires the prior designation of an adversary and a specific target. This confirms the security dilemma explained by Ben Buchanan[14]. Indeed, in the digital realm, this is potentially more intense in that intrusion into the networks of others is a necessary precondition for defence or even preventive attack. The risks of misinterpretation and a crisis of confidence between partners are therefore multiplied.

However, while retaliatory deterrence seems illusory in the face of complex digital

attacks, it appears that deterrence by prohibition may partly explain the absence of a "Cyber Pearl Harbor". Indeed, the implementation of active and passive defences, which are increasingly sophisticated and effective, increases the cost of attacks. As such, the number of actors capable of penetrating critical information systems in order to cause significant damage remains limited. Moreover, if the investment required to prepare and conduct an attack exceeds the expected gains, deterrence by prohibition will have proved its effectiveness.

In short, cyber-dissuasion by retaliation remains for the time being a utopian dream. The restraint observed by States when using digital means is explained more by the fear of creating a precedent. This balance, which can be described as a numerical balance, in no way prevents the exponential increase in smaller-scale attacks which, by remaining below a certain threshold, do not lead to any real response from the countries attacked. The interconnection of networks and the dependence of modern societies on digital technology also help to explain the absence of a "cyber 9/11". Even attacks against the cognitive sphere have not led to massive retaliation. This means that there is still proportionality in the response. Nuclear weapons therefore continue to play their deterrent role. However, States are trying to protect themselves from cyber attacks by establishing a real deterrent by prohibition and by threatening aggressors with retaliation by conventional forces. This is, moreover, the French position.[25] As the Minister of Defence recalled in an interview with Le Journal du dimanche on 8 January 2017 : "France reserves the right to respond by any means it deems appropriate. This can be done through the cyber arsenal at our disposal, but also by conventional armed means. Everything will depend on the effects of the attack.

[1] "Communication space constituted by the worldwide interconnection of automated digital data processing equipment". Défense et sécurité des systèmes d'information stratégie de la France, ANSSI, 2011.

[2] Bonnemaison Aymeric and Dossé Stéphane. "Attention cyber! Towards the cyber-electronic combat". Paris, Economica, 2014.

[3] Direction générale de l'armement.

[4] Either 4,000 citizen cyber defense reservists and 400 operational reservists.

[5] Speech delivered on the occasion of Jean-Yves Le Drian's visit to the Directorate General for Armaments / Information Management (DGA-MI) for the inauguration of the cyber centre of excellence on 12 December 2016.

[6] Joint Glossary of OperationalTerminology, framework document DC-004_GIATO (2013), No. 212/DEF/CICDE/NP of 16 December 2013, amended on 1 June 2015.

[7] Example of the MINOTAURE exercise simulating a nuclear raid by strategic air forces towards the Middle East in September 2015.

[8] United States, Russia, France, United Kingdom, China, India, Pakistan. The Hebrew State has never officially recognised possession of nuclear weapons and the effectiveness of North Korea's capabilities has yet to be proven.

[9] The Stuxnet computer worm discovered in 2010 was probably designed by the NSA in collaboration with the 8200 unit of the Israel Defense Forces to slow down Iran's nuclear programme.

[10] Estonia suffered a prolonged "denial of service" attack in 2007 on government, bank and newspaper sites. This attack, which disrupted the functioning of Estonian institutions for several weeks, appears to have been launched by Russian activist groups.

[11] A Zero day vulnerability is a computer vulnerability that has not been published or has no known patches (Wikipedia).

[12] APT: an Advanced Persistent Threat is a stealthy and continuous computer attack, often orchestrated by "organizations" for espionage or sabotage purposes. An APT usually targets an organization for business reasons or a state for political reasons (Wikipedia).

[13] Attribution is a complex process of gathering technical and environmental evidence by studying the political, economic, social and geopolitical context of an attack. It is all of these clues that will enable a policy maker to attribute an attack to a state or group with a certain degree of uncertainty.

[14] Ben Buchanan, "The cybersecurity dilemma: hacking, trust and fear between nations", London: Hurst & Co., 2017.

[15] Also taken up by the United States and the United Kingdom

Officer of the Army, of the promotion "General Béthouart" 2000-2003 of the Special Military School of Saint-Cyr, the Chief of Battalion GERLINGER served in the 1st regiment of the "General Béthouart" of Saint-Cyr.Marine Artillery Regiment of Laon-Couvron, the Pacific Marine Infantry Regiment of New Caledonia and the Centre d'analyse technico-opérationnelle de défense of the Direction générale de l'armement. A graduate of the 23rd class of the École de guerre (2015-2016), he is currently a trainee in the specialized master's programme of the Saint-Cyr Coëtquidan Schools "Operations and crisis management in cyber defence".

Acknowledgements

The author would like to thank Mr. Stéphane Taillat and Mr. Jean-Pierre Letanche for their sound advice and investment.

Bibliography:

- Ben Buchanan, "The cybersecurity dilemma: hacking, trust and fear between nations"London: Hurst & Co., 2017.
- BOYER, Bertrand. "Cybertactics: Conducting Digital Warfare." Éditions Nuvis, 2014.
- Bonnemaison Aymeric and Dossé Stéphane. «Attention cyber! Towards cyber warfare». Economica, 2014.
- Kello Lucas, Richard Thomas, et al, "Cyber Weapons: Dilemmas and Possible Futures," Foreign Policy, 2014, no. 4, pp. 139-150. Kempf Olivier, Introduction to Cyberstrategy. 2012.
- Kempf Olivier. «Introduction to e-strategy». 2012.
- Boyer Bertrand. «Cyberstrategy: the art of digital warfare». Nuvis, 2012.
- Lupovici Amir. "Cyberwarfare and deterrence: trends and challenges in research". Military and Strategic Affairs, 2011, vol. 3, no. 3, pp. 49-62.
- Dogrul Murat, Aslan Adil and Celik Eyyup. "Developing an international cooperation on cyber defense and deterrence against cyber terrorism". In: Cyber conflict (ICCC), 2011 3rd international conference on. IEEE, 2011. pp. 1-15.
- NATIONAL RESEARCH COUNCIL et al.".Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy». National Academies Press, 2010.
- Goodman Will. "Cyberdeterrence: tougher in theory than in practice?"Senate (United States) Washington Dc, Committee on armed services, 2010.
- Libicki Martin C."Cyberdeterrence and cyberwar". Rand Corporation, 2009.
- Power Marcus. "Digitizedvirtuosity: video war games and post-9/11 cyber-deterrence." Security Dialogue, 2007, vol. 38, no. 2, pp. 271-288.

Title : Chef de bataillon Frédéric GERLINGER

Author (s) : Chef de bataillon Frédéric GERLINGER

Release date 10/10/2018