Cyberwar or the questioning of France's rank on the international stage

military-Earth thinking notebook

le Chef de bataillon Bruno EMPTAZ

Published on 04/06/2018

Sciences & technologies

Based on various and eloquent examples of cyber attacks, this article demonstrates the urgent need to consider cyber warfare as a fact and not as a hypothetical threat born of a few alarmist minds. It also recalls the concrete measures taken by the French public authorities since the 2008 White Paper, particularly within the Ministry of Defence. A comparison with other major nations finally reveals the extent of the threat and the path to be followed to guarantee France's rank in this new area of conflict.

Le cyberspace: "the communication space constituted by the worldwide interconnection of equipment for the automated processing of digital data".

This technical and restrictive definition, given by the SGDSN in 2011 in its strategy for the defence and security of information and communication systems, is a technical and restrictive one.This technical and restrictive definition, given by the SGDSN in 2011 in its strategy for the defence and security of information systems, could confine cyberspace to the role of the fifth battlefield mentioned by some authors, after land, air, sea and space. But cyberwarfare, in a modern approach to international relations, based much more on American smart power than on the conventional balance of power inherited from the Cold War, takes on a much more important cross-cutting dimension. War in this virtual space no longer resembles a classic military confrontation between states, but takes the form of multiple and very real actions in each strategic sector: security, the economy, energy, information...

As early as 2009, President Obama was concerned about this by making cyber defence one of the priorities of his mandate: "The cyber threat is one of the greatest economic and national security challenges facing the United States."

Events have proven him right, as the diversity and number of attacks have demonstrated that cyber warfare is not science fiction. As a result, an unbridled race for cyber defence

was launched by the world powers to protect their vital interests and maintain their supremacy. France has been no exception to the rule, particularly in the defence sector, even if the effort to be made in this area, which is a guarantee of maintaining its rank on the international stage, is proving to be permanent and costly.

War in cyberspace has a wide variety of variations, in terms of the techniques employed, the targets targeted, the origin of the actions and, incidentally, their motivation. Cyber-attacks thus target not only information, but also the information and communication systems (CIS) that contain it, and even certain equipment or physical installations. The consequences can be manifold: obtaining primacy over information, recovery of industrial or security secrets, neutralisation of weapons systems, means of communication and destruction of sensitive infrastructures.

"Cyber war is well declared"

Cyber-espionage is undoubtedly the best known phenomenon, particularly following the resounding Snowden affair, the consultant to the National Security Agency (NSA) whorevealed a vast espionage campaign orchestrated by the agency through the intermediary of large American firms operating in the Internet sector. The discovery in May 2012 by the Russian anti-virus publisher Kaspersky Lab of a particularly powerful piece of malware, called FLAME, was less publicized but just as significant [1].

The targets of this modern espionage are varied, with the American "cyber-commander " , General Alexander, recently acknowledging that the systems of the Department of Defense were attacked nearly six million times a day. Serious intrusions into the information systems of the Pentagon, the State Department or NASA have also been noted in recent years and largely blamed on the Chinese competitor.

France and its some two hundred public and private "operators of vital importance" (OIVs), listed in particular in the industrial sector, are also of great interest to pirates. M. Le Drian, the Minister of Defence, is unambiguous on this subject: "It is now the attack on the strategic interests of the State and our autonomy of appreciation, decision and action by cyber threats (...) that is a major challenge for defence and sovereignty".

The denial of service (DoS) attack technique is also common. It aims to saturate servers in order to prevent access to certain computer services, particularly institutional sites.

The massive attack against Georgian cyberspace that preceded the Russian intervention in Georgia in 2008 was an illustration of this and the first known case of integrating a cyber attack into a global military manoeuvre.

The risk of a "cyber Pearl Harbor".

Other types of attacks raise the threat level even further by concretely engaging the physical security of infrastructures and individuals through direct action on the information systems and software of critical equipment in the industrial, energy and transport sectors. Leon Panetta, the US Secretary of Defense, even believes that "some

countries would already be capable of provoking a cyber Pearl Harbor worse than September 11! Attackers could derail a passenger train or a convoy of dangerous chemicals. Or they could contaminate the water systems of large cities or shut down a large part of the power grid. The irony is that its most significant illustration is the STUXNET computer virus, probably the result of US-Israeli cooperation, which delayed Iran's nuclear programme by damaging Siemens centrifuges at the Natanz uranium enrichment site.

The defence sector is obviously a privileged target of these various attacks, while the effectiveness of information and communication systems (CIS) is unanimously recognised as one of the keys to operational superiority. The digitisation of the battle space (NEB), the complexity of weapons systems and the search for increasing interoperability between allied CIS (such as ISAF's Afghanistan mission network) are allsources of vulnerability. For example, a multi-mission frigate (FREMM) today brings together nearly 2 400 information systems.

Cyber warfare is all the more pernicious in that the legal uncertainty surrounding it and the beginnings of international cooperation, particularly within the EU and NATO, do not yet make it possible to provide a homogeneous and comprehensive response. The recent Snowden case even demonstrates that cyberspace allows the lowest blows between official partners and unofficial competitors.

The tense relations in this area between the United States and China are a paroxysmal manifestation of this. The middle empire is regularly accused of resorting to massive industrial and military espionage, as demonstrated in particular by the very substantiated report of the Mandiant security firm in February 2013.

The recent information from the Washington post on pirate access to the plans for the US Army's most advanced weapons systems, such as the Patriot missile, the Aegis radar and the F-35 fighter development programme, could have far-reaching consequences.

Moreover, the origin of cyber attacks is not formally confined to state services. In the Chinese case in particular, it is the work of private agencies acting for the benefit of the state, but also of activist, terrorist or criminal groups with financial or ideological motivations. These various malicious actors take advantage of the two facilities offered by cyberspace.

First, no significant human and financial investment is required to launch a cyber attack. A few connected computers and high-performance malware or spyware (malicious or spy viruses), which can be downloaded online, allow a handful of hackers, delocalized and with no direct link to the sponsoring service, to launch a cyberattack.

Secondly, the difficulty of locating the attacker, maintained by the widespread use of hacked IP addresses, software for the protection of the Internet, is a major obstacle to the success of a cyber attack.The difficulty of locating the attacker, which is maintained by the widespread use of hacked IP addresses, anonymization software (TOR), "zombie" computers or a system of bounces on servers located in different countries, contributes to his impunity.

These facilities, which are becoming increasingly acceptable to certain "rogue states"or

terroristgroups, only amplify the risks for the targeted states. For example, on April 20, 2013, theAssociated Press Twitter account was hacked, allowing the dissemination of false information about an attack on the White House that injured President Obama. This action was then claimed by the Syrian Electronic Army, close tothe El-Assad regime.

According to James Clapper, director of national intelligence (DNI), cyberterrorism is the most serious threat to the United States, noting that terrorist groups affiliated with al-Qaida are also beginning to develop sophisticated cyber-attack capabilities.

War in cyberspace can therefore no longer be regarded as a hypothetical theory maintained by a few catastrophic authors. On the contrary, because of the breadth of its scope, the seriousness of its potential consequences and the very favourable context in which it takes place, it must be seen as a concrete problem. This is undoubtedly what Hamadoun Touré, Secretary-General of the International Telecommunication Union (ITU), believes when he solemnly states: "Cyberwar is well declared".

The need for cyberwar arms control

The 2008 White Paper on Defence and National Security already showed that there is an awareness of this new challenge: "In the next 15 years, the increase in attempted attacks by non-state actors, hackers, activists or criminal organisations is a certainty".

This led to the creation in 2009 of a national authority attached to the Secretary General for Defence and National Security, the National Agency for the Security of Information Systems (ANSSI). In January 2011, ANSSI will publish an interministerial strategy on defence and system security.

Due to its specificities, the Ministry of Defence is developing its own cyber defence structures in parallel. To protect its dedicated information and communication systems, it has built a joint operational chain of command under the authority of the Chief of Defence Staff and integrated into the CPCO. In 2011, a "Joint Cyber Defence Concept" is being developed and a CYBER OG (General Officer in charge of Cyber Defence) is appointed, Rear Admiral Coustillière. Advisor to the CEMA and the Ministry authorities, he leads the defensive cyber defence (LID) by means of a reactive system. His armed wing, the Centre d'analyse en lutte informatique défensive (CALID), monitors networks and seeks to counter computer infections. It is thus part of Piranet, the interministerial plan for responding to cyber attacks, which provides for the deployment at very short notice of real computer commandos, the "rapid intervention groups" (GIR).

CALID's collaborative work within and outside the department is also a guarantee of effectiveness. To this end, it relies on the technical expertise maintained by the DGA on its "information control" site in Bruz, where are notably tracked down possible security breaches in the armed forces' weapons and information systems. It also benefits from a citizen cyber defence reserve, made up of a core of volunteers accredited by the military authority, including some fifty engineers capable of reinforcing the system in the event of a major crisis.

Cyber defence intelligence", provided in a short loop by the DGSE, the DRM and the DPSD, completes the system by anticipating certain threats.

At the interministerial level, CALID runs a permanent network for the exchange of technical and operational information. It works closely with the ANSSI operational centre (COSSI), with which it is to be co-located by the end of 2013.

Since the 2013 White Paper and the identification of certain shortcomings, additional efforts have been made to prepare for the future. This is leading to a tripling of the funding for research and development in the field of cyber defence to EUR 30 million per year. The promotion of skills for the benefit of defence is also being strengthened by the growing importance of the university centre of excellence for cyber security in Brittany, on which the "cyber" research chair of the Saint-Cyr Coëtquidan schools (supported by THALES) depends in particular. Finally, the new military programming law should provide for a substantial increase in the number of staff working in this sector: almost 20% more, to approach the 2,000 people working in the Ministry.

"Have we been too naive?"

The question remains: given the risks incurred in cyberspace, has France taken all the necessary measures to prevent a cyberwar involving its vital interests? Jean-Yves Le Drian, the Minister of Defence, asked himself at a conference on cybersecurity in June 2013: "Have we been too naïve,too confident in the development of the Internet and, more broadly, of information systems?»

This questioning is particularly acute in view of the "cyberarmament" race undertaken by certain nations, which are simultaneously hardening their doctrine of use in the context of cyberwarfare.

In this way, the Americans are offering themselves means that are equal to the stakes and their undeniable leadership in the field. Thus, cyber defence is one of the few growing items in the US defence budget. The national press reports $10 billion in annual budgets and thousands of recruits. The cyber command alone is expected to grow fivefold to 4,900 in the near term.

Two of our major allies, Great Britain and Germany, are also talking about a major budgetary effort in this regard.

China, which has a nebulous cybernetic system due to a system of civilian subcontracting, is said to have nearly 20 staff.There are estimated to be some 20,000 people dedicated to this sector within the "third department of the People's Liberation Army", reinforced by a significant number of research institutes and private companies. The technological means and human skills essential to the efficiency of digital weapons naturally go hand in hand with the financial commitment of these states.

There has also been a significant strengthening of doctrine in response to cyberthreats. TheInternational strategy for cyberspace , published in May 2011 by the United States, equates cyber attacks against the country's critical infrastructure with "acts of war" that could lead to a military response that is not limited to cyberspace. Therefore, the Pentagon, like other countries, clearly recognises that it is developing offensive capabilities in the field of information technology.

Thirteen "teams" are, according to General Alexander, already dedicated to this aspect and can be engaged on the orders of the President in reaction to an attack, but also to prevent it. These capabilities are clearly part of a framework of deterrence, whether used exclusively or in combination with other weapons, in particular nuclear weapons, and whether they are used against a cyber attack or a more conventional attack.

In the 2013 White Paper, France also refers to the use of an "offensive IT capability" if national strategic interests are threatened. However, it makes it conditional on an intelligence capability that is indispensable for characterising the threat and identifying its origin.

Indeed, any offensive response to a cyber attack is conditioned by this prior formal identification, which the Minister of Defence calls "the intimate conviction thatconvergent clusters of clues allow". But the acquisition of these clues remains particularly difficult. In addition to the problem of the time required to detect the attack, only substantial means of collecting and processing computer data can make it possible to effectively attribute the malicious act by tracing its path and identifying the perpetrators. The NSA's Echelon American interception network seems to be the only one for the moment to allow this traceability in a quasi-exhaustive manner.

Should a state be held responsible for a cyber attack launched from its territory, without demonstrating that it is formally at the origin of the attack? The step could be taken quickly by drawing inspiration from precedents from conventional wars, such as Operation Enduring Freedom. The latter was in fact conducted in 2001 by the Americans, with the support of a large part of the international community, to sanction the Taliban regime, host to the al-Qaeda terrorists who had just destroyed the Twin Towers.

The Israeli intervention in Lebanon in 2006 is even more significant, with the Beirut government standing out from the Hezbollah terrorists who were carrying out attacks against Israel from its territory.

Vice-Admiral Coustillière acknowledges France's possession of such offensive means, without going into their nature and capacity. These weapons, under the exclusive jurisdiction of the Ministry of Defence and the DGSE, are in fact covered by defence secrecy. Unlike conventional weapons, they can hardly be the subject of a "show of force"since their main advantage is to technically surprise the enemy. Moreover, collateral damage linked to the viral propagation of the attack cannot be excluded. The STUXNET virus, after realizing its effect on Iranian atomic power plants, infected, for example, the Intradef military network in Afghanistan.

Ambitious preparations for the future

Without excessive naivety or alarmism, France has therefore set itself up to face the cyberwar that is increasingly shaking international relations, far beyond conventional power relations. However, it will only be able to hold its own in this new battle space if it constantly adapts and invests heavily. Defence will have to constantly improve its specific skills and capabilities, particularly offensive ones, in the face of this highly evolving threat. More broadly, the public authorities will have to raise the awareness of each national

player, optimise interministerial cooperation and involve civil society and economic players in its efforts, while preserving its industrial independence in the most sensitive sectors.

Finally, the international community, following the example of NATO's creation of a cyber defence centre of excellence in Estonia or the European coordination of the European Cyber Defence Agency (EDA), will also be involved in this process.Finally, the international community, such as the creation by NATO of a cyber defence centre of excellence in Estonia or the European coordination of Computer Emergency Response Teams (CERTs)[2], must equip itself with the legislative tools and binding procedures to curb the malicious use of this space without geographical and technological limits. It is only on this condition that the individual efforts of each State can be reduced in favour of collective cyber-dissuasion. France has understood this too, by explicitly supporting international initiatives, notably in the latest white paper on defence and national security.

1] FLAME malware, described as the most powerful malware ever encountered, offered a remarkable range of features and seemed to have been rife on the web for several years. In addition to the classic ability to infiltrate a computer without the user's knowledge to take control, collect information or delete files, it was able to read emails, remember keystrokes, take screenshots, record conversations and film the environment by activating the computer's microphone or webcam itself.

2] Various European countries, including France, have set up Computer emergency response teams (CERTs). These independent structures inform the organisations attached to them (administrations, research centres, companies) about vulnerabilities and how to protect themselves against them. The European Government Computer Security Incident Response Team (EGC) complements this panel by bringing together certain government CERTs.

Holder of a master's degree in law, specialising in multimedia and information systems, the EMPTAZ Battalion Commander has been working in the field of electronic warfare for more than ten years. In this capacity, he has directed the Intelligence Analysis and Exploitation Centre of the Electronic Warfare Centre and conducted several specialised operational missions. Admitted to higher military education, he is currently projected within the European Defence Agency in Brussels.

Title : le Chef de bataillon Bruno EMPTAZ

Author (s) : le Chef de bataillon Bruno EMPTAZ

Release date 01/06/2018