Cyberwar: A New Face of War?

Cahiers de la pensée mili-Terre No. 43

le Commandant Jean-Sun LUIGGI

Published on 03/04/2018

Histoire & stratégie

Many States, terrorist or mafia organizations continue to develop or improve their cyber' capabilities, with the most advanced among them devoting very significant human and financial resources to this. France has taken up this challenge by making the necessary intellectual and material investments. The author of these lines, however, argues for a more ambitious reflection: cyber defence must be comprehensive, it must concern offensive aspects; it must become cyber warfare.

In 2012, noting "probably the most destructive attack the private sector has ever experienced" against oil companies, the World Bank said in a report released in July 2009 that it had "aoil and gas companies and several banks, US Secretary of State Leon Panetta said there was now a risk of a cyber Pearl Harbor. Have modern Western societies become "cyber-dependent" by relying so heavily on technology? How unwise it is to ignore the new ways of confronting each other via the Internet and new information technologies, since competition with certain emerging nations is inevitable in cyberspace! The possibilities offered are renewing operational capabilities. The new White Paper on National Security and Defence of 2013 reaffirms the need to enter into an increasingly active cyber defence[1]. 1] However, while the term cyber defence refers to the defence of critical infrastructure, it can also be applied to the field of offensive operations.

Symptoms of a breakdown

The Chinese strategist Sun-Tzu recommended a short war in order to commit as few resources as possible. "One cannot keep troops in the field for long without doing great damage to the state and deadly damage to one's own reputation. What better than a new weapon to surprise and defeat an adversary quickly?

- Scope and level of threat

The Army has chosen to digitize the battle space and is developing the SCORPION program. The arrival of this major programme includes the delivery of new equipment "connected" to information and command systems. The dependence of our armed forces on information technology appears to be growing. What are the risks involved? Cyber attacks are constantly on the rise and represent a significant financial cost per industrial sector. In 2014, they cost an average of $145 million compared to $130 million in 2013 [2].

2] While there are strong presumptions about the origin of these attacks, there is no legal proof of the involvement of a particular state. 3] The difficulty in "attributing" the origin of these attacks is technical and legal. There is the notion of attribution describing a technical action in cyberspace and the notion of attribution in the political domain[4]. 4] In legal terms, it is at the international level that the problem arises. The Netherlands does not allow the disclosure of a person's identity on the basis of his or her IP address[5]. 5] It is therefore easy to find asylum under the various existing national laws.

- Disturbance of the balance of power .

An attacker enjoys relative impunity. If one of the forces involved is unable to respond to cyber attacks, an imbalance of power is created. It's called "technological disruption".

The risk is that the source of a cyber attack cannot be determined and therefore cannot retaliate because it is unclear who the adversary is. States find themselves potentially opposed to transnational organizations with blurred contours. The information conflict has in fact shifted to the level of third-party actors, sometimes far removed from national logic. Thus, if the motivation of "Hacktivists" is to protect individual freedoms on the net, it will be difficult to anticipate the reactions of these groups. Following the attacks of January 7 and 8, 2015 in France, the struggle between cyberjihadists and members of Anonymous demonstrated the similarity of their mode of action (disfiguring websites, denial of service attacks, propaganda through social networks).

- ...with an asymmetry that is miscible in conventional warfare.

In recent years, cyberwarfare has been enjoying a very favourable breeding ground for expansion. Some countries have launched their programme to create "cyber units". For example, China, Syria, the United States and Great Britain have invested heavily in setting up cyberbattalions. The awareness of the Chinese, faced with the technological obsolescence of their military equipment in the 1990s, accelerated the search for a vulnerability that would enable them to get ahead of the United States. This vulnerability lies in particular in the dependence of Western nations on information technology. China's creation of a 9,600-strong cyber army corps, including units 61398 and 61046 [6], is a clear response to the desire to wage war in cyberspace.

Future conflicts are likely to mix conventional and cyber warfare. Both military and civilian targets would be targeted. In the Ukrainian crisis, which revealed old power relations underlying the NATO-Russia relationship,[7] the use of media and social networks to influence opinion is sometimes highly targeted. For example, separatist forces in eastern Ukraine posted images of French volunteers fighting in their ranks on Youtube.

Cyber warfare: what are the patterns?

Is cyberwarfare a war in its own right or a complementary means of warfare?

- Hybrid warfare and cyberwarfare: new rules?

Are cyber attacks intended to be part of a panoply of techniques that subject the adversary to his will and lead to victory? The means recently deployed by Russia in Ukraine resemble a new kind of so-called non-linear warfare involving multiple actors: media, diplomatic, humanitarian, economic, influence, mercenaries and volunteers. The combined use of these means is akin to an interpenetration of soft and hard power[8]. This diversity of actors paradoxically expresses the search for a concentration of efforts in order to win the information battle. With no apparent links between them, these actions have the same goal: to convince public opinion of the merits of this or that operation. In such a framework, the cyber dimension takes its full place[9]. 9] In reality, if certain actions, such as operations of influence, information campaigns and aid to populations are applied by NATO nations, they already belong to the wars of the past. To Win hearts and minds is a concept dating back to the Vietnam War, which stems from the experience of the European colonial wars.

The French principle of concentration of effort tactically implies to carry the effort to a certain point with a maximum of forces. The interest of cyberwarfare is to concentrate where military force does not operate. Conventional strikes can be carried out in one sector, while cyber warfare assets can operate elsewhere. This brings us closer to John Warden's five-circle concept of parallel attack, where the goal is to strike as close to the command centre as possible when the focus is on conventional forces. The author cites the case of the Vietnam War, where the Viet Cong succeeded in overthrowing American public opinion .

Tactically, at the level of combat units, it is still tricky to put digital warfare into practice. While military literature is developing new theories on the use of computerised means (Tactical Perspectives"by General Guy Hubin), or makes comparisons with known modes of action (cyber warfare is compared to combat in urban areas in "Cybertactics, waging digital warfare." by Bertrand Boyer), the concrete implementation of digital combat generalised by contact units is not yet on the agenda. The Army uses light electronic warfare units that intervene in operations. On this model, duly trained and equipped digital combat units could one day complete the tactical military arsenal.

- Weapon of the weak or average universal?

Although the application of the notion of preventive warfare to the virtual sphere may open up new perspectives, a cyber attack is not the primary intention of a nation that is already militarily powerful. A cyber attack is more likely to be used by the weak as a means of cheaply circumventing that power. Countries with weak technological capabilities offer little leverage for cyber warfare actions. An attack against these nations would not offer massive effects and would only be of interest in the context of one-off high value-added objectives (the case of enrichment plants for Stuxnet). On the other hand, techno-compliant nations offer a target of choice where the domino effect is at its peak. Estonia, which in 2007 suffered the effects of DDoS (DistributedDenial of Service)

attacks that were relatively simple to implement, was gradually paralysed by a successive attack on all economic, financial and governmental systems. 58 websites were blocked, including the site of the country's main online bank. The paralysis lasted three weeks, with most Estonians unable to withdraw money from ATMs. This type of operation is carried out at low cost, at the cost of maintaining a small, well-trained cyber army or mercenary hackers not attached to any government. By the admission of some Russian "hacktivists", Estonia's computer protections were non-existent.

- Shoot-and-forget technology

A cyber attack often allows the perpetrator to remain anonymous and hide his intentions. While the Stuxnet virus could be quickly detected by computer security companies such as Kaspersky on a wide range of computer media around the world, its real purpose was revealed when its target was reached: Iranian centrifuges.

The cyber attacker retains his freedom of action, not being "fixed" at the time of the attack. In "Tactical Perspectives"General (2S) Guy Hubin stressed this questioning of the notion of fixation in the age of new technologies. Cyber attacks are more akin to the use of a "shoot and forget" technology with little constraint than to the deployment of conventional military means with a strong political and logistical footprint. Even if it is always possible to find a cyber-attacker (the in-depth study of viruses has made it possible to link Israel and the United States for the attacks by Stuxnet, Duqu and then Flame to slow down the Iranian nuclear programme), the time needed for this search does not allow the guilty party to be really worried at the time of the events. This idea also finds its fulfilment in the many cases described in the thirty-six Chinese ploys, which favour the use of indirect means of action: striking with a borrowed sword.

Cyber warfare can be used to achieve a limited objective. In the case of Stuxnet, a vital infrastructure has been destroyed, which can be the object of a so-called "limited" war or a simple tactical objective.

Indirect confrontation logic and coercive action

In the West, cunning has long been denigrated because of a chivalrous tradition [10]. 10] However, the results can be spectacular and contribute to the principle of economy of means.

- An analogy with **"The**Art of War"

According toThe Art of War"..."keeping the enemy's possessions is what you must do first, as the most perfect thing; destroying them must be the effect of necessity". By hitting a few lines of code, the enemy may be dispossessed of his resources. The Estonian crisis is indicative of this mode of action. The aim of the cyber attacks against that country was not theft, but the paralysis of its economic and financial institutions.

This new cohabitation of symmetrical and asymmetrical means prolongs the interpenetration of Yin and Yang actions (also called direct and indirect forces) described in "...".The Art of War" by Sun-Tzu: "Generally use direct forces to engage the battle, and indirect forces to win the decision".

Moreover, the intelligence value of cyberwarfare naturally arises when infected computer servers and systems are infected without the knowledge of their victims. Certainly, cyberwarfare achieves the goals of the thirteenth chapter of "[c]omprehensively, cyberwarfare achieves the goals of the thirteenth chapter ofThe Art of War"including disinformation and subversion.

- Cyberwar: The Holy Grail of Five-Circle Theory

Cyber and information warfare in the broadest sense allows the application of J. Warden's five-circle theory. Striking the opponent's critical infrastructure - power plants, communication networks, road networks or distribution networks (the second and third circles) - remains the core target of cyberwarfare. These attacks can have a lasting impact on a state's economy, but also on its population (the fourth circle), much more surely than an embargo. In theEnemy as a system"Warden explains that hitting the opponent's armed forces (the fifth circle) is not the most important thing. Achieving the will to fight and causing strategic paralysis will force the opposing command (the first circle) to compromise.

Cyber warfare is already a new area of strategic thinking. A nation or system of alliances relies fully on its civil resources. Cyber warfare allows for a form of total warfare and is perfectly applicable to the five-circle theory.

Capability leap or technological backwardness?

Cyber warfare refers to a revival of modern warfare, including information warfare in all its forms, where the interpenetration of conventional military means and the strategic level are paramount. This is why defensive and offensive cyber defence components should be integrated with civilian and military means. Estonia has founded a cyber defence centre of excellence for NATO and is relying on the Alliance to develop this capability. Should we give up maintaining a national cyber defence? The Snowden case proves otherwise, if we recall the espionage activities of some of our allies. The national agency for information systems security, created in 2008, meets this requirement by providing France with national and independent means. The Minister of Defence's cyber 2014 action plan translates into concrete action the measures to be taken regarding cyber risk.

It is the lack of means to counter cyber warfare, a capability gap, that constitutes a technological breakthrough for states that lack them. Cyber warfare is merely a renewal of proven methods with innovative and plural technical means.

There is a convergence between the conduct of symmetrical warfare, the exercise of soft power and the asymmetrical struggle of cyberwarfare. Tomorrow's war, if not today's, would combine conventional means with the tools of cyberwarfare to achieve particular objectives, creating confusion among the enemy and its population. In a context of economic constraints, cyber defence in its broadest sense is not the preserve of rich nations or large military alliances. This vital challenge remains within France's grasp. The risk of major cyber attacks against a backdrop of international terrorism is now a real test.

1] "However, the continued growth of the threat, the ever-increasing importance of information systems in the life of our societies and the very rapid development of technologies make it necessary to take a further step to maintain protection and defence capabilities adapted to these developments. They now require us to substantially increase the level of security and the means of defence of our information systems, both to maintain our sovereignty and to defend our economy and employment in France. The human resources

devoted to this will therefore be substantially increased to match the efforts made by our British and German partners. LBDSN 2013, page 105.

2] Cost of Data Breach Study 2014, Ponemon Institute, based on a sample of 314 companies from ten different countries.

3] Viruses hide on multiple remote servers and multiple hosts in different countries. The STUXNET virus was allegedly hidden, among others, on an Indonesian server of a football club.

4] See on this subject "Cybertactics, conducting digital warfare». Bertrand Boyer (ed. Economica).

5] Internet Protocol: a kind of "registration number" used to identify each connection.

6] Unit 61398 is in charge of the USA/America area and unit 61046 is in charge of Europe.

7] We can cite the case of Moldova with the secession of Transnistria since 1992, but also the recent Georgian crisis of 2008,

8] Terminology of Joseph Nye, differentiating the notions of non-coercive leadership (soft power) andhegemony(hard power) in international relations. «Bound to Lead: The Changing Nature of American Power"New York: Basic Books, 1990.

9] As such, since 9 September 2000, there has been an information security doctrine of the Russian Federation, which clearly sets out a global vision of information security as a bulwark, but also as a cultural vector of Slavic civilization. See "The Russian cyber strategy"of Y. Harrel (ed. Nuvis).

10] See "La Ruseet les formes contemporaines de la guerre" by Jean-François Holeindre in "[10] See "La Ruse etles formes contemporaines de la guerre" by Jean-François Holeindre in "[11].The end of the major wars"(ch.3, Ed Economica).

11] "The latter we call strategic paralysis. Which parts of the enemy system we attack (with a variety of weapons ranging from explosives to nonlethal computer viruses) will depend on what our objectives are, how much the enemy wants to resist us, how capable he is, and how much effort we are physically, morally, and politically capable of exercising". J Warden in "Enemy as a system". Cyber attacks are clearly mentioned in this context.

In charge of the pyrotechnics and information systems security of various SEVESO II classified equipment establishments during the first part of his career, Commander Jean-Sun LUIGGI was posted to the Bourges military schools between 2012 and 2015. There, he directed the teaching section of battle space digitization and logistic information systems. He is currently a trainee officer at the École de guerre (23rd promotion).

Title : le Commandant Jean-Sun LUIGGI

Author (s) : le Commandant Jean-Sun LUIGGI

Release date 17/02/2018