note n°15/19

6 September 2019

FONDATION *pour la* RECHERCHE STRATÉGIQUE

Olivier Kempf BRIG (RET)
Associate Fellow ,Fondation pour la recherche stratégique

On cyber and war

Le In the 21st century, war will inevitably be soaked in digital technology. The only relevant question remains whether this constitutes a strategic revolution or whether, as is often the case, there will be nothing new under the sun. Cyber is also the tool of a convergence of struggles in previously distinct fields. There are strong links between cyberconflict and economic warfare that make it difficult to properly appreciate a phenomenon that is necessary to understand a fundamental dimension of war in the 21st century.

Let us say a brief word about this notion of strategic revolution. A strategic revolution changes the modalities of war and can impose new strategic rules without destroying the basic grammar (whether it is inspired by Clausewitz or Sun-Ze).

According to this criterion, new sources of energy have brought about some major strategic changes which can be clearly identified. The coal went hand in hand with the corresponding engine (locomotive, steamer) which influenced the wars of the second half of the 19th century (American Civil War, War of 1870, Mobilization of 1914). Industrial warfare was then invented, and the role of infantrymen was massively expanded. With gasoline came the trio of trucks, tanks and planes, developed in the first half of the 20th century (Second World War, Korean War, Six Day War): there is no need to explain its lasting (and still perceptible) influence on the mechanized armoured structure of many contemporary armies. The nuclear detonation of 1945 shaped the entire second half of the 20th century with deterrence and the polarization of the Cold War. It seems that with data, described by some as the energy of the digital age[1], we are facing a new strategic revolution that will take us into the first half of the 21st century.

[1] See for example "The World's Most Valuable Resource is no longer Oil, but Data", The Economist, 6 May 2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. The expression "data is the new oil" seems to be attributable to British mathematician Clive Humby as early as 2006. But many question this idea of data as energy: see for example "Here's why Data is not the New Oil", Forbes, 5 March 2018 https://www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil/#213eb40a3aa9

This historical outlook puts into perspective the role of these strategic revolutions: they are undoubtedly important, but do not annihilate overnight previous strategic concepts. In other words, digital technologies will not abolish nuclear deterrence, which did not abolish the tank, which had not abolished the over-equipped infantryman, etc. This being said, digital technology is therefore a strategic revolution. It affects the conduct of war. Therefore, let us examine the links between cyberspace and war.

Cyber: what does it cover ?

Since the 1980s, we have witnessed several successive waves of the computer revolution, considered as a continuous trend: the first was that of personal computers in the 1980s. Then came the Internet - to the general public - in the 1990s. This was followed by the age of social networks and web 2.0 in the 2000s. Today we are faced with a fourth cycle, that of digital transformation (DT), which is shaking our societies ever more violently, in particular in the economic realm. We could of course refer to this whole massive computer world as "cyberspace".

These different cycles have had their equivalents in the strategic field.

A brief history of cyber

Before the emergence of the concepts of battlefield digitization and network-centric warfare, the rise of information technology prompted strategic concerns a long time ago.
If we go back to the early 1960s, the United States founded the ARPA (ancestor of the DARPA) in order to respond to the noted efforts of the Soviets in computing and in what was then called cybernetics: it is worth recalling given the role played by the DARPA in the invention of the Internet. This concern was later transformed by Zbigniew Brezinski who, as early as in 1970, spoke of a *technelectronic revolution*[2]: computer power is considered by him as the means of victory over Soviet power. More recently, we must look back to the debates of the 1990s on the Revolution in Military Affairs (RMA): the aim was to take into account the changes brought about by personal computers, but also by mass networking, in other words our first two waves of computing. *Cyberwar is coming*, as two Rand authors stated in 1993[3] .

All in all, these debates illustrate only one perception: computer power should be used to give the armed forces new means. IT is only seen as a tool, a power multiplier. It applies to both weapons and staffs. It is this same idea that governs the definition of the Third Offset Strategy, launched by the United States a few years ago: to move forward technologically with a forced march so as not to be overtaken by another power in the field of capacities.

The networking of military staffs and the development of IT in weapons have led to a definite increase in efficiency. We are now talking about weapons systems, command systems. And it is true that there are undeniable gains in efficiency: just observe the precision of missiles or the capabilities of a modern fighter aircraft... From now on, an aircraft is no longer a bomb carrier, it is a computer that flies and transports computers that explode on their targets previously identified and designated by networked computers.

This embedded computing is therefore the natural target of cyber attackers. Faced with a falling bomb, we could only take shelter. From now on, we can imagine sending it a malicious code that would give it false information that will cause the projectile to deviate from its trajectory.

But it is in the area of command that the evolution is most clear-cut. The Anglo-Saxons use the term *Command and Control* to refer to it, simplified in C2. During the 1990s, the computerization of the command function led to the construction of a C4, then a C4ISR, then a C4ISTAR[4] and then... it stopped there, to our knowledge[5]. Let us return to our C4 (the ISR function being specific to intelligence and Target Acquisition to targeting): it is not only

[2] Zbigniew Brzezinski. *Between Two Ages: America's Role in the Technetronic Age*, Viking Press, 1970.

[3] John Arquilla & David Ronfeldt, "Cyberwar is Coming", *Comparative Strategy*, Vol. 12, No. 2, Spring 1993, pp. 141-165. Rand corp. 1993, https://www.rand.org/pubs/reprints/RP223.html

[4] Computerized Command, Control, Communications, Intelligence, Surveillance, Target Acquisition and Reconnaissance

[5] It seems that C5 is mentioned in recent American strategic literature, with the 5th C being used for cyber. This raises the question of the difference between computer and cyber... see: https://c5isr-ccdc.army.mil/inside_c5isr_center/history/_c5isr_center . In February 2019, the former CERDEC became the US Army's C5ISR centre CCDC (https://c5isr-ccdc.army.mil/inside_c5isr_center/history/_c5isr_center/history/). But there are other extensions of this acronym where the fifth C means "combat systems",

Command and Control but also Communication and Computer. Command functions have been automated through networked computing. It was not only a question of dispelling the fog of war but also of accelerating the OODA loop[6]. The method was able to produce results (think, for example, of the two Gulf wars) without convincing ourselves that it was enough to win the war (think of Afghanistan and Iraq).

Basically, this network warfare - the American strategic literature of the 1990s-2000s talked about network centric warfare - is a very utilitarian and vertical war, "from top to bottom". All practitioners know that command networks are often used to feed the top with information and at the risk of increasing micro -management, while bottom users ultimately benefit much less from the new tool.

Size and imprecision of cyberspace

Before the 2010s, when we talked about cyberspace, we were not only talking about this distributed and networked computing, but also about its strategic characteristics. Gradually, the notion of cyberspace has been forgotten in favour of cyberdefence and cybersecurity, the prefix cyber being used by security and defence organisations to cover it all. This shift occurred during the 2010 decade.

The first cases of cyber assaults date back to the 1980s (*Cuckoo's egg* in 1986, *Morris Worm* in 1988). With more systematic attacks (first denial of service attack in 1995, first known attack against the Department of Defense in 1998, first "international" case with *Moonlight Maze* in 1998), strategy started ruling these developments. It entered into the debate on the Revolution in military affairs.

These questions were addressed in the 2000s. The creation of an American Cybercommand in 2009, the Stuxnet case in 2010, Snowden's revelations on the NSA (2013) show that the United States is very advanced on the subject. In France, since the 2008 Defence White Paper, cyber has been identified as a new strategic factor, an approach that was highlighted in the 2013 edition and confirmed by the 2017 Strategic Review. NATO is taking up the subject following the 2007 aggression against Estonia, commonly attributed to Russia, although, as almost always in cyber matters, the evidence is lacking[7]. Before that, cyber was a simple subject of interest, but it has risen on the scale of threats to become a priority concern. Nowadays, a cyber-attack could, if necessary, trigger the implementation of Article 5 of the Washington Treaty. The Allies even agree that cyber to define cyber space as "a fighting environment", just like other physical environments. Without entering into conceptual debates on the accuracy of this assimilation, let us note that this globalizing approach puts everything IT in a cyber pot.

The notion of cyber has evolved

But is it that simple?

It must be noted that the very notion of cyber has evolved. Other prefixes and adjectives have followed: electronic (e-reputation, e-commerce) or, simply, digital. This semantic evolution is now causing the use of the term cyber to be limited to the field of security, defence and strategy. For example, the Lille Forum is an international Cybersecurity Forum, the American command is a Cybercommand.

Basically, while ten years ago there was little awareness of the dangerousness of cyberspace, it must be noted that the transplant has finally taken root and that cyber refers precisely to the protective function that surrounds computer activities of all kinds. Nowadays, when we talk about cyber, we mainly refer to the conflict associated with cyberspace, whether it is crime or defence: on the one hand, we have the particulars of protection and defence itself, on the other hand, the trademarks of aggression, traditionally espionage, sabotage and subversion. This activity is carried out in the three layers of cyberspace (physical, logical, semantic).[8]

To put it simply, cyber now deals with the struggle between various agents using computers to achieve their strategic or tactical

for example https://www.acronymfinder.com/Command%2c-Control%2c-Communications%2c-Computers%2c-Combat-Systems%2c-Intelligence%2c-Surveillance%2c-and-Reconnaissance-%2c-Control%2c-Communications%2c-Computers%2c-Combat-Systems%2c-Intelligence%2c-Surveillance%2c-and-Reconnaissance-(C5ISR).html

[6] The OODA loop is a concept invented by United States Air Force fighter pilot John Boyd in 1960: "Observe, Orient, Decide and Act", its shortening is supposed to be the guarantee of the strategic initiative.

[7] More precisely: while it is undeniable that most of the attacks against Estonia were carried out by Russians, it is not proven that this was orchestrated by the Kremlin: many "patriotic hackers" played a major role in this case. However, at a minimum, the Kremlin allowed this to happen, which is a way of endorsing the operation. In this respect, it can be held liable.

[8] Office of Naval Research, Data Focused Naval Tactical Cloud (DF-NTC), ONR Information Package, June 24, 2014.

1

goals. Networks and computers are the vehicle of various weapons (worms, viruses, Trojans, DDoS, fakes[9], hoaxes, etc.) that make it possible to reach the enemy device and neutralize, corrupt, destroy or lure it.

To conclude on this point, cybersecurity is based on the control of networks, data and flows, which often requires a quota of these and restrictions on their use, whether in terms of IT hygiene or more secure devices, hardened depending the information handled. In other words, cybersecurity tends to restrict the uses that IT intended to simplify, automate or liberate.

There is no cyberwar

Cybersecurity or cyber defence?

The notions of cybersecurity and cyberdefence are similar. It is necessary to identify each of them because while there are obvious links between cybersecurity and a defensive stance, just as there are obvious links between cybersecurity and the Ministry of Defence, these links are confusing and need to be clarified.

First of all, cybersecurity could be considered as a civilian domain whereas cyber defence could be associated with the domain of the armed forces and the military. This approach is widespread, sometimes unconsciously, but it is inaccurate. For example, in the case of France, the civilian ANSSI is the national authority for the security and defence of information systems. However, the word defence is a misleading terminology that causes confusion here.

We could also consider that cybersecurity is a state while cyberdefence is a process. In order to achieve cybersecurity (to be in cybersecurity), it is necessary to provide cyber defence. In one case a stative verb, in the other an action verb. This approach, which is conceptually correct, is unfortunately not widely followed by practitioners. Above all, cyberdefence is sometimes considered as a whole (strategic action in cyberspace) and as a part of this whole (the defensive function of strategic action in cyberspace).

A more operational approach is therefore recommended that avoids the word cyber defence and retains the word cyber security only in a very specific case. In general, it is advisable to avoid the cyber prefix affixed before any noun, because the terms are rarely well defined, and this leads to a lot of confusion.

Cyberwar will not take place

Cyberwar will not take place: this is the title of a remarkable little book by Thomas Rid, published in 2013 in Oxford[10] . He was already questioning the notion of cyber warfare. The term "cyberwar" sounds good, and it is regularly used by uninformed journalists or commentators. However, it is wrong, which does not mean that war ignores cyberspace (on the contrary, cyberspace is increasingly present in the conduct of conflicts).

The problem with the term "cyberwar" is the word war. We have regularly asked ourselves about its profound meaning, that of the past but also of today. If the *great war* of the past is dead, the deadly war remains, often at a low level, even if it can be very deadly[11]. It is no longer the monopoly of the States.

We are witnessing a strong rise and a real diversification of armed crime[12] where actors clash and strike, including weak States that cannot cope with it (we are of course thinking of Mali and many African countries).

If war is no longer fought by organised and, more often than not, national armies, what is now its distinctive criterion? Lethality: the violent loss of human lives for political reasons. From now on, the war criterion that remains is the existence - or not - of human deaths affecting either the combatants in the conflict (military) or the surrounding populations (civilians). We can of course keep in mind the number of one thousand military deaths per year that polemologists have identified to mark the threshold at which there is a war and not an armed conflict. Without going as far as this (are the people drowned in the Mediterranean sea, having tried to reach Europe, victims of a war?), let us note that for the time being, there is no death directly attributable to cyber aggression. Today, the cyber does not kill; at least not yet.

Moreover, we must be wary of all the discourse produced on this theme: a "cyber

[9] DDoS: distributed denial of service - Fakes: false news.

[10] In response to the article by Arquilla and Ronfeldt published twenty years earlier, with perhaps a quotation from Giraudoux's pessimistic work, *The Trojan war will not take place* (1935), since at the end of the play, the Trojan War did take place.

[11] See « Under the strategic thresholds”, https://en.lettrevigie.com/2019/07/17/la-vigie-nr-122-pariahs-and-states-under-the-thresholds-lognette-in-kosovo/

[12] See J.-F. Gayraud, *Théorie des hybrides*, CNRS éditions, 2017.

Pearl-Harbour" is looming, cyberspace is the fifth physical theatre of war, we need cyberarmies, etc. This is an American pattern of thinking that militarizes everything from the outset, in order to justify budgets and a quantitative and destructive approach to all political oppositions. Without being so pitiless as to recall the repeated failures of this American approach for more than seventy years, let us simply point out that there is no exchange of electrons that would strike each other down with winners and losers[13]. Things are more subtle than that.

This does not mean that cyber is not dangerous, nor that it is not in warfare. Rather than cyberwar, let us talk about cyberconflict. It pervades everything.

Operations in cyberspace

Cyber actions

T. Rid's book already recalled the essential point, namely that the three types of cyber-attacks are well known (espionage, sabotage and subversion), and that they do not justify the over militarization of the cyber age.

Cyber espionage is the first brick of cyberconflict. Indeed, almost all cyber offensive actions begin with a phase of observation of the target and therefore, in the most acute cases, of espionage. Whether it is a matter of defacing a site or bombarding it with requests (basic technique known as DDoS: distributed denial of service) or, on the contrary, going much further into the system in search of sensitive information, it is necessary to define the outline of the objective, its strong and weak points. This is the first phase common to all actions because the information is first sought or because it will be used for something else. This is a common feature of all military operations: no matter what you want to do, you always start by getting information. However, the essence of cyberspace is to manipulate information, either to store it or to exchange it with duly identified correspondents. Intelligence (or information) methods and the characteristics of cyberspace are deeply interwoven. However, cyberspace multiplies espionage capabilities. This was widely realized with the revelations of Edward Snowden who taught the world about the potential of the American NSA, spying on the whole world, including its allies and friends.

The preservation of secrets is a property common to sovereignty and freedom of action. This is obvious for States, but it is also true for companies. As a result, massive cyber espionage is changing international or business-to-business relations. Certainly, "*we have always spied on each other, even among friends*", an argument developed by the defenders of the NSA, first and foremost B. Obama[14]; however, the scale of the means implemented and the depth of intrusion allowed by the technique have changed the meaning of this practice. Cyber espionage is indeed the first form of cyber aggression.

Cyber sabotage is the second. It is perceived as the main attack by popular opinion, which often reduces cyber-attacks to those viruses that break computer systems. From Stuxnet to NotPetya, these worms, viruses and malware have often been in the news (journalists rarely miss the opportunity to explain that there has never been such an attack in history, then forgetting their reckless assertion the following week). Thus fear around sabotage is widely spread, enabling the elaboration of incredible fantasies, such as the absurd scenarios of James Bond where brilliant hackers destroy collective systems and cause mayhem.

The reality is more commonplace: there are many attacks, but today, more often than not these are ransom operations (against individuals or organizations, especially cities such as Atlanta or Baltimore[15]) where the attackers block the operation in exchange for a ransom. But it can also have political motives: a few years ago the Saudi Aramco company was blocked by aggressors, obviously Iran's neighbours.

Cyber subversion is the third mode of aggression. It aims to modify the decisions of an individual or a group, whether through sabotage (for example, defacing a website to make Hitler's face appear instead of the company/country leader) or other, more or less advanced, processes. Many neglected this subtle aggression until the development of debates on the question of fake news[16] and post-truth.

[13] This also explains why the notion of cyber-deterrence, which is very much supported by American strategists, is not very convincing. On that, see O. Kempf, Ibid., chapter 8.

[14] Who partly justified the espionage of allies as a protection and revelation of their own flaws; this is the theory of the third party espionage

[15] https://thehackernews.com/2019/05/baltimore-ransomware-cyberattack.html

[16] See F-B. Huyghe, O. Kempf and N. Mazzucchi, *Gagner les cyberconflits, action dans la couche sémantique*, Paris, Economica, 2015 Astronautics, 2019, pp 421-440

Thus, these three processes are frequently used in what must be called real contemporary cyberconflictuality. Let us note two specific characters. The first is that of the actors concerned: from now on, all actors (individuals, groups, agencies or States) can be both the perpetrators and the targets of such attacks. As a result, the reasons for the attacks are extremely varied (political, economic, cultural, reputational, egos, etc.). This gives this battlefield a Hobbesian dimension, that of the *conflict of all against all* that was thought to have been settled with the Westphalian order three and a half centuries ago. This is deeper than political *multism* e.g. the diversity of international relations' participants or the notion of hybrid warfare.

Strategic responses in cyberspace

Denying the existence of cyber war does not mean denying the importance of cyber in the conduct of war, quite the contrary. Cyber is now everywhere in military operations. It is at the heart of armaments: we discuss how autonomous these weapons can become thanks to robotization and artificial intelligence. Cyber activates all command and control networks, which are referred to as Command and Information Systems (CIS).

Strategic action in cyberspace is a general approach. Let us consider that it is normally within the reach of all organizations (or even individuals) except in the particular case of the offensive, which is a state prerogative (and for the moment, specific to the Ministry of the Armed Forces, at least in France). In other words, all non-state offensive actions are illegal.

To start with, there is a first function that will be referred to as **defensive**, also called cybersecurity (strictly speaking). It is the essence of cyberconflict. It covers:

> Protection measures (or cyber-protection, or information system security -ISS- in the strict sense of the term), which consist of all passive measures that organize the security of a system (firewall, antivirus, IT hygiene measures, security procedures). This notion of "passive measures" does not mean that we remain inactive, on the contrary: an ISS manager will constantly be on the lookout, updating his system and mobilizing the attention of his employees.
>
> Defensive measures (or defensive computer struggle, DCS), which include all active monitoring and reactive measures in the event of an incident (probe systems examining network activity and anomalies, establishment of 24/7 operation centres, etc.).
>
> Resilience is the set of measures taken to operate a network under attack during the crisis and then return to a normal state of operation after the crisis (including with reconstruction operations in the most severe cases).

The second function is **intelligence**. It is obvious that it is part of the defensive process. However, intelligence can be identified as a separate activity. A distinction has to be made here between intelligence of cyberspace origin (ICO), that comes from cyberspace but contributes to the overall military intelligence situation, and intelligence of cyber-defence interest (ICI) (which is not necessarily exclusively of cyber origin) and which aims at building a particular situation in cyberspace, which can be friendly, neutral or, in most cases, aggressive. This is thus an information on cyberspace. It is clear that in a global military manoeuvre, the ICO is of greater interest to the decision-maker, while in the case of a manoeuvre specific to the cyber environment, the ICI will predominate. The ICI makes it possible to strengthen the defence but also to prepare the offensive. For example, the passwords of TV5 Monde's social network accounts, recorded in a France 2 TV report, represent ICI, while the Strava application's dynamic race maps, which allow military activity to be observed to locate military sites, are ICO.

Logically, the third function is the offensive. Without getting into too many subtleties, it covers both the offensive computer struggle (OCS) and the digital influence struggle (DIS). The first is turned towards sabotage, the second towards subversion. With regard to influence, let us mention former French Chief of the Defence Staff (CHOD), General de Villiers[17]: in early 2016 he said that there was a "new theatre of engagement" – that of "influence and perceptions". "*It is all fields - including cyberspace - that make it possible to carry the war for, through and against information. This battlefield, which is not linked to physical geography, offers new possibilities for knowledge and anticipation,*

[17] http://www.opex360.com/2016/01/18/pour-le-general-de-villiers-le-domaine-de-linfluence-constitue-nouveau-champ-daction

as well as a field of action to modify the opponent's perception and will". The propaganda of the Islamic State on social networks has made it urgent to take into account the "battle of perceptions".

Cyber environment

These operations are conducted in the cyber environment. This term of environment eludes the notion of domain, although it has become a NATO doctrine. Talking about cyber environment (as we talk about electromagnetic environment) enables this cyber function to be in its right place. It is basically a support weapon much more than a direct weapon. This approach also helps to resolve the dilemma between the strategic and tactical levels, a dilemma that is still the subject of private but essential debates.

It is under these conditions that cyber is present in military operations, in all three layers of cyberspace (physical, logical and semantic). While the operations are discreet, they are nevertheless real. But that does not mean that cyber will not be used in other operations, this time non-military. This is a very different matter, even if it is part of cyberstrategy.

Cyber and new forms of conflict

We have previously talked about the links between cyber and military actions, but also with some civil actions (notion of cyber security). Cyber is undoubtedly a part of war as we have demonstrated. But perhaps war is no longer only in war. In other words, we are now witnessing new forms of inter-state conflict that are below the threshold of war: legal sanctions, economic blockades, fines, economic warfare, massive actions of influence, others. Cyberspace is a remarkable tool for all these hostile actions, which are not just "civilian" but at the same time not military.

Expansion of the field of cyber-fighting

Yet this cyber-conflict does not only take place in the field of military operations. This certainly makes it possible to better understand what is happening, to identify operational principles. Nevertheless, it cannot hide the fact that cyberconflictuality takes place mainly outside the realm of conventional military actions.

One notes several features of this cyber-fighting: it is accessible to many, which does not mean that everyone is capable of doing everything. While it is only in novels that a gifted individual succeeds in defeating great powers, it is true that many individuals can act - and harm - in cyberspace. This has two features that are used by many: relative anonymity if adequate measures are taken (and despite the feeling of general supervision created by both the NSA and the GAFAM); and the ability to aggregate skills during an operation (coalescence).

Therefore, whatever the motive (ideological or patriotic motivation, profit and greed, boasting to prove one's technical superiority), many parties can act in cyberspace (which explains our caution in analysing the Estonian case). In other words, cyberspace allows a general struggle that mixes power interests (traditionally reserved for States), economic interests (multinational firms, mafias), political or ideological interests (NGOs, jihadists, Wikileaks, Anonymous, cyberpatriots) or individual interests (from the individual hacker selling his services to the whistleblower Edward Snowden).

The result is a generalized conflict, mobilizing everyone in a melee all fiercer because it is relatively discreet. Indeed, there are no examples of deadly blows given via cyberspace[18] even if the fantasy of a Cyber Pearl Harbour is constantly being repeated by the Cassandras. Before an extreme tragedy occurs, we should note that ordinary cyberconflictuality rages daily. And, above all, that, before being political, it is mostly economic warfare.

Cyber and economic warfare: the convergence of struggles

Make no mistake: the most important thing is the economic war. This has gone hand in hand with the development of globalization, which itself has been made possible by what were then known as Information Technologies. This radically changed the cornerstone on which the economic world was previously based, that of fair and relatively perfect competition. This

[18] However, there is a complementarity of operations, particularly on the physical layer. Thus, during the Orchard operation conducted in 2007 by the Israelis against the Syrians, the anti-aircraft radar network was disconnected by a cyber operation, each radar being blinded by electromagnetic interference, which allowed Israeli fighters to pass and carry out their raid. We can also consider the destruction of cyber nodal centres or wifi transmitters. For example, Israel has announced that it has carried out raids on certain installations in Gaza to deter Hamas Palestinians from launching cyber-attacks, see, for example, "After suffering a cyber attack, Israel responds by force", The Digital Century, 6 May 2019, https://siecledigital.fr/2019/05/06/apres-avoir-subi-une-cyberattaque-israel-repond-par-la-force/

base no longer exists and nowadays all blows are allowed. Cyberspace is facilitating this profound change. Spying, sabotage and subversion are now weapons that are used daily and underground.

What did Snowden teach us? That the NSA, under the pretext of the fight against terrorism, was spying mainly on the United States' competitors. That it actively collaborated with the major American economic players, in particular the GAFAM, in a two-way relationship; that if they had to cooperate actively with the Federal Administration (who seriously believed that Apple refused to cooperate with the FBI in the San Bernardino attack? on the other hand, it was a remarkable marketing coup), the latter did not hesitate to transmit relevant information to their manufacturers.

China has practiced a sturdy strategy of economic espionage, by all means, including cyber. There are many examples and American denunciations in this area reveal a probable truth. In Israel there is a very close symbiosis between its specialized services (around the famous 8200 unit) and its ecosystem of start-ups (Israel has gone the furthest in building a "start-up nation"). Similar links are to be found in Russia or Singapore.

In other words, there is now a certain convergence of struggles: between actors (collaboration between States and companies, "contracts" between companies and underground hackers) and between domains (geopolitics is never very far from economic "interests": just think of the number of business leaders who accompany political leaders during official trips abroad).

Cyber allows this convergence thanks to its apparently painless effects (who will ever be able to evaluate the cost of sensitive information that has been stolen by a competitor?), and to its obvious discretion, to its comfortable anonymity.

An all-encompassing conflict

Leyber is now at the centre of all conflict strategies, whether military or not. Its plasticity and transversal character allow the development of a multitude of manoeuvres by parties of all types.

Acting in cyberspace, whether you are a military commander, a political leader, an economic leader or a simple CISO (chief information security officer), requires you to be aware of this general dimension. Basically, cyberspace cannot be reduced to a simple technological environment managed by technical but subordinate managers. Cyberspace allows the creation of a new conflict that will, in a way, merge the traditional fields of hostilities: military wars as well as geopolitical oppositions or economic competition. That is why talking about cyber warfare is extremely misleading: it is first of all false (because the criterion of lethality is not met) and above all reductive because the conflict in cyberspace certainly has military dimensions, but these are also broader and often more insidious than the "simple" use of force and coercion at the root of military actions.

In this sense, there is a globalization of cyberconflictuality. Realising it is the first step in an appropriate strategy, regardless of the organization for which you are responsible, whether it is the State, the armed forces or a company.

Les opinions exprimées ici n'engagent que la responsabilité de leur auteur.

La Fondation pour la Recherche Stratégique est une fondation reconnue d'utilité publique. Centre de recherche indépendant, elle réalise des études pour les ministères et agences français, les institutions européennes, les organisations internationales et les entreprises. Elle contribue au débat stratégique en France et à l'étranger.

WWW.FRSTRATEGIE.ORG

4 BIS RUE DES PÂTURES 75016 PARIS TÉL : 01 43 13 77 77 FAX 01 43 13 77 78

ISSN : 2273-4643