CHAIRE DE CYBERDÉFENSE ET CYBERSECURITÉ

Commencement of cyber-weapons

Djamel Metmati

July 2013 – Article n°III.9

If the United States is contributing to cyber-war, by uploading tactical and strategic documentation, it must be noticed that it is causing other countries to tag along. The movement is double, because it unites who stick to the concept of cyber-war and those who consider it still a myth. In addition, the state of the art, in terms of cyber-attacks, shows two different trends. The first indicates a strategic reflection in which attacks are considered a consequence or network spreading. The second trend describes the appearance of reasonable and thought-out cyber-attacks with economic, political and military goals.

However, cyber-attacks exist only through a weapon. And this weapon can be designed through a specific and more or less complex method, for its design and implementation, according to the sought effects. Most of the current attacks resemble "gerra"[1], those states of violence produced by organizations and non-state groups. The waning of conventional conflicts suggests that the forms of violence are multiplying. This phenomenon, boosted by the development of networks intertwined with societies and economies, announces a redistribution of violence, with new parameters.

Cyberspace embodies this process by integrating this type of violence, using unprecedented modi operandi with identical effects. The question is therefore how cyber can be used as a weapon, all the more because the observation of the network situation leads to a mix of "gerra"[1] with states' wish to restore the principle of monopoly in the exercise of lawful violence, in defensive and offensive capacities.

The establishment of the Tallinn manual, an international text which broaches international law in cyber-warfare, indirectly defines the use of offensive and defensive actions within cyberspace, on the basis of regulations which aims at limiting possible actions, in the course of militarizing cyberspace. This means, in the end, that weapons exist and that their actions combined by a state and non-state organization partakes in the modification of the military-natured action, by transferring combat rationale into networks.

To illustrate this point, cyber-weapons are processes coming from computer programs, created or existing which answer to military modi operandi, in the sought effects. They rely on national security strategies, on the basis of direct actions within networks or combined to armed forces' maneuvers in a destruction/interception and detection/discretion.

[1] Frédéric Gros, États de violence. Essai sur la fin de la guerre. Paris, Gallimard, 2006, 310p.

I – Conception principles

Thomas Rid's[2] and Peter McBurney's approach gives a general but restrictive frame of work for the cyber-weapon, but without associating to it, in its « network » dimension, the actors and targets of cyber-operations. This characteristic, which defines our societies today, sees in a cyber-weapon anything that can be used as a weapon with the cyber-environment.

These two authors define cyber-weapons as "*a code used or conceived to threaten or cause physical, functional or psychological harm to structures, systems or human beings*[3] *"*. This weapon is assessed according to three potential levels: poorly potential[4], strongly potential[5], and a combination of the two[6].

These levels qualify an attack, which can range from service denial to the destruction of computers[7]. Technology therefore reflects the theoretical power of the weapon. However, the assessment criteria used to define potential depend on the desired effects and on the final product expected to hit the targets. The technical level of the weapon only defines its potential power, which will only be validated by implementation, on the basis of plans which include other vectors.

A cyber-weapon is therefore the product of the technical level combined to its targets, multiplied by the network in which it is intended to operate. In this case, the systemic approach in the design and execution of a weapon gives it its form, its power, its life expectation in a defined time-frame.

Given that a cyber-weapon doesn't outlive the evolving characteristics of defensive weapons, planning and coordination remain essential to assess the "TAZ"[8], so to launch an attack from a weak point which can be strengthened by the defense in a shorter lapse of time. The cyber-weapon fills a set of criteria, such as: the objective, the "Find and fix", the technical aspects, the use tactics, the "TAZ"[9], the closure.

The result comes from a team of developers who develop the weapon according to sector-specific vulnerabilities, identified through the mapping out of the opposing party. This method follows an attack implementation process which relies on the technical part as much as on the human part. Upstream, open intelligence gathering on the basis of combining data, useless by itself, gives the cyber-weapon its typology.

By gathering data in a specific period of time, corresponding to the sought effect in a specific situation, data-mining[10] enables the construction of the attack plan, in which the upstream analysis, of the potential, related to human and technical vulnerabilities, make the reachable targets converge to achieve the sought effect at a given time. Like principles ruling over ad-hoc networks, the cyber-weapon is a code but finds its place within an existing and desired action towards the target[11]. A cyber-weapon is built on the basis of job-related and human vulnerabilities

[2] Thomas Rid,Cyberwar will not take place. Hurst/Oxford University press, 2013.

[3] This definition from Thomas Rid introduces the cultural and technical aspect of the cyber-weapon through the use of same-nature codes.

[4] Denial of Service.

[5] Flame-type viruses.

[6] A major attack is announced by warning shots, in the form of Denial of Service.

[7] In 2012, the Shamoon virus infected the Saudi oil company Aramco, and caused the destruction of 35 000 computers.

[8] Autonomous temporary zone : A technique which enables mastering network streams for a given time.

[9] Hakim Bey

[10] A technique which makes multiple data converge in order to make hidden sense out of it.

[11] The Flame virus example.

by seeking alteration. It attacks both weak and strong points of human-machine systems[12].

The system perception, on the defense side, is different from that on the attacker's side. The confrontation of friend/foe action modes defines the notion of strong and weak points. The result is a balance of powers which can be measured in vulnerabilities. The advantage of one on the other then hinges on the imagination and readiness to strike hard and fast, while remaining constantly in movement. In that case, planning, possible scenarios and their updates remain paramount[13].

Once the attack opportunities come out of the analysis phase, the cyber-weapon can be thought out and designed. To create it, the gap market shapes the potential of the cyber-weapon by enabling the compression of the creation time of the attack program. It reflects the state-of-the-art and fosters destructive effects by combining, all the more because societies entrust networks with part of their running processes[14]. Computers, telephones and tabs have become, for instance, the modern day's shopping cart.

If the industrial revolution of the 19th century led to a shift in armament, with greater firepower and range at hand, cybernetics today renders weapons even more powerful by diminishing their volume while maintaining their effects. Cyber does not escape this process; the developed weapons are all the more powerful that networks grow and connect to people and objects[15]. Makeshift "network" attacks against systems give way here forth to more sophisticated[16] weapons, involving developer teams. Their leaders include them within maneuvers which, according to the circumstances, be part of a conventional military operation.

In the opposite case, its action on networks stems from a political choice, where a state- or non-state-organization wishes to perform a low-cost operation, with identical effects, without placing itself under international law[17].

I I- Creation principles

Whether he belong to a state or non state organization, it is the cyber-fighter's job to tactically achieve what is possible, on the basis of a strategy chosen by an organized entity. Then comes the technological and organizational phase of the weapon, with the objective.

The cyber-weapon stems from a direct or indirect strategy, according to the engagement, type of chosen target which corresponds to the different brackets of the "pipe", that is : psychology, information, physics and electronics. This covers three types of enemy: state entities, vital organizations and industrial facilities or small to medium companies which behold the targets necessary to produce the effect.

The technological danger for the cyber-weapon lies in creating a purely technical product, or even a commercial one, on the basis of an identified gap, usually coming from the feat market.

[12] The open web application security enables the visualization of existing gaps on the web.

[13] This method consists in ranking one's own gaps and attack opportunities, on the basis of an analysis, with a dedicated workgroup.

[14] Web sales jumped 14% in the first quarter.

[15] According to Thierry Berthier, transversal spreading of algorithms has an effect on every aspect of human life.

[16] The sKywiper virus bundles malware programs, keyloggers, file misconfiguration, local-share infections, Stuxnet feats and DLL.

[17] In the case of Flame, with Iranian centrifuges.

Oppositely, it is the developer's job to produce a defense or attack algorithm, which will take its place within the coordination designed for the attack.

The military aspect is one of the most sophisticated facets of the cyber-weapon, because it can mobilize state resources, which other entities would never have. This is because, facing threats and risks, the state is the first line of defense or the first echelon. Whether it be efficient or permeable, the weapon's effect suggests a new dimension within the military operation. Be it Flame, the Aramco case, or naval exercises simulating network attacks, they rely on a presumable and verified plan.

However, other cyber-operations use cyber weapons use psychological cyber-weapons, with speeches and rumors, which the media vector reinforces. The Cahuzac case, revealed by Mediapart shows that this type of weapon produces a technical effect on networks[18] and also takes the shape of a disruption in the balance of powers between entities exclusively through the social psychology linked to networks.

The production of cyber-weapons doesn't come exclusively from states, as the cyber-defense economy, which is booming, stands on a market in which computer security firms operate. For the moment, they seem the fittest to follow up and offer attack and defense solutions for individuals, companies and public administrations.

The command of the code is a key point for the constitution of a cyber-weapon. It determines the technical level, which depends on the target. This comprehension of the target determines the effect of the cyber-weapons and efficient counter-measures. This technology lies in an underground cyber-armament economy[19] which must not fall into the monopoly of criminal organizations.

In that perspective, security firms no longer appear as threat illustrators. They now have the job to detect and create counter-measures, facing cyber-weapons. A company such as HTTPCS detects, on average, 3000 breaches per day, 30% of which being critical or very critical. Moreover, as some military equipment relies on dual technology, this type of company is part of classic armament industry. Thus, Kaspersky[20] detected that the Skygrabber program enabled the interception in 2012 of an American drone in Iranian air space. States therefore have two solutions. The former consists in calling upon this type of company to develop their defense and attack software programs. The latter wold lead to encouraging the creation of public interest companies, similar to defense companies, in order to detain a deterring and reactive striking force, exclusively dedicated to the defense of the nation's vital interests.

To the advantage of weapons which pre-exist and are not centralized in a digital heart, cyber-warriors form varied profiles in the conception and execution of the weapon. A team of this type concentrates network specialists, systems, developers, watchmen, analysts and a coordinator, keeping the whole system together.

Insofar as cyber tends to equalize online structures, virtual action modes tend to take the shape of those used in the real world, with two modes: aggression and hunting. They are either operated within networks or in support of a conventional military operation.

To counter the superior imagination of the attacker on the defender, the offensive or defensive weapon aims at an objective which carries an effect to produce onto the networks, or which the network enables on the real-life situation. It manifests with the possible realization of the weapon's reach, on the basis of a TAZ, designed for the attack.

[18] Online publishing or website modification.

[19] Underground web, through the Tor network.

[20] A Russian company named after its founder.

It then is discrete or brutal, according to the chosen mode of action. The attack may have no "pipe[21]" effect, regarding the perception the individual has of the machine or the system, its declination into other styles of use is created with the surprise effect. Therefore, aggression, hunting or active defense are along those lines. If the cybernetic weapon is accurate by nature, it can be autonomous, due to networks cross-connections and the links between the individuals who use them.

For a weapon to express itself in the network, it needs a sought final effect. The attack induces differentiated forms of movement and of weapon types. The aggression declines a high-potential weapon aiming at the destruction or deliberate paralysis of an organization's running. In this case, the weapon is the product of professional vulnerabilities of the targeted system. Which implies an accurate human and technical mapping out of the target. The hampering of the nuclear program, through the logical destruction of the coordinated rhythm of the Iranian centrifuges with the Flame virus is built on the basis of a program targeting industrial processes, the vector of which remains the individual.

The hunt is a target-seeking stance, to multiply the effects of a primary action. The corresponding program will aim at collecting data to cross-check them with others. The result will enable the building of a larger attack or will supply elements for air strikes, land or naval actions.

To these declinations should be added the theatres of operations on which the weapons express themselves. Be it by the network or in the networks, a cyber-weapon receives a "TAZ[22]" to generate its effect. In this context, the attacker chooses the moment and the defender chooses the place for the confrontation. He remains free, under the condition that he have an in-depth and active defense system and a line onto which he can place it[23].

The cyber-weapon is therefore a program characterized by technical command and human organization knowledge. Yet, its effect goes beyond the network's physical limits.

It also broaches the individuas' psychology. This raises several problems, the main being the idea of cyber-armament proliferation and the future role of security companies. The qualitative and quantitative increase in cyber-attack suggests they are militarizing. This trend induces the introduction of tactical cyber-weapons in conventional operations. By doing so, cyber joins ancient military practice by letting it perform better, and making it innovating in the conception, command and execution of an operation[24]. It would assist the lethal weapons which the currently evolving international law would change into a destructive weapon, recognized and accepted.

[21] Psychological, information, physical, électronic.

[22] Temporary autonomous zone.

[23] Honeypoot, firewall, redundant network architecture.

[24] A bandwidth saturation in enemy tactical networks can, for example, counter its capacity to maneuver. See the CAC concept from the Marine Corps.