« Cyber warfare » and « cyberattacks »: the reality on the ground

“How can cyberattacks paralyse a country?”

Eric Filiol efiliol@netc.fr

ESIEA – CNS/(C+ V)^{O} Laboratory

Over the last decade, armed forces and their governments all around the world – at the instigation of the United States – have begun to reflect upon the evolution of the war concept and more precisely on cyber warfare. It comes out from their discussions that future wars would mainly take place on digital space: attacks would use malicious codes or zero day exploits. From the perspectives, cyber weapons such as like Stuxnet, Aurora , Duqu, Regin, Babar or GrayFish[1] are the most significant and dangerous innovation in the 21 st century.

Barely a day goes by without officials or experts boasting about the unprecedented destructive capabilities of the new digital weapons. Some of them premise an apocalypse. This allegedly “sword of Damoclès” hanging over our heads appears as a pretext for requesting a substantial increase in budget allocation for this new form of warfare. It brings with it paradigm shifts in military doctrine (from strategy to tactics aspects), in military industry sector. This perception also modifies the existing ethical approach to issues of war and peace.

The mass hysteria developed around cyber warfare is supported by various communities (especially the academic one) who wish to take advantage of emerging opportunities in the global cyber security market [1]. Indeed, this conception of cyber warfare is illusory, wrong and even dangerous insofar it puts aside many unsolved essential security issues that will undoubtedly make our societies vulnerable. This view is a heresy enhanced by opportunistic and blind people.

Let us have a closer look at the dangers associated with this view:

- The digital dimension –term more appropriate than the word “cyber” which was awkwardly borrowed from the Wiener’s works [2] – of modern wars in only an additional dimension within the Art of War but in no case, it can be considered as the sole dimension. The essential act of any war is to capture enemy’s resources and to have an ultimate impact on the real sphere. The scenario was the same when aircrafts and air forces were used for military purposes early in the 20th century; there were first a strong belief that military aircrafts were a wonderful opportunity to achieve and maintain complete battlefield supremacy. The historical events showed that, contrary to the expectations, military aircrafts were essential to win air battles but not wars and that it was just an additional dimension to naval and ground forces. Recent historical

[1] It is worth mentioning that the underlying malware techniques used in those allegedly “modern” malware are known for a longer time than often mentioned in the press. As an example, the author in 2003 developed malware which were directly implemented in the BIOS of a motherboard.

events clearly demonstrated that American air strikes were simply not sufficient to win the war against Daesh in Syria for example.

The same scenario is in play with cyber warfare and this time again, it will be an additional dimension to land, air and sea warfare.

- Contemporary conflicts (for instance, in Ukrainia, Irak, Syria, Africa) and the ever-growing terrorist threat show that conventional wars take precedence over cyber warfare. The cyber dimension is only a supporting player in the theater of war.

  Paradoxically, cyber wars take place during "peacetime" periods and mainly involve protagonists from the G-20 member countries. In this context, digital attacks happen in countries in dispute (state vs. state conflicts like China vs. the United States, Russia vs. Nato..) that causes a permanent state of global instability. Cyberwar is bound to be more a peacetime war.
- Digital attacks are a real threat but large-scale attacks in the real life proved to be inefficient. A successful digital large-scale attack on a computer fleet or a SCADA system requires that, at the same time the attack is launched, there are a number of machines containing the same exploitable flaws or being in a suitable insecure state. However in real life, even if we consider a homogeneous fleet of computers, the rate of variability among computers is high enough to limit the effectiveness and scope of these attacks. Moreover, the delay between the intelligence phase (detecting a potentially exploitable vulnerability) and the maneuver phase (really exploiting the vulnerability) may be too long to insure that the vulnerability will still be exploitable. No experimented chief of war would base his general maneuver on such an uncertainty.

  If we look closer at the famous Stuxnet malware (often quoted as an example) and at the result of its code analysis (which clearly shows the way it was intended to run), there is no evidence that the Stuxnet attack was really successful. According to Iranian officials, the attack was effective but given the historical context in Iran during that time, it cannot be ruled out that Iranians had a vested interest in making believe that their nuclear program was delayed by Stuxnet. This is a typical example of what NATO countries call "InfoOps" (information operations), an area which is unfortunately not taken sufficiently into account in cyber warfare.

- Unlike conventional attacks whose effects can be mostly contained and forecast, cyberattacks may have extensive and unpredictable consequences even for attackers[2]. Over time, the Internet has become an integral part of our lives but in the meantime, it has grown complex and today no one would be able to draw an exhaustive functional map due to its size, complexity and ever changing structure. As an illustration, over the first months of the US intervention in Afghanistan, the American Headquarters planned to carry out an attack against the Afghan phone networks (mobile phone mast) as the mobile phone networks were a key battleground in the war against the Talibans. As the damages on the infrastructures would have prevented American soldiers to make personal calls, the operation was cancelled for fear of lowering the soldiers' morale

[2] In this respect, cyber warfare has many similarities with biological/nuclear warfare.

(while abroad, military personnel, when not in duty, mostly use local infrastructure for their private communications).

- From a human, ethical and philosophical point of view, the concept of cyber warfare, as it is seen today, ultimately aims at calling into question the traditional ethics of the war: as a first rule in a conventional war, all soldiers are equally vulnerable and equally innocent; soldiers play a fair game: as a principle, they kill enemies and accept to be killed. As a second rule, in a conventional war context, protagonists are military experts who strike military targets.

  In contrast to conventional/classic war, cyber warfare is essentially asymmetric: attacks are perpetrated by the few upon the many and no differentiation is made between soldiers and civilians. Attackers are also all powerful whereas civilians are vulnerable targets.

  The concept of cyber warfare is obviously similar with that of the so-called inglorious *Zero-dead war* doctrine which was popularized by the United States during the Gulf War. The use of drones monitored by pot-bellied military operators located in Arkansas aimed at shooting and killing afghan or Iraqi civilians was deeply shocking [3]. In the near future, it is likely that attacks launched by elite-hackers secretly hidden behind computer screens will be quite common. It is a step further towards what we can call “a coward’s war”.

- To end, the concept of cyber warfare is dangerous insofar it can deeply undermine the Internet and Western countries (especially civil society) which become very dependent on the Internet. In order cyber warfare may be viable and efficient, governments need to ensure a continual insecurity on the Internet and take advantage of 0-day exploits, attack tools, unsecure protocols, weak digital industrial facilities…. This permanent and global state is insecurity is enforced through the control of IT technology by the nation states and the USA in the first place due to its nearly monopolistic power over the IT world [4].

  However, this policy is not consistent with one of the sovereign functions of the States – especially about the safety and security of its population, its territory or the one of allied foreign countries (Europe, NATO…). In addition, this policy may affect the function of wars as it is seen by governments: whereas the democratic countries consider conventional war as the last but necessary solution to maintain peace (or get back to it), cyber wars build on a constant digital instability environment.

Even though the perception of the cyber warfare offers a sharp contrast with the reality on the ground and our traditional ethical values, this is a real threat to our security. Contrary to what is generally believed, cyber offensives are not much involved in military maneuvers and just act as a support to conventional military operations (the attack, dubbed *“*Operation Orchard*,”* [5] is very illustrative in this regards). Undoubtedly, cyberattacks play a key role in information gathering (intelligence phase) process or strategic planning [6].

The goal of this paper[3] is to show how the cyber dimension can effectively cause huge damage on large-scale infrastructures using both conventional approaches and few perpetrators. In a word, it explains that cyberattacks perpetrated by only a few people may be as damaging as conventional wars waged by an entire military division.

How can cyberattacks cripple a whole country?

The main principle is based on the combination of the concept of Open data (information freely available to everyone) and Big Data techniques (huge volume of information is processed using data mining). However, it may include targeted attacks (cyberattacks or not) designed to collect additional information that is not openly accessible. Attackers first choose a target, and then select the kind of effect they wish to create on the target while assessing a probability of success. Once it is done, they choose the most suitable attack methodology. If the attack is launched against a country or a large-scale infrastructure, the action is likely to be complex, made of different steps involving both conventional or possibly cyber operations. The efficiency rate of operations closely depends on the weakest link: in most cases, the probability of success may be affected when cyber operations are involved (CNO or CNA[4]).

The vulnerability of modern nations is not so much due to our digital technology addiction but to the huge amount of data of any kind available on the Internet. The information collected as a first step, will enable attackers to identify vulnerabilities that can be easily exploited in order to build up appropriate tactical scenarios.

Two different kinds of information and intelligence are available:

- Open data -which account for about 70 percent of all information - only requires to be collected, crossed-checked, compiled and suitably sorted. During the planning phase of an attack, massive and accurate geographical location data is needed and can be found via Google Earth and Consort. Blogs, twitters and a wide range of social networks like Facebook [7] are very useful when it comes to collect information about people. By nature, all data is worthy of consideration but must be selected according to the attack context.
- Hidden data (about 25 percent of all information) is located either in metadata (data embedded in document format such as geolocation data in pictures) or can be obtained through data mining process that provides invisible and often sensitive information from open data.

Other data (about 5 percent of all information) refers to confidential or classified information obtained through common spying methods (mostly but through cyber approaches as well). Massive and systematic collection of data or metadata, and its process (carried out by programs like PRISM) is not a matter of pure coincidence. It is essential.

[3] This paper is a summary of our research conducted from early 2013 to mid-2014 with fourth-year ESIEA students (who wish to remain anonymous).

[4] Computer Network operation, Computer Network Attacks (NATO terminology)

In 2013 and 2014, we made a large-scale study to assess the real importance of the cyber-dimension in current attacks (detailed results of the study have not been released yet). Other preliminary surveys were published in [8, 9].

In this study, we chose, as a target area, the western part of the United States (including California which ranks as world's 8th largest economy in 2015). The intended purpose was to take down the electrical power grid in this part of the U.S. The desired effect was to create a blackout of at least two days[5]. It is essential for the reader to keep in mind both the above target and effect on target to understand the following statement:

- Even if we are not aware of it, the supply of electricity is of vital importance in today's society. When disrupted, everything associated with the cyber space becomes useless as emergency backup power generator systems are not sufficient to provide an entire territory with electricity.
- Any attack starts with an initial strike followed by a "knock-on "effect due to various factors associated with the target (human, technical, services..) and their interactions [6]. In big cities, riots, vandalism and disturbances usually take place within the first few hours after the beginning of a general blackout. The result is often a mass hysteria among the population that delays the task of utility workers to restore power and get things back to normal. That situation may have a global bad impact on economies (drastic fall of the Nasdaq index, drops in U.S. and global stocks markets and even the social stability of countries. This makes electrical grids a prime target for cyberattacks and makes the consequences of a successful attack even more severe.

In most industrialized countries, electrical grids are aging infrastructures which make them vulnerable –not to say highly vulnerable-. The U.S power grid system is very illustrative in this regards. When American engineers designed transmission networks some decades ago, they had to face both geographical constraints imposed by the country's size and landscape (mountainous terrains for example) and financial constraints (in contrast to Europe, the U.S electrical grid is mostly owned by private companies[6]). Basic power grid systems, aging control systems, the primacy of economic considerations over national security, all make the U.S. power grid a relatively soft target for attackers. These are the key points that can be easily exploited by attackers. Similar security concerns also exist for other "critical infrastructures" such as railway networks, ports, roads, dams, bridges and so on...

As a first step, the **intelligence phase** consisted in:

- Mapping the U.S. electrical grid (including generating stations, transmission lines, distribution lines, sub-stations…). It is very important to identify the sections of the grid which correspond to redundant sources or logistic support between the three main U.S. electrical areas (western, eastern parts and Texas area).

[5] Some coordinated cyberattacks have been launched against the US power grid over the last two years (see [10])

[6] The existing power grid system in the U.S. is inadequate in terms of reliability, power quality, and efficiency and prohibitively expensive to overhaul.

- Gathering technical data on critical infrastructures such as nuclear plants, especially their external electrical grid or their emergency back-up generators which are vital facilities not only to ensure the proper functioning of the nuclear plant but also in case of emergency situations (*cooling system).*
- Collecting and analyzing various types of other openly available data:
    - ✓ Road system (identification of the roads which are close to the power infrastructure, and details about special road/traffic regulations around the sites (for example, the vehicle weight and dimension regulations).
    - ✓ Sitemap and data on the security system of the infrastructure (monitoring system) (see Picture 1)
    - ✓ Data on Response units (rescue teams, firefighters, police, army, national guard…) and also various data such as the number of people working on the spot, the kind of facilities or past incidents recorded from the press for instance.
    - ✓ Data on weather conditions and its impact on possible rescue operations ...The time when the attack is launched, is as important as the manoeuver itself. As an illustrative example, attacks that take place in winter or during a heat wave – when the electricity consumption is high- will maximize the final effects.
    - ✓ Any helpful detail to plan the attack and increase its success probability.

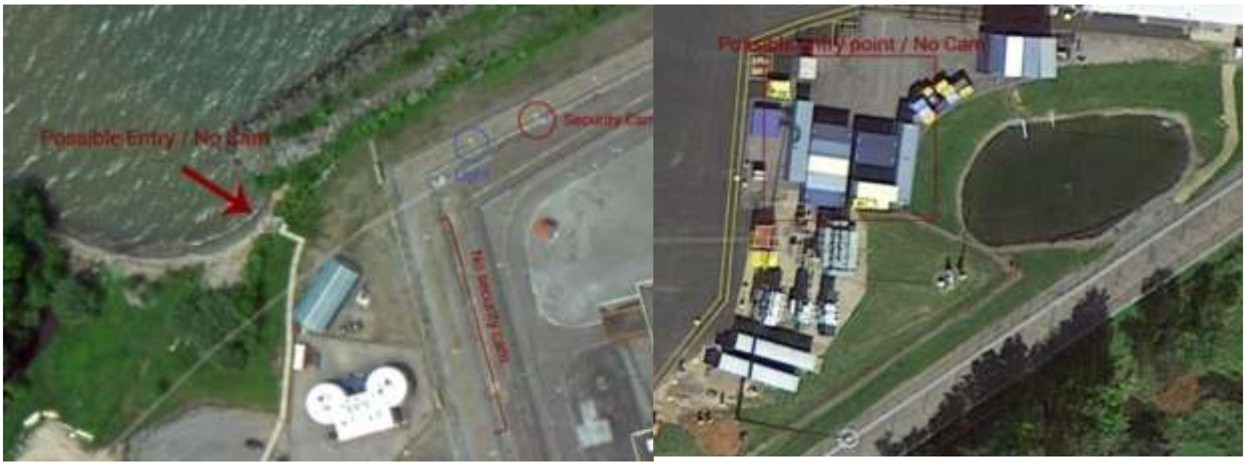

Figure 1.- Information about security aspects in two major nuclear plants in the USA.

The **planning step** then consists in building a scenario, in identifying the forces involved, in gathering the human, material and logistics resources to use. We developed mathematical models to process all the information before implementing them on a software platform (a French company called ARX Defense is currently carried out the industrial software development). The purpose is to identify vulnerabilities easily, to develop operational scenarios (attack models, possible path to attack), in order to create a “knock-on effect” and consequently inflict maximum damage. From the attacker’s point of view, it also means minimal costs and minimal risks. This step determines if there is a need for additional cyberattacks and envisages all the necessary planning details.

Here are the main steps and results of the study we carried out on the US power grid:

- As a first step, we identified a few dozen of relevant facilities (electrical pylons and towers, substations…) and we selected the facilities that could be of interest to attackers. For example, we spotted areas of difficult access for trucks or helicopters, facilities for which incident detection and repairs are difficult. We then drew up a graph (see a virtual example on Picture 2) which has a sparse and very simple structure due to the nature of the electrical grid. As you can see it on the picture, it describes a weak instance.

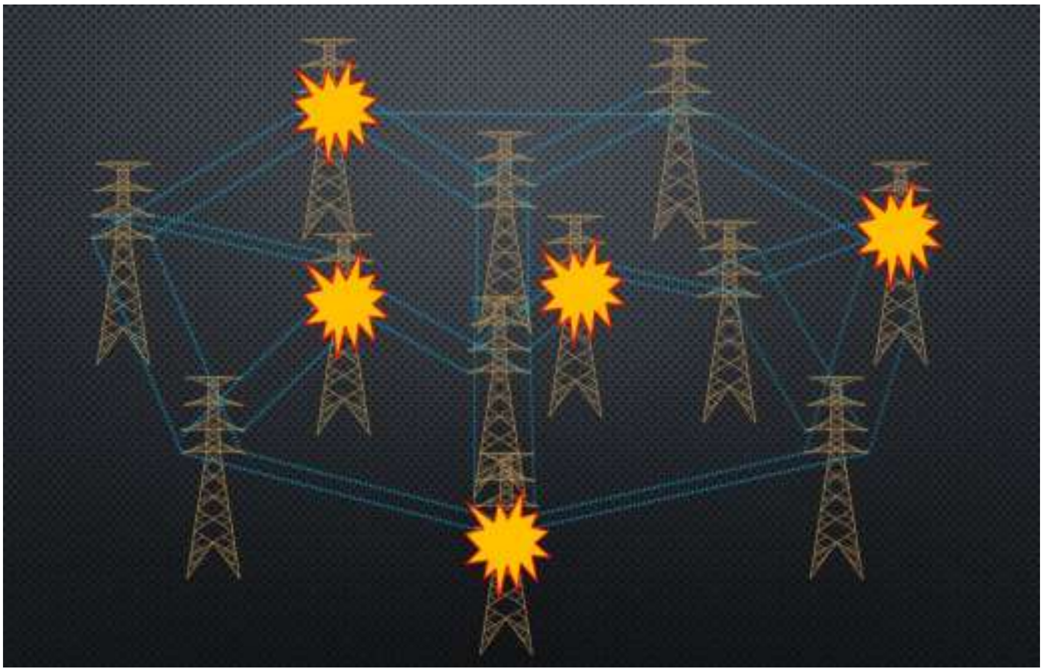

Figure 2.- Graph which describes an electric grid (fictive case) et the five critical nodes (vertex cover) in this graph.

- To complement our study, we decided as a second step, to use the so-called "*Vertex Cover Algorithm*" [12]. The goal was to identify the minimal set of graph nodes to be destroyed in order to get a global impact on the whole graph. There are, of course, other possible combinatorial approaches and structures depending on the kind of attacks, targets, the desired impact, the operational context you select, for instance, networks for security surveillance cameras [11]).

The **attack step** can be carried out by a relatively small group of persons (members of the group do not know each other) using the means available on site[7]. It is even possible to choose two target groups while deploying several operational teams on the ground. This

[7] This aspect requires considering the target's culture: In the U.S., it is easier to get explosives and firearms than in Europe that is the reason why the strategy must be different.

enables to maximize the probability of success (operational redundancy) while minimizing operational risks.

Conclusion

Even if cyberattacks will undoubtedly play an important role in the future, it is unlikely that they will represent the sole dimension in future attacks as some people claim. Cyberattacks using malware or other digital tools are not sufficient to carry out large-scale attacks successfully just because they need to be incredibly sophisticated (from a technological point of view) to cause significant damage. So far, very few successful large-scale cyberattacks on critical infrastructures have been recorded.

However, the cyber-dimension proves to be both immensely effective and threatening when it comes to plan attacks and especially during the intelligence and planning steps. With the ever-growing amount of operational data available on the Internet, collecting, processing, analyzing information has become extremely easy. The tools of *Big data combined* with increasingly *Open data* constitute the biggest threat as it enables attackers to get the necessary information to attack successfully critical infrastructures while using limited conventional means.

In this study, we identified other existing large areas of vulnerabilities across the world. As an illustrative example, attackers could use a “knock-on effect“ to launch an attack against a country that would affect another country’s interests (In some areas of China, existing security breaches in critical infrastructures can have a negative impact on European economies). To exploit this vulnerability, attackers just have to inquire about existing patterns of dominance and dependency across the world, be it of economic, structural, political nature.

In this respect, our study shows that if our governments are aware that there is a vital need to protect critical infrastructures, they find it hard to determine which are truly critical among those which are just important. It also demonstrates that there is not reliable mapping of functional dependencies between infrastructure components or between economies.

Bibliography

[1] Thomas Rid (2013) *Cyberwar will not place place*. Oxford University Press.

[2] Norber Wiener (1948). *Cybernetics or Control and Communication in the Animal and the Machine.* The MIT Press

[3] Grégoire Chamayou (2013). *La théorie du drone*. Editions la Fabrique.

[4] Eric Filiol. "*The Control of technology by Nation States: Past, Present and Future - The Case of Cryptology and Information Security*". Journal in Information Warfare, Vol. 12, Issue 3, October 2013

[5] http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html

[6] Eric Filiol (2011). "*Operational Aspects of a Cyberattack: Intelligence, Planning and Conduct*", chapter of the book edited by D. Ventre "Cyberwar and Information Warfare", ISTE, Wiley.

[7] http://www.lemonde.fr/proche-orient/article/2010/03/03/tsahal-annule-une-operation-apres-une-fuite-sur-facebook_1313918_3218.html

[8] Eric Filiol and F. Raynal (2009). "*Cyberguerre : de l'attaque du bunker à l'attaque dans la profondeur*". *Revue de Défense Nationale et Sécurité Collective*, volume 2009-3, pp. 74--86, mars 2009.

[9] Eric Filiol (2011). *Operational aspects of Cyberwarfare or Cyber-Terrorist Attacks: What a Truly Devastating Attack Could Do*". In Leading Issues in Information Warfare & Security Research, Volume 1, pp. 36--53, Julie Ryan Editor, Academic Publishing International Ltd.

[10] Rebecca Smith (2014). Assault on California Power Station Raises Alarm on Potential for Terrorism. The Wall Street Journal , February 4th, 2014. http://www.wsj.com/news/articles/SB10001424052702304851104579359141941621778

[11] Eric Filiol et Thibaut Scherrer (2013). *Securing Cities with CCTV? Not so Sure - A Urban Guerilla Perspective*" with Thibaut Scherrer. La nuit du Hack (NDH'2013), June 22nd 23rd, 2013, Paris

[12] Ashay Dharwadker (2006). *The Vertex Cover Algorithm*, http://www.dharwadker.org/vertex_cover/ and Proceedings of Institute of Mathematics, 2011.