

## **Operational aspects of cyberwarfare or cyber-terrorist attacks: what a truly devastating attack could do**

LCL Eric Filiol (ret)  
ESIEA - Operational virology and cryptology laboratory  
38 rue des Dr Calmette et Guérin 53000 Laval, France  
[filiol@esiea.fr](mailto:filiol@esiea.fr)

**Abstract:** Cyberwarfare and cyber-terrorism (mainly e-jihad) are nowadays a fashion topic. Since the Estonian attack in May 2007 and some intents of computer attacks by Al-Qaida, many papers have addressed, discussed not so say disputed about this. But those papers, for the most interesting ones, have just explained the effects of those attacks, drawn some conclusion and give only a very few technical details. But no paper has ever presented and pro-actively addressed the problem of operational and planning aspects of such cyber-attacks. In other words, how a terrorist group or a nation state could plan, organize, launch and conduct a real, large scale attacks? In this paper we present an in-depth reflection of how an attacker could plan such a wide-scale attack against a country, its infrastructure and its population, simply with a few clicks of a mouse. Based on real-cases analysis, military planning techniques and technical proactive research, we present a multi-step attack with the operational planning in mind (e.g. the attacker's view) without forgetting to explain how to technically execute each of the different phases of the attack. We will restrict to the case of attacks against a nation state conducted by a terrorist group or another country.

**Keywords:** Computer warfare – Cyber war – Cyber terrorism – Critical infrastructure – Attack against people – Disinformation – Information Operations. .

### **1 Introduction**

Cyberwarfare has nowadays become a fashion topic and it is quite impossible nowadays to count them. However most of them share quite the same misleading idea: cyberwarfare is a war on the cyberworld (i.e. the set of all of the computers systems, communication system, networks infrastructure...) only and against that cyberworld only. While there is no real clear and widely accepted definition of what cyberwarfare really is, quite almost everybody seems to agree on the fact that this kind of war is naturally disconnected from any other reality and to begin with, with the real world at first. There is no such thing as a digital only war as we will try to explain in this paper. As a consequence of this misleading idea comes the fact that the real targets of computer attacks are largely underestimated thus making our countries far from being protected. Moreover, while there is a beginning of consensus about a few tools that could be technically exploited to conduct computer warfare – malware, software flaws, network attacks ...- there is no deep reflection on how such an organized attack against a nation state could be planned and conducted. What NATO calls CNOs (*Computer Network Operations*) [NATO], still remain vague, fuzzy, imprecise and rather restricted.

In this paper, we first aim at identifying the different possible targets and methods of cyber warfare. In this respect, the analysis has been clearly inspired by the Chinese doctrine (Qiao & Wang, 1999) which seems to have been applied in computer attacks during the recent months, as far as facts and reports enable to have a precise idea. But at the present time, know digital attacks are just digital skirmishes against a few yet critical networks (mainly defence networks from USA or Western countries for espionage or Denial of Service purposes). It is very likely that those skirmishes should be considered just as local technical repetitions of chunks of a bigger, wider attack, whose overall complexity can be neither perceived nor analysed.

Here comes the second critical point with respect to cyberwarfare: operational and planning aspects of such a war from the attackers' perspective. In other words, how a terrorist group or a nation state could plan, organize, launch and conduct a real, mid scale or large scale attack? What does he need for that? In this paper we present an in-depth reflection of how an attacker could plan such a wide-scale attack against a country, its infrastructure and its population, simply with a few clicks of a mouse. Our study is based on real-cases analysis (forensics analysis of legal cases, targeted attacks analysis) military planning techniques and technical proactive research, we present a multi-step attack with the operational planning in mind (e.g. the attacker's view) without forgetting to explain how to technically execute each of the different phases of the attack. We will restrict to the specific case of attacks

conducted against a nation state, by a terrorist group or another country, for internal destabilization purpose. The case of cyber-attacks conducted in the context of military operations will not be addressed but the reader may refer to (Filiol, 2008).

The paper is organized as follows. Section 2 will shortly present the different concepts behind the notion of war and to what extent cyber attacks can interfere with those concepts. We will in particular explain why a war in the cyberspace only, is a nonsense. Section 3 then presents a "simple" tactical scenario to illustrate our approach. First the theme itself will be given and then we will detail the course of events as any newspaper reader could observe them: as a sequence of apparently uncoordinated, unrelated events. Finally, in section 4 we go behind the curtain to explain what really happened and present the previous sequence of events as the steps of a planned, organized computer attack with a true conduct of manoeuvre as military use to do.

## **2 Basic concepts of war and computer warfare.**

### **2.1 Introductory concepts in computer warfare**

The general prevailing security concept considers that a critical system must be "bunkerized" to withstand attacks. But this is a very bad interpretation of the main existing security models. Furthermore it is never possible to ascertain the actual optimality of this approach, it is conceptually wrong. Indeed, it implies to subscribe to the belief that security is to prevent attacks - which is nonsense - while its true role is to be able to identify as quickly as possible such attacks, to move in conditions, time to restore the system and especially to leave the priority at the heart of business (industrial world) or the operational mission (military). In other words, security must consider a risk management approach and an in depth rather than a sanctuary policy.

But if this vision of defence in depth is becoming - particularly in the world of Defence and of governmental offices in the face of attacks whose number is increasing month after month - it is still very limited in scope. The perspective of the depth limit remains compartmentalized to the walls of the sanctuary: it makes more interior walls in the hope that if the wall falls outside the sanctuary is still preserved. This is an unfortunately narrow vision of security (Filiol, 2009). In a context of cyberwar, it would be a fatal, misleading sense of security. While in a conventional conflict, the enemy must eventually deal directly with a target (final phase of the battle ground after the air raids, for example) and bring down a sanctuary, in the context of cyberwarfare, it is no longer true. The target is in one way or another interconnected with other components according to a mapping and an interdependence that is often impossible to specify ... except for the enemy.

The digitization of our space, it is "battle" or social causes, to our security, the abolition of time and space. In a conventional conflict, the target is located in a space and time not only different from that of the attacker, but also from "friendly components (allies)" of the target. This means at the operational management level a graduated conduct of the maneuver for the enemy and protective measures and / or responses for the intended target

An excellent recent example - but unfortunately not only because this type of attack has struck the U.S. Air Force a few months ago - comes from the attack by the worm W32.Conflicker<sup>1</sup>, attack that hit the French Defence and the British Navy. On 15 and 16 January (Blog Secret Défense, 2009) Rafale aircrafts from the French Navy Air Force have been nailed to the ground. The attack has not affected their onboard computers – they are a priori highly protected - but the air traffic control system which, under Windows, was attacked and put out of service. He never delivered the flight parameters<sup>2</sup>. The dependence of system did the rest. But this case is exceptional and limited in scope because the dependence is direct and supposedly easily identifiable - at least it would have been expected, and above all it is limited to a purely technical scope. Precisely it is where security still considers a too narrow a vision of the reality of the systems it is supposed to protect. Considering only the purely technical aspect, in identifying the dependencies of a system, is illusory. This is often what one finds in most security and risk analysis methodologies. Moreover, only the immediate area is generally taken into account.

---

<sup>1</sup> The code analysis reveals that the attack apparently originated from Russia or Ukraine.

<sup>2</sup> The same case very recently (January 2009) struck a Chinese battle tank squadron.

The main reason is that since (too) long security based solely on the vision of the defender. Still anathema struck, the vision of the attacker is neglected and as such everything that can be implemented by the latter is ignored. The vision developed by China military experts, from this point of view, especially in advance (Qiao & Wang, 1999). The key element is to have this vision and way of thinking the military in the conduct of the operation: be the approach of infantry and cavalry based on a doctrine of warfare, strongly supported by intelligence. There is no doubt in this approach - and analysis of actual attacks is clear - that intelligence is vital to the cyber attacker. The gathering is to identify these dependencies and to establish their precise mapping. But never in our time, it has been easier to collect information, compiled and cross-gain operational scope. Blogs of military personnel or engineers working on military systems to social networks, through the analysis of tenders for public procurement, the critical mass of information that can easily be collected is staggering and unbelievable. This makes our central intelligence, tools suddenly obsolete and ridiculously vain. One wonders what is the role of internal security agencies (MI5 in UK, FBI in USA, DCRI/DPSD in France...- working very effectively, however - if the authorities and decision-makers do not take into account the risks and threats that those agencies identify every day.

This information, once collected, must be processed to establish the mapping of dependencies to determine the point of weakness and build an operational scenario. This is the central element of genuine thought and doctrine for cyberwar. In the present paper, we are going to expose how a cyber attack could be launched in a more directed towards the safety of territory and civil security, by applying the previous introductory concepts. A similar case in the context of a military operation is presented in (Filiol, 2009).

We must beforehand clarify what the term "cyber attack" means since it is still unclear to many. A commonly accepted definition is (Knowlckedgerush, 2009): *"a strategy for undermining an enemy's data and information systems, while defending and leveraging one's own information edge. This type of war has no front line; potential battlefields are anywhere networked systems can be accessed --oil and gas pipelines, electric power grids, telephone switching networks, etc. Information warfare can take countless forms: trains and planes can be misrouted and caused to collide, stock exchanges can be sabotaged by electronic "sniffers" which disrupt international fund-transfer networks, and the signals of television and radio stations can be jammed and taken over and used for a misinformation campaign"*. However this definition still ticks too much to the technical aspects of computer attacks. That is why in our recent analysis and case studies, we rather favour the following short definition inspired by the French definition of cybercrime: *"part of an attack using conventional means and/or the networks, computer systems or communications infrastructure to act in a dematerialized way so that to get rid off the limits of time and space"*. Thus in our definition – as in the case of cyber crime – computer/network attacks are not a goal in itself but just a tools – among many others, possibly conventional – to control or destroy a given target.

It is essential, in our opinion, to keep in mind that a war purely restricted to the digital world (networks, systems, communication infrastructures...) is an aberration and does not make sense from a military or terrorist point of view. In addition, the specificity of the attack is to operate without the constraints not only of space but also and above all of time. The attacker can act in advance of phase (put its pieces in place in advance like in chess) and especially not to leave any incriminating evidence. Finally, a cyber attack is the optimal combination of Information Operation techniques, as formalized by NATO (Nato, 2006), conventional attacks ... and a total lack of ethics (Qiao & Wang, 1999).

Before illustrating this vision with a tactical scenario, let us first explore the key approach components that a cyber attack could consider.

## **2.2 Key targets in a cyber attacks.**

Let us recall the main characteristics a cyber attack must have according to our definition:

- Dematerialization. In particular, not only the true origin of the attack must remain hidden, but also it must be possible to wrongly frame an innocent party (another country or group) as the perpetrator of the attack (fooling the digital evidence). From a military perspective, the main interest is to avoid or to delay the target reaction by misleading it.

- Cancelling time and space limits. Both factors are generally a strong barrier to bypass for the attacker. Network connections will just make possible to have immediate access from anywhere and at any time.
- Gaining control over time and space, and besides all over physical resources. The aim of war is precisely to gain such a control over the physical world (including people). Attacking a server with no effect over the physical resources has no sense. In other words, cyberwar is not war into the cyberspace, unless the enemy “Nation state” is Second Life! Even defacing a server directly targets the human minds and not just the server.
- Exploit the complexity, interdependencies of modern system. Never attack directly the target which is generally (and hopefully) secure. Attack instead some secondary, ternary... targets whose target is depending and which are not protected, most of the time because the target dependence has not been identified yet. Among those indirect targets, you can consider anything: people or group of people including leaders and decision makers (military or police chiefs, union leader, influence leader...), transportation facilities (train, road, planes...), resources distribution (electricity, water, air conditioning...), communication facilities (telephone, internet, fax...), media... The list is quite infinite when considering the possible chain of interdependencies. As for the attacks against influent people – by wrongly framing them in criminal acts – may be dramatically efficient.
- Exploit generalized intelligence. The efficiency of intelligence – contrary to what most espionage films show – directly lies on the capacity to openly collect a large amount of possibly useless or common data and to compile them in order to have a significant and deep knowledge of a given target. In our modern world of communication, the work has never been so easy: blogs, data centres, relocation of software industry<sup>3</sup> or critical services in low salary countries (as an example, western countries are relocating their telephone call centres and their network supervision centres in north Africa countries where the security conception is far from being the same as our), professional trade shows, analysis of public contract offers, newspapers, professional directories... This list is potentially infinite. Most of those data gathered will be very useful to draw a complete and accurate view of the interdependencies of the final target with some unprotected, unidentified systems, which are less or not protected and therefore which will become secondary targets.

Let us now detail a totally fictitious tactical scenario but in which all elements, all data, all events ... are for the most part inspired by recent events and cases. For obvious reasons of ethics, all of them have been anonymized. Moreover, we will not detail the actual procedure and technical means used by the attackers, directed below. This does not harm the general understanding.

### **3 A “simple” scenario**

#### **3.1 The tactic theme (extracts)**

##### **3.1.1 General situation**

The bidding process for the 20xx Summer Olympic Games was officially launched on May 20yy. The first step for each country was to submit an initial application to the International Olympic Committee (IOC) confirming their intention to bid. Completed official bid files, containing answers to a 25-question IOC form, were to be submitted. Four candidate countries (a city) were chosen for the shortlist on June: BLUE City, YELLOW City, GREEN City, and WHITE City. Two other countries failed to make the cut (RED and PURPLE cities) officially for insufficient preparation and economic problems. But according to unofficial sources, many countries threaten to boycott the event for political reasons. Sir John Doe of RAINBOW country will head the Evaluation Commission. The commission will make on-site inspections in the second quarter of June 20zz. They will issue a comprehensive technical

---

<sup>3</sup> In 2007 – 2008, a large scale espionage case based on Trojan horse hidden in professional software has been discovered in Israel. Those software were also sold in Europe. Let us recall that one of the first critical flaw found in Windows XP in 2001, has been suspected to have been introduced by an Al-Qaida programmer who managed to infiltrate the Microsoft Indian development teams. While no clear evidence has ever been officially given, the doubt still survives. Whatever may the truth, this alleged case poses the problem of software development in countries where the sense of security is not comparable to ours

appraisal for IOC members one month before elections; the final selection will be made by the full IOC membership around mid October 20zz.

In a very uncertain economic environment, and for various reasons linked to the international situation, hosting the Summer Olympic Games represents a strategic interest for the four finalists. The objective of each of these four finalist countries is therefore to discredit the proposals of the other three during the inspections in June 20zz. Moreover, RED and PURPLE countries intend in retaliation to discredit the commission and thus prove that their application was rejected because of political pressures and that the selected countries did not offer the suitable environment for the Summer Olympic Games. All the analysis as well as a few indiscretions in the entourage of the committee strongly and recurrently suggest that only the GREEN and BLUE countries have a genuine chance of being selected. Competition between these two nations, as well as the increase of respective biddings, becomes more and more intense with the approach in June 2009.

### **3.1.2 Environment and intelligence situation**

GREEN and RED countries, as well as RED country, have a significant capacity in the field of CNOS (Computer Network Operation):

- In the GREEN country, many organized groups of pirates (hackers), strongly active e-groups of virus writers working actively for the benefit of the nationalist militia, known to be supported by the former right wing party and a large part of the army.
- In the RED country, state structures, known to drive other groups of hackers are known to have strong activity in terms of attacks; in addition, reports have established that the country handles and manipulates certain groups of hackers of the GREEN.
- The BLUE country has a huge activity in computer warfare both at the national level and at the population level (universities, militia). Moreover, the BLUE country has gained a world monopolistic position in the software industry (95 %) and the chip manufacturing industry (100 %), thus selling its products all around the world.

RED and BLUE countries are known to have a very strong capability in Intelligence. While this capability relates more to HUMINT for the RED country, the BLUE country is more has concentrated its capability on SIGINT, ELINT and COMINT.

The main telephone operator of the GREEN country is owned by the main BLUE operator which manages the supervision of the GREEN communication network (including Internet access and cell phone network). Commercial agreements have resulted in large policy of wide installation of BLUE equipments (in particular network active components and servers). A BLUE consortium is owning and managing most of the GREEN data centers. Finally, governmental GREEN encryption systems have been sold by the RED country<sup>4</sup>.

## **3.2 The course of events**

Let us give first the sequence of events that led to the final selection of the BLUE country by the IOC, without explanation. The core idea is to present this course of events as the reader is bound to perceive them: as the man in the street or the viewer of the prime time news would. In other words, we will present them as a sequence of events without any apparent correlation or any apparent connection. We will then analyze in the next section what really happened.

### **3.2.1 Initial phase: until June 20zz**

At the very beginning of April, recurrent strikes are triggered in the central province of GREEN city according to a phenomenon of slow spreading. Most of the industries, located in the main economic area suffer from a slowdown of their activity. Confidential documents stolen from the main companies were sent on March 26th to a major daily newspaper, which refer to a plan of massive layoffs, motivated by heavy losses of the company, due, according to these documents, to misappropriation of funds for the nationalist and extreme right militia by the different directors of the factories in the area. Forensics investigation on different computer of some companies, which has been ordered by the

---

<sup>4</sup> As surprising as it may be, even in the field of very sensitive systems like national cryptographic equipments, many countries are not independent and consequently buy them to other nation. The Hans Bühler case in 1995 shed a particular shadow on that very specific trade.

financial investigation court on March 27th, has confirmed the veracity of those documents and of the allegation published by the journalists. The activity of the factories progressively stops, including intermittently the production and delivery of electricity in the central province.

On March 31st, two company directors are arrested while two others are fleeing overseas. Investigation are conducted which reveals – through leaks in the press – that a generalized system of corruption for political purposes has been organized. Strikes are becoming harder.

On April 2<sup>nd</sup>, ethnical clashes erupt between gangs in northern part of GREEN city. They are relatively common in those city districts. Cars are burning, many injured with knives and an explosive situation monopolizes the attention of law enforcement. The origin of these conflicts seems related to threats and insults towards ethnic communities that have been posted on *youtube* *dailymotion* websites. Exchange of provocative videos cause a slow rise of tension and street confrontation between gangs until May 25<sup>th</sup>.

On April 16<sup>th</sup>, Mr Alonzo Boïs living in GREEN city is arrested under suspicion of involvement in child pornography. Three days later, after his computer at home has been analysed, the Police has collected a large amount of evidences that he was indeed guilty and he had organized a whole network in the central province of GREEN. A number of people, including some notables from the capital, have been indicted due to their belonging to that network, newspapers said.

The GREEN authorities try to minimize the case and on May 2<sup>nd</sup> a series of documents are sent to international press association which proves that some members of the GREEN government would be involved in this network of child pornography.

### **3.2.2 Phase 2: June 20zz**

As a result of new videos, on June 1st, new clashes in the northern districts of GREEN city and several deaths by firearms are recorded. The situation is tough, the police intervene. The situation is blocked: recurrent demonstrations take place in GREEN city in memory of the victims. Economic activity is disrupted. The authorities fear an escalation of violence.

On June 3<sup>rd</sup>, further investigation by the police, at the request of the financial investigation office of the High Court established that a few union leaders have been involved somehow in the misappropriation of funds that have been discovered. Those leaders would have covered the fact in exchange to personal advantages. Those facts would have been established by analyzing the home computers of those union leaders. The affair has now gained a world attention as a major event. The basis of union is disgusted and decides as retaliations a massive strike to bar the route to the “extremism and the attempts to crush democracy for the people”. The strikes crush the economic activity of the province, including transportation and electricity supply (both economic sectors are key components of the union).

Between June 24th and 27th, frequent breakdowns in the telephone network disturb certain areas including the capital and major cities. Those disturbances affect intermittently the mobile telephone network and Internet communications until June 29<sup>th</sup>, electricity supply, transportation facilities (railway signalling) are intermittently recorded. Several journalists evoke an attack by a worm. The operators speak of a failure of some network equipment, being replaced.

### **3.2.3 Phase 3: from June 20zz to October 20zz**

On July 12<sup>th</sup>, Sir Allistair Been, from the UK department for culture media and sport is forced to resign since the press said that he was involved in a sexual harassment affair. Investigation is under way said the journalists since they send to the police testimony of a victim which repeatedly received emails and suggestive phone calls from Sir Been. Journalists later evoked that digital evidences have confirmed the allegation. Sir Been also resigned from his position in the IOC.

On September 3<sup>rd</sup>, Mambaza Doueki, from Western Africa, a former marathon gold medallist is arrested in London under the charges of illegal drug traffic between Africa and England. No drug has been found until now but customs officers received evidences that the traffic has been organized by Mr Doueki. Investigations in his computer, customs spokesman said, confirm the traffic. Mr Doueki has

resigned from all his official positions, mainly in Culture and sport organizations. Mrs Doueki which is suspected to have taken part to the traffic has decided to stay in Africa for the moment.

October 10<sup>th</sup>, riots and mass protestations have dramatically increased in GREEN city, requiring for the Police to deploy important forces in the city. Four wounded protestors have been killed. New audio files have been released on youtube, in which a leader of one of the largest gang of GREEN city is insulting the other gang leaders and promising punitive actions against them.

October 11<sup>th</sup>, in BLUE country the world biggest company of soft drinks stopped its production for one week and decided a product recall for its production in some cities. The company's shares dramatically dropped as a consequence. The company's spokesman officially spoke about "malfunction of the production chain due to failure of automated manufacturing. The products were recalled as a precautionary measure to avoid minor stomach disorders". Unconfirmed rumours told spoke about computer attacks and money extortion attempts against the company.

In October 20<sup>th</sup>, the IOC makes its decision public: the BLUE city will organize the 20xx Olympic Summer Games Summer.

#### **4 Course of events analysis**

Before presenting what really happened, it is essential to keep in mind that in any conflict, the attacker has a depth in time and not other "players". Any operational planning considers options for the forces in front, possibly by weighting them by the time factor. In the case of our tactical scenario, it was easily predictable that only the GREEN and BLUE cities had a significant chance of being selected by the IOC. While the GREEN was the victim of different attacks whose purposes aimed at undermining his candidacy with the IOC, both RED and BLUE countries could anticipate this decision in advance of phase, to include in their strategic and tactical preparation then the conduct of their respective maneuver. From there, it is easy to study and identify areas of weaknesses for local action at the operational level, through computer attacks only.

This explains the fact that operations against the country GREEN city central province began several weeks before June, far ahead before the official date of candidacy reviews by the IOC members in June and the final selection in October. Who was behind those attacks, no matter! What really matters is the nature and conduct of operations: only attacks, without a trace, leaving afterwards analysts with the opportunity of endless epilogue on real responsibilities.

A first series of attacks had targeted several companies and their leaders. False documents, imitated from information processed offshore, were placed in personal and office computers of the main company's CEOs, and later personal computers of GREEN Nationalist Party leaders and extreme right-wing militia leaders and finally those of union leaders to strengthen the movement of strikes and make it uncontrollable. Then it was enough to send these documents to the press according to an appropriate timing, consistent with the conduct of other operations. Among those targeted companies are the centers of power supply, whose production is vital for economic activity in the province. Additional information (indiscretions on engineer blogs, politicians, union leaders...) make easy to suppose that tensions existed between unions and employers. By triggering those strikes, the goal was:

- To create a deplorable economic and social climate with rampant and recurrent movements of strikes;
- To block in short term, the economic activity in the province.

Finally, social movements created intended to provide a general picture of social and economic instability, incompatible with the Olympic Games organization in GREEN city.

The second series of attacks deals with the filing of provocative videos on two sites used by young people to exacerbate their rivalries and then trigger and feed riots over a rather long period of time<sup>5</sup>. The idea, based on classical coverage techniques used in infantry or cavalry, is to trigger a second

---

<sup>5</sup> This is based on real facts of the same nature which concerned France, fortunately in a very localized way and area, in November 2008 (*VinceNail Case*).

zone of instability and an image of unstable country where rivalries between gangs and between ethnic groups undermine social stability.

Faced with those problems, the GREEN power GREEN strives to organize. This implies an increase in communications between the various decision-making centers. A third series of attacks aimed at greatly hinder those communications and to extend the deadlines in the decision-making. Knowledge of the architecture of the telephone network has helped to see that the Research and Development network is connected to the operational network. An attack by viruses targeted against the personal laptops of several engineers and scientists of the operator (gathering information via blogs, social networks...) was used to attack the network by exploiting the fact that those engineers used to connect their laptop directly to the internal network (thus bypassing the DMZ), thus causing an indirect cause of infection. Similar attacks were launched against the main services and supplies of resources (public transport, electricity, rail and road signals management...) whose aim is to give a bad image with respect of the organization, stability and quality of public infrastructures.

Several destabilization operations against people subsequently conducted through attacks on their computers and mobile phones:

- The attack against members of the GREEN government aimed to falsely incriminate them in a case of child pornography network, aimed at discrediting the morality of the leaders of the GREEN country and thus indirectly at manipulating the world public opinion. Mr Alonzo Boïs was known to be very close to the official GREEN government members.
- In the same way, attacks against Sir Allistair Been, a member of the IOC who supported the GREEN candidacy (intelligence gained by spying his emails by means of computer Trojan) and Mr. Mambaza Douek, whose wife, also a member of the IOC who supported the GREEN candidacy, sought to shift the balance of votes in favour of the BLUE country.

Finally the attack against computer systems managing the production of the world biggest company of soft drinks was targeting in fact the major sponsor of the Olympic Games. This attack was made by manipulating RFID tags used to automatically select and mix drinks ingredients within the production chain. The analysis of the attack later showed that these attacks seemed to come from servers located in the GREEN country. The sponsor threatens to withdraw its financial support to the IOC GREEN if the GREEN country is selected.

## **5. Conclusion**

What can we say about the origin of these operations against the GREEN country: have they been launched by the BLUE country or by the RED? It is impossible to say, even by applying the principle of "Who benefits from crime?". This is the main interest of cyberwar operations. While in a conventional war, the notion of objective evidence is a tangible one (satellite imagery, human testimony cut, outside observers...), it is no longer valid when dealing with cyber warfare operations. The concept of evidence disappears completely with the concepts of time and space. But more serious, is that it not only disappears but it can be easily manipulated. It is possible to build any picture of reality and thus framing innocent parties.

The main results of our analysis show that

1. planning and conducting such attacks is unfortunately dramatically easy, both on the technical and operational (conduct of maneuver) level,
2. our modern nation who relies too much on Internet and the Information (media) itself are currently totally unprotected and therefore totally vulnerable,
3. the scope of such attacks is currently dangerously underestimated by our decision-makers and the possible targets are far more numerous than expected. We must think global as would attackers do.

This scenario is far from being hypothetical and it shows a possible aspect of what a true, generalized cyberwar can be. Far from the fantastic ideas of the concept of virtual war, which would run on the networks only, the war, may it be real or "cyber", has the sole purpose to intervene in the real: control of resources, territories, power ... As such, the targets of a cyber war are also very real, but much more difficult to identify because of mapping very difficult to establish. In our scenario, the IOC have secure networks (defence bunker-type), indirect attacks can cause so

much havoc. To do this, simply hit the physical or logic resources (including people) on which they more or less indirectly depend. This non-exhaustively includes:

- attacks against persons (deception, disinformation, wrong criminalization...);
- attacks against lines of communication and transportation (demonstrations, riots, movements of crowds ...);
- attacks against any possible vital resources (telephony, industry, services, goods, water, electricity ...);
- influence (*InfoOps*) or manipulation of the media (*Black InfoOps*) or public opinion through the media...;

The type of attack scenario we presented in this article may seem easy to achieve for the attacker. This is only in appearance. This type of approach, in addition to a phase of long and tedious intelligence gathering, is a complicated design, plan and lead. The timing must be accurate, but must allow some flexibility at the same time. Several options should be considered to switch from one to another depending on the actual effects on the ground (the “battlefield”) and the reactions of opponents or “human pions” on which the situation and or the target indirectly depends.

Finally, it is necessary to situate the concept of computer war in the broader context of war (Qiao & Wang, 1999) and emphasize the concepts of intelligence, taking into account the real by the policies and policy makers and protect professional (professional discretion) and personal information (privacy).

## References

Blog Secret Défense (2009), « *Les armées attaquées par un virus informatique* » (*French Defence attacked by a computer virus*), [online] Last retrieved February 5<sup>th</sup> 2009, <http://secretdefense.blogs.liberation.fr/defense/2009/02/les-armes-attaq.html>

Col. Qiao, L. and Wang X. (1999) “*Unrestricted Warfare*”. People Liberation Army Litterature and Arts Publishing House, Beijing. [online] <http://www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf>

Filiol, E and Raynal, F. (2009) « *Cyberguerre : de l’attaque du bunker à l’attaque dans la profondeur* » (*Cyber war : the attack on the bunker to attack in depth*). *Revue de Défense Nationale* (National Defence Journal), to appear March 2009.

Knowledgerush. Information Warfare [online], [http://knowledgerush.com/kr/encyclopedia/Information\\_warfare/](http://knowledgerush.com/kr/encyclopedia/Information_warfare/) .Last retrieved January 26<sup>th</sup>, 2009.

NATO (2006) “Information Operations – Analysis Support and Capability Requirements”. Research and Technology Organization, TR-SAS-057. [online] [http://ftp.rta.nato.int/public//PubFullText/RTO/TR/RTO-TR-SAS-057/\\$\\$TR-SAS-057-ALL.pdf](http://ftp.rta.nato.int/public//PubFullText/RTO/TR/RTO-TR-SAS-057/$$TR-SAS-057-ALL.pdf)