

## Chapter 2

# Cuba: Towards an Active Cyber-defense

Democratic states do not wage war on one another. Certain of the universal scope of this theory, democracies put pressure on authoritarian regimes to change their very nature. To steer states down the path of change, there are a number of tools that are required.

One rests on the theory of economic democratization, which incites developed, democratic states to provide financial aid to underdeveloped states, and involve them in the dynamics of the global economy. The economy would have democratic value.

Another is based on the theory of the democratizing power of information and information technologies. They have the capacity to bring individuals together, enable them to think collectively, bring an end to isolation, and expose connected communities to the influence of ideas and information from the rest of the world. These information technologies would therefore be a powerful tool or weapon, in the service of global democratization, enabling us to overthrow authoritarian political regimes. This technological determinism is reminiscent of the convictions of military men and their revolutionary strategies: it assigns technology a central role, conferring the power to change the world on its user, enabling them to achieve goals by means other than confrontation and armed conflict.

Since the early 1990s, it has been widely accepted that information technologies represent a genuine challenge for authoritarian regimes [KO 09], posing grave

---

Chapter written by Daniel VENTRE.

danger to their existence. The revolts of the Arab Spring, whose success is largely attributed to the mobilizing power of digital networks, seems to support this belief: the Internet has become an arena for political contest, a place of opposition between civilian society and the State, enabling dictatorships to be brought down.

Authoritarian regimes, for their part, are faced with the “dictator’s dilemma” [PRE 97]: they may be tempted to profit from the global economy, but do not wish to lose control over their society. Hence, they need to balance this double strain – the risk of democratizing pressure through the economy and through opening the door to the worldwide information society. It must be recognized, however, that a number of authoritarian regimes in the world remain strong, and are able to get around this dilemma. China and Saudi Arabia are not democracies, but have been able to integrate themselves into the movement of globalization, and integrate networked communication technologies. Yet these States have difficulty in accepting total information openness. They want the technologies, but also want to manage their development, monitor their users and control their uses, applications and content. Thus, this is a conditional opening, with rules aimed towards protecting the political regime and putting a stop on the pressure towards democratization.

Given the resistance of certain authoritarian regimes to the democratizing force of the Web, which is supposed to sap the resistance of all dictatorships in the world<sup>1</sup>, this postulate was called into question [HIL 98, DRA 00, ROH 00, BOA 00], meaning not that this capacity was denied, but rather that its automatic effectiveness was debated. This is because various conditions have to be satisfied and brought together for this force to be able to operate, such as (and this is by no means an exhaustive list):

- a significant Internet and telephone penetration rate;
- the opening of networks to the global Internet; and
- social actors capable of transforming the ideas carried over the Web into action.

Evgeny Morozov’s thesis [MOR 11], which is a reappraisal of the postulate, underlines that authoritarian regimes can exploit these technologies and networks in order to strengthen their own position. (The Internet facilitates surveillance and propaganda; it is preferable not to censor, block, close or prohibit it, but rather to play the game and launch yourself on the Web, to prove your innovativeness at State

---

<sup>1</sup> On March 8, 2000, US President Bill Clinton declared: “In the new century, liberty will spread by cell phone and cable modem. We know how much the Internet has changed America, and we are already an open society. Imagine how much it could change China. Now, there’s no question China has been trying to crack down on the Internet. Good luck. That’s sort of like trying to nail Jell-O to the wall”. Quoted in [DRA 00].

level, set up Twitter accounts, have a presence on social networking sites, and adopt the same tools and methods as your opponents.) The idea of democratization through networks is thus not automatically and universally applicable. The Internet cannot only serve the interests of the proponents of democracy, freedom of expression or political change. All parties have learnt to exploit the potential of cyberspace. Even very early on, authoritarian regimes became aware of the potential menace of cyberspace to their own equilibrium. The balance of strength established between the various forces may still swing in favor of the claimants of democracy or in favor of authoritarian regimes.

Cuba's policy of managing the Internet and, more generally, access to information – seems one of the most anti-libertarian on the planet. The country has one of the worst rankings in the world in terms of Internet access [MOL 11, FRE 09]<sup>2</sup>. Opposition to the regime, organized from abroad, is not weakening, but has not yet found the tool it needs to accomplish its objectives in cyberspace. Cuba decries the United States' (US) strategy, which aims to destabilize the regime by action.

In this chapter, we offer an analysis<sup>3</sup> of this Cuban policy – an illustration of the strategic role the Internet can play in a state governed by an authoritarian political system capable of keeping part of cyberspace under its thumb.

## 2.1. Cyberspace: statistics and history

### 2.1.1. *The marginalization of Cuba*

South America has a population of 570 million people<sup>4</sup>, of which a little over 182 million are Internet users<sup>5</sup>. Thus, with 8% of the world's population Latin

---

2 Scoring 15 countries from 0 (with the most freedom) to 100 (with the least freedom), Cuba comes in last place, with a score of 90, preceded, in descending numerical order, by Tunisia and China (78), Iran (74), Russia (51), Egypt (45), Turkey, Malaysia and Georgia (40). Estonia, in first place, scores 10. Those countries scoring lower than 30 are considered "free"; those whose score is over 70 are deemed "not free".

3 This analysis is based on cross-referencing the information available on the Web, bearing in mind that documents produced by external observers and official information published by the Cuban authorities alike are often biased, and we lack the means of validating the data thus collected. The limitations of research on Cuba lie in the difficulty in accessing official sources of information, and the impossibility of carrying out studies of the strategic factors on the ground (a practical difficulty that, it should be noted, is not necessarily peculiar to authoritarian regimes). The main source of information on Cuba comes not from Cuba but from abroad.

4 These statistical data were established for 2009.

5 <http://www.internetworldstats.com/stats10.htm>.

America is home to around 10% of Internet users on the planet. The country with the greatest number of “surfers” (nearly 72 million) is Brazil, followed by Mexico (27 million), Colombia and Argentina (20 million each). This list includes the countries with the highest gross domestic product (GDP) in the region (Brazil, Mexico and Argentina) and those with the largest populations (Brazil, Mexico, Colombia and Argentina). The countries where the Internet penetration rate is greatest are Chile (50%), Argentina (49%) and Colombia (48%) [IWS 12a].

The current population of Cuba is around 11.4 million. The number of Internet users is not known to any degree of certainty. Official statistics from Cuba claim there were 1.6 million in 2009 [ONE 09]. Data from the CIA gives the same figure [CIA 11], which represents a little over 14% of the population. Other studies (e.g. the Freedom on the Net report [FRE 11]) estimate the Internet penetration rate in Cuba as less than 1%, which is equivalent to the most backward countries in the world in terms of technological development. According to these figures, 2.9% of Cubans regularly have access to the Internet; 5.8% irregularly use e-mail; and only 200,000 residents have access to the World Wide Web [FRE 11].

At any rate, Cuba comes in far below the average in South America in terms of Internet access: with its 11.4 million inhabitants, it represents 2% of South America’s population, but only 0.87% of Internet users in that same population (this figure is calculated based on the highest estimate of 1.6 million Internet users in Cuba). The Internet penetration rate in the South American population is over 32%.

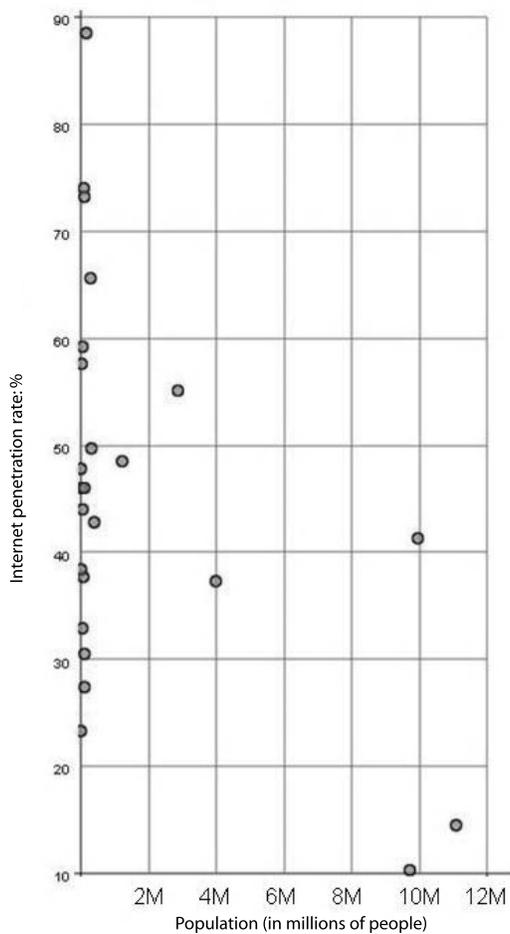
The population of the Caribbean is 41.4 million, including 11.4 million Internet users (a penetration rate equal to 27.5%)<sup>6</sup> [IWS 12b]. Cuba is the most densely populated island. It is also the island where the Internet penetration rate is lowest, along with Haiti (10%). Overall, it could be said that the Caribbean islands occupy their correct place in world Internet rankings, because with 0.6% of the global population, they are also home to 0.6% of the world’s population of Internet users. Hence, Cuba stands out clearly in this geographic ensemble, by its accumulated lack of progress; with nearly 27% of the region’s population, it represents only 13% of its Internet users. By comparison, the Dominican Republic represents 24% of the region’s population, but 35% of its Internet users.

Cuba is also the country with the lowest penetration proportion of people owning cell phones, in spite of the increase in subscriptions in recent years (75,000 subscribers in 2004; increasing to 443,000 in 2009). The market is monopolized by a single operator, Cubacel [ONE 09], a subsidiary of ETEC S.A. However, at the end of 2011 the number of cell phone users had increased significantly, reaching 1.2 million

---

<sup>6</sup> Statistical data from 2011.

active lines, i.e. 300,000 more than in 2010.<sup>7</sup> Yet there remains a lot of room for improvement.

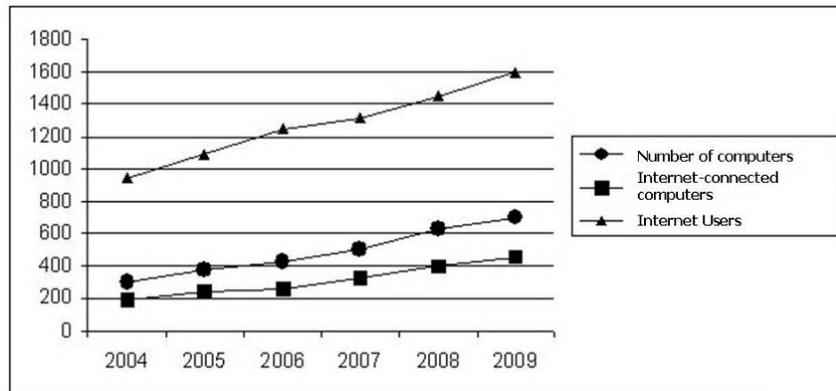


**Figure 2.1.** The number of people with access to the Internet in Caribbean countries (each country is represented by a dot). Most of these countries are small and their Internet penetration rate ranges between 23 and 88%. The two countries represented in the bottom right of the graph, on their own, have the highest populations and the lowest Internet penetration rate (Haiti and Cuba)

<sup>7</sup> Comenzaron a Aplicarse hoy las Nuevas Tarifas de los Celulares, Granma Internacional, Havana, Cuba, 1 February 1, 2012, (Today, the new cellphone tariffs came into force), <http://www.granma.cu/espanol/cuba/1febre-Comenzaron%20a.html>.

There are two networks in Cuba – a national intranet and the Internet, access to which is strictly limited. The content offered on the national network consists of an encyclopedia, government-run information sites (such as Granma<sup>8</sup>), educational sites, and official press and e-mail services. A small blogosphere is being organized around platforms that necessarily share in the spirit of the revolution, such as *Blogueros y Corresponsales de la Revolución*<sup>9</sup>, or *Blogs Periodistas Cubanos*.<sup>10</sup>

On June 1, 2011, there were some 124,158 Internet protocol (IP) addresses registered in Cuba, equating to 0.003% of the worldwide total (in 109th position on a list of 242 countries).<sup>11</sup>



**Figure 2.2.** *Number of computers and internet users (in thousands) according to statistics published in [PRE 11]*

### 2.1.2. Cuban cyberspace as the target of attacks

Probably due to its low degree of connectivity to the Internet, Cuba has thus far been spared from malicious activities (malwares). However, it is surrounded by countries (Brazil, Mexico, Colombia and Venezuela) where there is a great deal of this activity. It is probable that the island's newfound connection to high-throughput networks should in time result in the exposure of Cuba to this surrounding security

8 <http://www.granma.cu>. This site is translated into six languages, its aim clearly being to reach a wide global audience.

9 <http://bloguerosrevolucion.ning.com>.

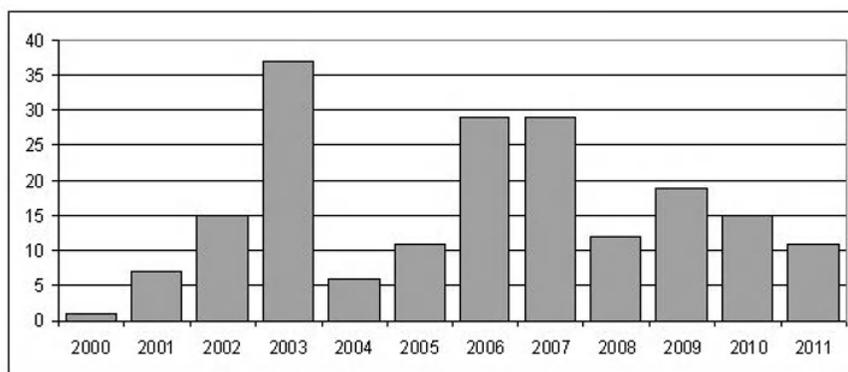
10 <http://blogcip.cu/>.

11 <http://www.domaintools.com/internet-statistics/country-ip-counts.php?f=total&o=asc>.

risk. The countries with the highest rate of malicious activity (viruses, spam, phishing, bots, etc.) recorded, both as the originators and the targets of attacks<sup>12</sup>, are Brazil (44% of South America's activities), Mexico (12%), Argentina (10%) and Colombia (7%). Venezuela, one of Cuba's closest allies, accounts for 3%. The attacks aimed at South America, according to reports from Symantec, come mainly from the US (50%), Mexico (14%) and Brazil (7%), followed by China (2%) and Argentina (2%) [SYM 10].

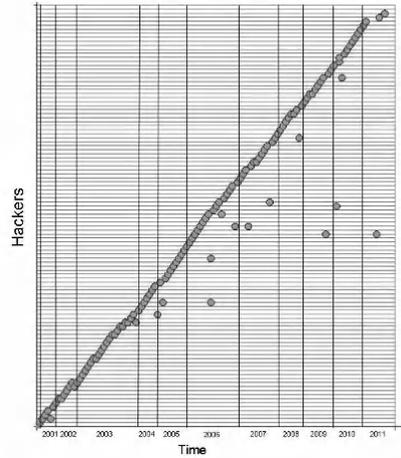
We can conclude from this that the attacks affecting the continent (except those from China) come from the American continent itself. In South America, Brazil looms not large but gigantic. For years, it has been considered a significant source of online security risks on a global scale, and as a country possessing well-qualified and underemployed computer scientists who are likely to sell their services to the criminal element.

In terms of cyber-crime and cyber-security, we do not have enough data to allow us to evaluate the situation on the island. However, the country appears relatively unaffected by site-defacing attacks, as the statistics compiled based on the data published on zone-h.org would seem to suggest. The low number of available sites is undoubtedly a contributing factor to this.

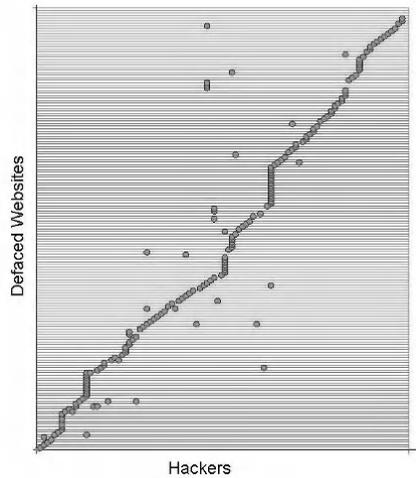


**Figure 2.3.** Histogram of defacements of sites with the domain name ".cu", according to data published on zone-h.org (accessed June 14, 2011)

<sup>12</sup> Symantec report 2010 [SYM 10].

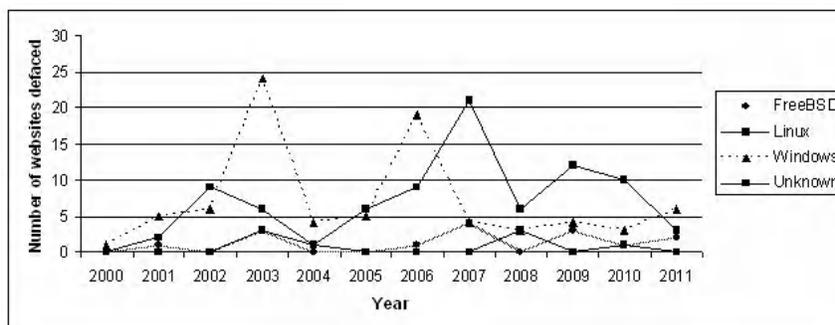


**Figure 2.4.** Number of “.cu” sites defaced from 2000 to 2011. Several points on the same horizontal line signify that the hacker attacked the domain on dates  $x_1, x_2, \dots, x_n$ . The diagram shows that the hackers’ actions are not long-lasting. It is not even possible to affirm that the Cuban sites were specifically targeted – these statistics simply illustrate the fact that the attacks are collateral effects of operations aimed at other online actors



**Figure 2.5.** The number of hackers defacing websites in the 2000–2011 period. Horizontally: a single point on the line denotes the site was defaced by one hacker and multiple points relate to multiple hackers. Vertically: the hacker attacked a site (a single point on the vertical line) or several sites (multiple points on the same virtual line). Overall, no one site appears to have been the target of a large-scale aggressive operation from multiple hackers

These same statistics show that over the past 12 years, the servers whose sites have been defaced are founded, in equal part, on private and free systems.



**Figure 2.6.** *The systems that have been the target of attacks over the 2000–2011 period (according to site defacement data published on the zone-h.org database)*

However, let us not forget that a project to develop a national open source solution for all governmental systems is officially under way<sup>13</sup>: the system Cuba Nova Linux is to be installed on nearly all government workstations. This policy, which consists of ensuring a State’s technological sovereignty and independence from the US, is an approach that is increasingly widely being used the world over.

The part played by free software in Cuba, however, remains modest, even though according to a recent study it seems that Cuba has the highest proportion of machines running Linux. (In Cuba, 6.3% of machines operate on Linux; by comparison, in France only 1.72% of computers have that platform installed.<sup>14</sup> In Italy, the market share is 1.54%; and in the UK and the USA it is only 0.73%; the global average is 0.76%.<sup>15</sup>)

13 Cuban minister “Fighting cyber-attacks is matter of national security”, *Cubaheadlines*, on February 25, 2011, [http://www.cubaheadlines.com/2011/02/25/29755/fighting\\_cyber\\_attacks\\_is\\_matter\\_of\\_national\\_security\\_cuban\\_minister\\_said.html](http://www.cubaheadlines.com/2011/02/25/29755/fighting_cyber_attacks_is_matter_of_national_security_cuban_minister_said.html).

14 *Cuba, premier pays utilisateur de Linux*, May 16, 2011, (Cuba the world’s main user of Linux). <http://www.webimag.com/2011/05/cuba-premier-pays-utilisateur-de-linux/>.

15 <http://royal.pingdom.com/2011/05/12/the-top-20-strongholds-for-desktop-linux/>.

## 2.2. Theoretical and practical considerations on information warfare and cyber-warfare

### 2.2.1. Development of capabilities

The history of computer science in Cuba goes back to the 1950s, when two first-generation American computers were installed there. After the revolution of 1959, trade with the US ceased. New computers arrived, particularly from France [MES 92], but after this time they were mainly imported from the Soviet Union. Cuba even invested in a program to develop its own computers in the 1970s. Specialists were trained in East Germany and the Soviet Union. An embryonic computer industry was formed at this time, but mainly involved assembling computers from imported components.

It was in 1991, a time when the economic situation was very difficult for Cuba (the Berlin Wall had come down, the Soviet Union had dissolved and a close ally had disappeared) that the first UUCP<sup>16</sup> connection was established between CENIAI (*Centro de Intercambio Automatizado de Información* – Center for Automated Information Exchange) and Web/NIRV in Toronto.

Since the 1990s, Cuban cyberspace has developed very little, not taking advantage of the Cuban Democracy Act passed in the US in 1992, exempting international telecommunications from the scope of the American embargo. The strategic measure was aimed at promoting democracy in Cuba by technological means [BOA 00]. The CENIAI is now one of only two Internet service providers in Cuba, the other being ETEC SA (*Empresa de Telecomunicaciones de Cuba S.A* – Cuban Telecommunications Company Ltd)<sup>17</sup>; both companies are under State control because of their strategic value. ETEC S.A. in which Telecom Italia had a 27% capital share until late January 2011, has since then been under total control of the State. The shares were bought out by the finance institution Rafin S.A., said to belong to Raul and Fidel Castro themselves<sup>18</sup>, and to finance the Cuban army. In May 2010, Rafin S.A is thought to have created a joint venture with South Pacific Holdings Ltd, controlled by Russian money<sup>19</sup>. According to the Cuban authorities, the low level of infrastructural development is due to the American policy which has maintained a trade embargo against the island since 1962. This has forbidden US companies trading with the Castro regime, preventing Cuba from tapping into the

---

16 Unix-to-Unix Copy Protocol.

17 <http://www.etecsa.cu/>.

18 *The Internet is a Question Mark in Cuba*, Cuba Verdad, May 18, 2011, <http://www.cubaverdad.net/weblog/2011/05/the-internet-is-a-question-mark-in-cuba-laritzadiversent/>.

19 Rafin, S.A, Raul & Fidel Inc., 5 February 5, 2011, [www.capitolhillcubans.com/2011/02/raul-fidel-inc-rafin-sa.html](http://www.capitolhillcubans.com/2011/02/raul-fidel-inc-rafin-sa.html).

ARCOS-1 cable (the constructor and main shareholder of which is the American company New World Network Ltd.)<sup>20</sup>, as well as depriving the country of good connections to the World Wide Web, forcing it to develop its own intranet relying on costly, low-throughput satellite connections.

The new undersea fiber optic cable that was deployed in early 2011, linking La Guaira (Venezuela) to Santiago de Cuba, is intended to increase the capabilities for communication with the rest of the world. Another segment links Santiago de Cuba to Jamaica. The project was carried out in part by the Franco-Chinese consortium Alcatel-Shanghai Bell<sup>21</sup>, at a cost of around \$70 million, financed by Venezuelan banks and Cuba's own money. The operator of the system will be Telecomunicaciones Gran Caribe S.A, which will then sell bandwidth to other countries. The installation of the cable, begun on January 22, 2011, was greeted by inflamed discourse from journalists<sup>22</sup>. The Cuban media emphasized the new opportunities offered, to both Cuba and the region, for a free world, with the chance to realize José Martí's vision.<sup>23</sup>

The country is financing new projects to develop, in particular, a software industry. It was to this end that the University of Computer Sciences (UCI – *Universidad de las Ciencias Informáticas*)<sup>24</sup> in Havana was created, and opened in September 2002. This institution's mission is to train thousands of software developers, capable of supporting the project, in order to bring the country into the information age in the years to come [HAA 05]. The following mission statement is displayed on the institution's homepage: "UCI is a productive university, whose mission is to produce software and computing services based on the link between study and work as a training model"<sup>25</sup>. A technological park must also be created in this context, in order to produce software to meet both national and international demands. The outfit was built on the site of the old military listening station, Lourdes, developed by the Soviets in 1964.

At its opening in September 2002, the university took in more than 2,000 students, taught by 300 professors. Four years later, the university had enrolled some

---

20 *Acceso a Internet en Cuba* (Access to the Internet in Cuba), September 17, 2010, <http://www.pcacordoba.es/?p=1326>.

21 *En busca de independencia, cable Cuba-Venezuela para el 2011*, October 31, 2009, (In search of independence – Cuba-Venezuela cable for 2011). <http://www.cubadebate.cu/noticias/2009/10/31/en-busca-de-independencia-cable-cuba-venezuela-para-el-2011/>.

22 See the video at <http://www.cubadebate.cu/noticias/2011/01/22/comienzo-instalacion-del-cable-submarino-venezuela-cuba/>.

23 1853-1895, Cuban politician, poet, founder of the Cuban Revolutionary Party, veritable national hero and martyr for independence.

24 <http://www.uci.cu/>.

25 <http://www.uci.cu/?q=node/46>.

10,000 students. The work carried out there is aimed to create a large-scale site accommodating 20,000 people, in what is known as the Digital City of the Future (*Ciudad Digital Avanzada*). The means invested and the scope of the Cuban project, are not sufficient to envisage anything on the scale of the gigantic technological parks found in the US or in Asia.<sup>26</sup> However, it does bear certain similarities to some of them. Cyberjaya, in Malaysia, is a digital city opened in July 2003, 25 km south of the capital, Kuala Lumpur. These projects, which were thus begun in the aftermath of 9/11, are focused on new technologies and are geographically close to the political capital in order to underline their strategic nature. The major differences are that the digital city in Malaysia houses thousands of national and foreign enterprises.

### 2.3. Cyber-warfare theories and practices

In Cuba, the questions of information warfare and cyber-warfare are not (as yet) asked in the same terms as in industrialized countries where, it must be remembered, the discourse and strategies are concentrated around:

- dedicated military forces;
- cyber-attacks against the systems managing countries' essential infrastructures;
- cyber-espionage; and
- attacks mounted by non-state actors of terrorist, anarchist, anti-globalization or libertarian etc. persuasion, which may not have much of an impact individually but can, by cumulative effect, create an atmosphere of disorder, significantly destabilize the function of national economies and in particular, global systems.

For the Cuban regime, the question of cyberspace-based attacks is an even bigger part of the natural extension of the protection of its information space. Hence, we are dealing with the field of psychological operations, propaganda, the manipulation of opinions, the battle of ideas, interception of communications (electronic warfare) and intelligence – areas which are likely to undermine national unity. For the Cuban authorities, control of cyberspace and the ideas communicated therein is deemed necessary for the survival of the political model. Cuba decries the American strategy of cyber-warfare – which consists not of using networks as a tool but actually as a weapon to attack enemy cyberspace, to destabilize states – and one of its declensions, the setting up of a blogosphere that appears to be independent but which is in reality subjugated to Washington. Egypt and Libya have been victims of this strategy. Cuba is another major target, according to official Cuban media [MEX 11a]. This American strategy must rely on recruiting cyber-mercenaries, ersatz bloggers in Washington's pay particularly exiled Cubans, charged with

<sup>26</sup> <http://www.cyberjaya-msc.com/>.

propagating untruths, misinformation, subversive ideas, etc. Here, Facebook, Twitter, YouTube, Flickr, etc., are vehicles for this destabilizing propaganda. Cubans would be approached, even within the country, to organize networks of cyber-dissidents. (Operation Surf, organized by the CIA and financed by USAID<sup>27</sup>, with the involvement of Freedom House, is yet more proof of the US strategy against Cuba [MEX 11b].)

Thus, the Cuban Internet is controlled – under the thumb of the State – and nothing favors the emergence of an open Internet society: the information space has to be controlled.

However, it is not beyond the realms of possibility for Cuba to carry out more offensive cybernetic operations (virus attacks and invasions) against countries that are better connected than it is. It is that asymmetry which now constitutes the strength of small States. However, in the short term, we have to wonder about the consequences of the new high-capacity connection between Cuba and the global Internet, from which it has hitherto been isolated. This new technological capability could be a harbinger of other consequences that are more offensive, in the same vein as occurs in the rest of the world. For the Cuban government, cyberspace must be the instrument of its power strategy – the government must help to reinforce it, extend it, and officially pursue the revolutionary goals in the long term.

### **2.3.1. Fidel Castro's discourse**

The various interventions by Fidel Castro over the past few years help to shed some light on Cuban policy in terms of the Internet, which is directly linked to the State's vision of using the media in the Cuban socialist society.

As regards the freedom of the media, Fidel Castro is intransigent. On the one hand, he states that the Cuban media have to learn the art of constructive criticism, in the spirit of the revolution; yet on the other hand he does not allow total freedom of the press, which would involve opening up the floor to the anti-revolutionary press (which, it is understood, would infect Cuba with subversive ideas, Western culture, capitalism and the call to revolt). The critical spirit is therefore restricted. The country would be unable to withstand another counter-revolutionary influence.

“Our press organs are not in the hands of the enemies of the revolution, nor of the agents of the United States. They are in the hands of revolutionaries. Our press is revolutionary, our radio and television journalists are revolutionary. [...] We have discovered that

---

<sup>27</sup> US Agency for International Development, <http://www.usaid.gov/>.

in the struggle against negative facts, the work of the press is very important. And we have stimulated critical spirit. We have come to the convinced conclusion that it is necessary to develop critical spirit a great deal further” [RAM 06].

This approach should not be seen as an indication of willingness to introduce total freedom of the press as Western media understands the term. Indeed:

“If by ‘freedom of the press’ you mean the right of counter-revolution and the right of Cuba’s enemies to speak and write freely against socialism and against the revolution, to slander, lie and create conditioned reflexes, I would say to you that we are not in favor of that ‘freedom’. As long as Cuba remains a country blocked<sup>28</sup> by tyranny, the victim of iniquitous laws such as the Helms-Burton Act<sup>29</sup> or the Cuban Adjustment Act<sup>30</sup>, a country threatened by the very President of the US, we cannot give that freedom to the allies of our enemies, whose objective is to fight against socialism’s very *raison d’être*” [RAM 06].

In addition, there can be no ‘free’ press in the sense that it cannot be a question of private property for the media, which are all State run.

The main points of argument lie in blaming the embargo situation, the total lack of freedom of the press and the little development in terms of Internet infrastructures primarily on the US, and more generally on the wider capitalist world. Cuba views itself as the victim of ‘media terrorism’ on the part of large international groups, who paint Cuba in an erroneous, untrue, negative light that is damaging to the nation<sup>31</sup>.

“Today there are means of communicating with the world which make us less the victims of, or dependent on, any large-scale, mass-distributed media, be they private or State run, because today, with this worldwide Internet, all those who have an aspiration, a goal, will work together, be they from a rich or a poor country” [CAS 03].

---

28 The Cubans speak of a “block” and the Americans of an embargo.

29 Cuban Liberty and Democratic Solidarity, Helms-Burton Act, 1996, <http://www.treasury.gov/resource-center/sanctions/Documents/libertad.pdf>.

30 The 1966 law which, like the Helms-Burton Act, forms part of the US policy of maintaining an economic embargo against Cuba.

31 Cuba llama a la “ciberdefensa activa” en la red y la “blogosfera”, December 1, 2011, (Cuba calls for “active cyberdefense” on the web and in the “blogosphere”). <http://elcomercio.pe/tecnologia/1341987/noticia-cuba-llama-ciberdefensa-activa-red-blogosfera>.

Fidel Castro emphasizes the liberating dimension of the Internet, the revolutionary potential of the Internet the world over. He underlines the capacity of that tool to reinforce the power of collective popular action; however, he cannot envisage or take the risk of that being so in Cuba. This is probably because, from his point of view, Cuba is more of a model of revolution for others, rather than a model to be rethought. The official position is to give no ground at all in terms of media freedom, in the name of preserving the gains of the revolution. The State wishes to be able to exert an influence on the international stage without being influenced in return.

### 2.3.2. *The concept of active cyber-defense*

The Cuban State perceives a threat in cyberspace and thus calls on a form of protection which it calls ‘active cyber-defense’; this would involve first defining a political strategy in cyberspace, which is thus far lacking<sup>32</sup>. In December 2011, the Cuban Foreign Minister, Rodríguez Parrilla, called for social networking platforms that pose a danger to peace in the country to be seized. This strategy involves the occupation of cyberspace. This does not necessarily imply an aggressive dimension in terms of cyber-attacks, but rather a position in the blogosphere, on social networks, in media space, and a strategy of influence. “It is fundamental that revolutionary movements will find their expression in cyberspace”<sup>33</sup>.

Are the authorities envisaging supporting foreign revolts? The primary objective is to counter the presence of detractors and opponents of the Cuban regime. This active cyber-defense does not (officially, at least) display a military aspect. It is not (yet) a question of military cyber-units for Cuba, as is now the case in many countries. A document published on the CubaDebate<sup>34</sup> site transcribing the proposals put forward during a conference organized in Havana on November 29, 2011 shows the outline of this concept of active cyber-defense:

- Cyber-warfare is reserved for military action.
- Active cyber-defense is a new concept, which the Cubans must use in the struggle against the model imposed by capitalist tyranny, to complement the action

---

32 *Cuba llama a la “ciberdefensa activa” en la red y la “blogosfera”*, 1 December 2011, <http://elcomercio.pe/tecnologia/1341987/noticia-cuba-llama-ciberdefensa-activa-red-blogosfera>

33 Reported proposals, attributed to the Foreign Minister, *Cuba llama a la “ciberdefensa activa” en la red y la “blogosfera”*, December 1, 2011, <http://elcomercio.pe/tecnologia/1341987/noticia-cuba-llama-ciberdefensa-activa-red-blogosfera>.

34 *De la ciberguerra a la Ciberdefensa activa*, November 30, 2011, (From cyber-warfare to active cyber-defense), <http://www.cubadebate.cu/opinion/2011/11/30/de-la-ciberguerra-a-la-ciberdefensa-activa/>.

of those who oppose the postmodern folly of digital evangelization, which tries to make us believe that a computer program is a social network, that a thing is a human being.

- Revolutionary action must be built up: we must identify the enemy's actions, imagine alternatives and provide revolutionary movements with scientific instruments to enable them to adopt an offensive strategy.

- This effort must guarantee the security of the revolutionary movements on networks and establish synergies with computer experts, ever more given to crime and who will form part of the global government and its systems of surveillance and control.

- We must study the experiments of resistance on the Internet; develop strategies of visibility, of cooperation, of alliances; we must know what to do in the case of an attack or censure against a blog, a website or an account on social networks; we must know how to defend ourselves; how to free ourselves from technological dependence on a few global actors who bow to the decisions of the capitalist empire.

- Active cyber-defense must be the top priority.

- It must not be forgotten that, though there may be major inequality between those who have materialistic power and proclaim the need for war and the moral forces that reclaim the right to peace, only the will of men can conquer the will of other men.

“Ideas are and always will be the most important weapon”, proclaimed Fidel Castro in a speech given on December 2, 2001 in Santiago de Cuba [CAS 01]. Hence, cyberspace can no longer be ignored by the authorities: active cyber-defense is presented first and foremost as taking account of the capacities of the medium to stage a veritable battle of ideas.

#### **2.4. Regulations and ways around them**

The Cuban authorities have many tools at their disposal to maintain control over the information space. Internet access is regulated by legal, technological and financial constraints. Content control is ensured both inside and outside the country. The immediate consequence is the limitation in the number of Cuban internet users; in addition, the impossibility of staying connected for a long time reduces the risk of any opening to the outside world, thereby reducing the influence of foreign ideas.

Cuba's strategy consists of developing and favoring collective access, but in actual fact still favors clearly-defined social classes.

#### 2.4.1. *The State's influence over cyberspace*

Internet access is rendered difficult. It is authorized in hotels for foreign tourists (at prices that are prohibitive for most Cuban citizens), and at official access points that are monitored (in particular the cybercafés that the Cuban postal service has been able to set up following Law No. 99/2009). Domestic Internet connections are not yet authorized, except for a handful of citizens (doctors, professors and government officials). Outside of hotels, only a privileged few actually have special authorization and are allowed to connect to the international network. Thus, a person has to provide a valid reason in order to obtain accreditation facilitating access to the Web. The level of merit of the requester is assessed by a committee for the defense of the revolution. The authorities rely as much on making it difficult to access the Internet as on actually filtering the contents to limit contact with the outside world and with ideas deemed subversive.

Limitations are also imposed by the legal framework. Thus, anyone posting articles deemed to be counter-revolutionary faces 20 years in prison, whether or not the content is distributed via foreign sites or platforms. This sanction is written into the Penal Code and in Law 88. Decree 209 of 1996, Access from the Republic of Cuba to the global information network<sup>35</sup>, stipulates that the Internet cannot be used in violation of the moral principles of the society or the laws of the country. Internet access is defined according to the country's interests, which are defined by the authorities. In 2007, Resolution 127 reminded us, as if it were necessary, that it is forbidden to use networks to broadcast information contrary to society's interests, to the norms of good behavior, to the integrity of individuals or to national security. The Internet service providers are obliged to put checks in place that are capable of detecting and preventing illicit activities; they are obliged to inform the authorities of any infraction of the law of which they are aware. Connecting to the Internet without authorization carries a sentence of five years in prison. Expressing yourself

---

35 *Acceso desde la República de Cuba a Redes Informáticas de Alcance Global*, *Gaceta Oficial de la República de Cuba*, no. 27, September 13, 1996 (Access from the Republic of Cuba to Computer Networks of Global Reach), <http://www.ordiecole.com/cuba/209-1996.pdf>. The text specifies the conditions of State control over Internet access: an inter-ministerial commission – made up of the Ministers of Science and Technology, Communications, the Interior, the Revolutionary Armed Forces and Justice, presided over by the Minister of the Steel and Electronic Industry – is charged with regulating the development of networks in the country, and the use of information coming from global networks. Contributions as regards the Internet are the preserve of the new Ministry of Computer Sciences and Communications, set up on 11 January 2000 (Decree-Law 204). In order to coordinate the institutional strategy on computer security, the Bureau of Security for Computer Networks (*Oficina de Seguridad para las Redes Informáticas*) was created on May 21, 2002 by Resolution 64. Cuba's legislation as regards the regulation of the Internet is relatively abundant: [http://www.informatica-juridica.com/trabajos/Resena\\_de\\_la\\_legislacion\\_informatica\\_Cuba.asp](http://www.informatica-juridica.com/trabajos/Resena_de_la_legislacion_informatica_Cuba.asp).

online is risky. In the past few years, a number of journalists/bloggers have been imprisoned, with sentences from a few months to several years for subversive propaganda that is menacing to society.

Limiting technological development is an additional tool of the policy of keeping society under control. Technologies are being introduced gradually: up until 2008, citizens were prohibited from owning a computer. This explains the low level of technological development on the island, where there are 3.3 computers per 100 inhabitants. VoIP<sup>36</sup>, a new form of technology, is forbidden, except at certain duly authorized and controlled access points in Havana. Besides the aforementioned technical constraints and the legal restrictions on access, the prohibitive costs of communication greatly restrict the number of Internet users. It should be borne in mind, by comparison, that the average monthly income in Cuba is \$20. An hour's connection at an Internet access point costs \$1.50, and \$7.00 in hotels for tourists. A computer (distributed by the State-controlled importer Copextel Corporation) costs roughly \$800 (or \$600 on the black market). While 30% of Cubans claim to have access to a computer, it is usually either at work or at school [ONE 09]. Mobile telephony, whose network does cover 70% of the territory, is no more accessible in financial terms. In May 2011, Cubacel reduced the fees for initiating and activating cell phone subscriptions to \$30.<sup>37</sup> The cost of international calls varies between \$1.40 and \$1.85 per minute. On February 1, 2012, the costs of SMS messaging were cut by 44%<sup>38</sup>.

In order to ensure control of the information space, the authorities have put processes in place that allow them:

- To occupy blogspace: the authorities have to be present in cyberspace, however little of that space they occupy. To this end, an official association of Cuban bloggers has been created.

- To pirate Cuban websites abroad: Cuban websites and blogs hosted abroad have been victim to pirating. In May 2008 during the trial of the economist Martha Beatriz Roque, proof came to light that the government was pirating dissidents' Yahoo! accounts<sup>39</sup>.

---

36 VoIP Voice over Internet Protocol.

37 *Cuba rebaja servicio de celulares en busca de mas usuarios*, May 24, 2011 (Cuba lowers its cellphone tariffs in search of more users), <http://www.cubaverdad.net/weblog/2011/05/cuba-rebaja-servicio-de-celulares-en-busca-de-mas-usuarios/>.

38 *Comenzaron a aplicarse hoy las nuevas tarifas de los celulares*, Digital Granma International, Havana, Cuba, 1 February 1, 2012, <http://www.granma.cu/espanol/cuba/1febre-Comenzaron%20a.html>.

39 *Cuba, Freedom on the Net*, Cuba Verdad, May 2, 2011, <http://www.cubaverdad.net/weblog/2011/05/cuba-freedom-on-the-net-2011-freedom-house/>.

– Software applications, such as Avila Link, enable communications to be monitored (communications are routed via proxies, and the authorities can obtain the usernames and passwords of surfers) at the level of the multiple public Internet access points [FRE 11]. As much as by the installation of tools for filtering and censorship, because of the poor quality of the networks filtering takes place almost naturally: international sites, such as that of the BBC and *Le Monde* are officially accessible, but too-low throughputs prevent them from being consulted. Sites judged to be anti-Cuban, blogs written by Cuban residents themselves but hosted abroad may be blocked. Censorship is certainly present on Cuban networks.

– In 2007, access to portals such as Yahoo!, MSN and Hotmail was systematically blocked [FRE 11]. The blocks remained in place for several months, including on blogger platforms. Facebook and Twitter were periodically available. For this reason, even those few citizens who could access the Internet rather than content themselves with the Cuban intranet could not surf the Web entirely at their leisure.

Thus, Cubans only have cyberspace, Internet, mobile telephony benefits and modern information and communication technologies (ICTs) in the broader sense, with limited and partial vision, access and usage.

#### **2.4.2. Getting around the restrictions**

Owing to Cuban politics, which is restrictive of fundamental liberties, Reporters Without Borders qualify the regime as an enemy of the Internet (a country that violates the freedom of expression online), similar to Saudi Arabia, Myanmar, China, North Korea, Egypt, Iran, Uzbekistan, Syria, Tunisia, Turkmenistan and Vietnam.

The socio-political climate in Cuba (a set of measures and conditions that limit both access to cyberspace and free expression) is clearly not very favorable to the emergence of a true information society, and of an Internet culture. The barriers and limitations, as always, drive individuals to come up with ways around them.

A black market appears to have taken root in Cuba, based on the trade in access to the Internet. Thus, those who have authorizations sometimes hire out their access. The cost proves high – around \$65 per month, i.e. two to three times the average salary. Content that cannot circulate freely on the Web is exchanged on USB sticks or CD-ROMs. Similarly, a market for counterfeit DVDs and software packages has developed on the island to get around the US embargo and for simple reasons of cost (the original products are beyond the reach of Cuban consumers because they are too expensive). Thus, although Microsoft is not authorized to sell its products in Cuba, almost all computers run Windows. In a study published in 1992 [MES 92],

the authors pointed out the existence of a counterfeiting system organized by the State in Cuba: a national center copied foreign software to distribute it to Cubans free of charge. The rate of software piracy in the country is estimated at 80% by the Business Software Alliance [ISR 10]. Cuba ignores the copyright system (although, paradoxically, copyright is imposed on some of its official websites).

In this environment so unpropitious for free expression, a small community of bloggers has nevertheless been able to take root. There are roughly 150 blogs that are hosted abroad. The contents are sent via e-mail from Cuban hotels to friends or family members living abroad, who then post the messages on the blogs, which most often talk about local, day-to-day life. The bloggers generally avoid politicized subjects that may be sensitive (auto-censure). However, some of them have acquired a reputation that extends beyond Cuba's shores, for their frankness. For instance, we can cite:

– Yoani Sanchez, who lives in Havana, and whose blog *Generación Y*<sup>40</sup> hosted on the *Voces Cubanas* (Cuban Voices) platform, describes daily life. The political dimension of her posts has brought her international renown, and in 2008 *Time* magazine dubbed her as one of the 100 most influential people. The Cuban authorities then attempted to discredit her, calling her a mercenary in the pay of foreign forces<sup>41</sup>.

– Luis Felipe Rojas, a blogger who has been arrested many times, and was placed under house arrest in 2009.

These individuals form part of the elite circle of bloggers who, in their respective countries, have become mediatized personalities on an international scale for their opposition to the regime and their participation in revolutions. Notably, such bloggers include Slim Amamou and Lina Ben Mehni (Tunisian revolutionary bloggers), Zouhair Yahyaoui (Egyptian), Hassan al-Djahmi<sup>42</sup> (a Libyan political exile in Switzerland, who on January 28, 2011 on Facebook called for a nationwide day of anger (day of celebration) to be organized) and even Mohamed Nabous<sup>43</sup> (an anti-Gaddafi blogger who was killed by a sniper on March 19, 2011)<sup>44</sup>. The appearance of emblematic figures, or you might even say 'heroic' figures, is significant of the evolution of information warfare, which up until now have not yet

40 <http://www.desdecuba.com/generaciony/>.

41 *Cuba says blogger Yoani Sanchez part of "cyberwar"*, March 22, 2011:

<http://uk.ibtimes.com/articles/125216/20110322/cuba-says-blogger-yoani-sanchez-part-of-cyberwar.htm>.

42 <http://www.facebook.com/hassan.aldjahmi>.

43 [http://en.wikipedia.org/wiki/Mohammed\\_Nabbous](http://en.wikipedia.org/wiki/Mohammed_Nabbous).

44 <http://www.facebook.com/MartyrMohamedNabous>;

<http://www.streetpress.com/sujet/2161-libye-mohammed-nabbous-est-mort> (Libya – Mohammed Nabbous dead).

found genuine combatant icons. Cyber-conflict is not merely dominated by anonymous hackers or state cyber-warriors, who are all nameless and faceless. The hacktivists of Web 2.0 give cyber-conflict a human face. It is no longer solely a question of shadowy hackers, viruses, virtuality and immateriality.

## 2.5. Capabilities of control, surveillance and interception

Cuba has had electronic surveillance systems (SIGINT)<sup>45</sup> at its disposal ever since the Soviet Union helped it build the Lourdes listening post near Havana, two years after the Cuban Missile Crisis. The station had 12 antennae<sup>46</sup> and 1,500 Soviet engineers and technicians. The base was shut down following the 9/11 attacks in New York, when Russia officially and unilaterally decided to withdraw from the project. The UCI was rapidly built on the site the following year. Classes began taking place, although the military equipment from the old base had yet to be removed<sup>47</sup>.

The Cuban government, who did not have use of the Lourdes base, which was reserved for the Soviets and later the Russians, wanted to have its own SIGINT infrastructure. The base at Bejucal, not far from Lourdes, was then constructed between 1995 and 1998 with the participation of Russia. The equipment left for Cuba from the port of Riga in Latvia. In 1998, the US Department of Defense picked up on a significant increase in the amount of illegal importation of American computing material into Cuba. The military base at Bejucal, a militarized zone near to DAAFAR (*Defensa Anti-Aerea y Fuerza Aerea Revolucionaria* – Anti-Aerial Defense and Revolutionary Air Force) and the Rescate de Sanguily base includes 10 Satcom antennae<sup>48</sup>. Besides the interception systems, the bases have systems for interfering with satellite communications (GPS, Satcom, et.) designed and based on equipment bought from the Russian enterprise Aviaconversa. The systems enable Cuba to intercept US telecommunications, international satellite communications satellites, Internet communications and communications within the embassies.

According to the unconfirmed information provided by Manuel Cereijo<sup>49</sup> (a Cuban-born engineer teaching at the University of Miami in Florida, who publishes a great many articles on the situation in Cuba, and particularly on issues relating to

---

45 SIGINT – SIGnal INTelligence.

46 [http://bbs.keyhole.com/ubb/ubbthreads.php?ubb=showflat&Number=521637&site\\_id=1#import](http://bbs.keyhole.com/ubb/ubbthreads.php?ubb=showflat&Number=521637&site_id=1#import). Accessed in October 2011.

47 <http://www.uci.cu/?q=node/48>. Accessed in October 2011.

48 [http://bbs.keyhole.com/ubb/ubbthreads.php?ubb=showflat&Number=521637&site\\_id=1#import](http://bbs.keyhole.com/ubb/ubbthreads.php?ubb=showflat&Number=521637&site_id=1#import) Accessed in October 2011.

49 CEREIJO M., *Cuba and Information Warfare*, undated, [www.amigospais-guaracabuya.org/oagmc207.php](http://www.amigospais-guaracabuya.org/oagmc207.php).

the Internet, telecommunications and electronic warfare), an agreement was signed between Cuba and China in 1999, relating in particular to the development of these SIGINT capabilities. Thereby, China contributed to the development of the Bejucal base (not far from the UCI), where a cyber-warfare unit is active in monitoring data traffic. Chinese military personnel use the Bejucal base, using the Chinese communication satellites rather than the Russian ones. In addition, large SIGINT systems have been installed at Wajay (not far from UCI) and Santiago de Cuba as part of the Titan project, the fruit of Sino-Cuban collaboration.

Such information, which is near-impossible to verify, paints a picture of a nation that is active in the field of surveillance, control, data interception, cyber-warfare and electronic warfare. It is dependent on foreign capabilities, first Russian and now Chinese. Other, more recent articles suggest that Cuban security forces provided the Venezuelan government with the transmitters used in the new identification cards and passports, thus facilitating the surveillance of individuals [CRU 11].

More important than the (unprovable) veracity of the information provided by the various sources cited here is the image which emerges: Cuba appears to be a 'Big Brother'-type of island, with wide-reaching international influence, infiltrated by allied powers and which in turn infiltrates its allies.

## 2.6. Enemies

Cuban policy as regards security and defense is spearheaded by the struggle against American imperialism. The enormous military exercise in Bastion 2009, held between November 26 and 28, 2009, was the first on such a scale since the political transition in 2008. It was aimed at preparing Cuban forces to defend against a military invasion by the US. The exercise involved tactical maneuvers, ground-troop exercise and aerial maneuvers.

However, the threat is not limited to the conventional military dimension. As Boris Moreno, Minister for Computer Sciences and Communications, pointed out in 2008, "the use of the Internet [should serve to] defend the Revolution and the principles in which Cuba has believed for years". Information space and cyberspace are also perceived negatively, as being vectors of foreign misinformation, a danger, a weapon that could be used against the interests of the Cuban people and the Revolution. "A cyber-war is a war fought not with bombs and bullets, but with communication, algorithms and bits. Cyberwarfare is a new form of invasion, dreamt up by the developed world"<sup>50</sup>.

---

<sup>50</sup> *Ciberguerra*, March 21, 2011, <http://idanielacubana.blogcip.cu/2011/03/21/ciberguerra/>. idanielacubana is a blog that conveys the ideology of the Cuban authorities.

Cuba is not alone in this anti-imperialist stance. Hugo Chavez's government is one of the most virulent actors. Let us not forget the Asian giant China, which may resort to similar rhetoric. In a speech in Shanghai in June 2000, the son of Jiang Zemin, Jiang Mianheng, Vice-President of the Chinese Academy of Sciences, trained as an engineer in the US, declared that China must fight against one of the negative aspects of internationalization: cyber-imperialism [LAM 00]. Internet technologies are controlled by the US, and he believes China's integration into the economy dominated by cyberspace presents the danger of subjugating the country to the fealty of capitalist, neo-imperialist Western powers. This threat justifies the construction of a national network independent of the Internet, the elaboration of new protocols and technologies on which it is to be based. Anti-communist values are penetrating Chinese society by way of the Internet. The intrusion of these Western ideas represents a threat to the Chinese Communist Party's power. The other danger lays in the existence of "back doors" in Windows applications, which could lead to the leaking of secret State documents. The West's technological domination is perceived as a colonial menace. This is a question not only of technological dependence, but also of influence and remote control by ideas and cultures. The West uses globalization, utilizing cyberspace as a tool through which to exploit the third world, the second world and developing countries.

After opium, which subjugated China to the West's influence, there now appears to be the 'electronic heroin' of bourgeois-liberal websites [LAM 00]. The Chinese Communist Party is becoming addicted to this Marxist rhetoric. The Chinese people must steel themselves to fight against foreign cyber-invaders. The only solution to preserve national security is therefore to develop national technologies, to escape from any possible dependence on foreign powers. Of course, all this must go hand-in-hand with filtering of the Internet. Thus, the following is at stake:

- preserving the prerogatives of the Chinese Communist Party;
  - preserving Chinese sovereignty;
  - assimilating foreign technologies and developing China's own technologies;
- and
- adopting international standards while retaining control on the home front.

Cuba is a long way from having the same industrial, human, financial and military capabilities as China that enable China to envisage maintaining this posture in relation to the American giant. However, in spirit, the Cuban discourse of struggle against American imperialism tends to converge with the arguments developed by Jiang Mianheng.

The new concept of Cuban active cyber-defense is borrowed from these anti-imperialist arguments and could be considered to stem from this struggle against American cyber-imperialism.

Since the 1990s, Cuba has been concerned about the enemy using the Internet to subversive ends. In this context, international associations (NGOs) were identified as potentially subversive. In his speeches at the time, Raul Castro spelled out the nature of that threat in no uncertain terms<sup>51</sup>:

“The enemy make no secret of their intention to use a number of NGOs recently installed in Cuba as Trojan Horses to foment division [...] it would be idiotic of us to pretend not to see the manipulation instrumented through the NGOs, whose only objective is to subject our country to slavery once more...”

The concerns voiced by Cuba are borne out by the projects carried out in the US. In a study published in 1992, David Ronfeldt recommended the adoption of a US policy of communication to help open up the Cuban system and speed up the emergence of an independent civil society [GON 92].

The adversary takes the form of a spy, an American entrepreneur attempting to smuggle telecommunication materials into Cuba. The US industrialist Alan Gross, 61, was arrested in December 2009 in Cuba and sentenced to 15 years' imprisonment in March 2011 for having attempted to illegally import communication materials [MIR 11]. These materials would have enabled Internet access to be provided to individuals by unlimited satellites (he was particularly looking at helping Cuban Jewish associations), thereby creating platforms beyond the control of the Cuban authorities. Havana, in turn, considered these attempts as manifestations of the American strategy to destabilize the existing regime, based on the model of the Orange Revolution in the Ukraine in 2004 or the Green Revolution in Iran in 2009. In late December 2011, the Cuban government announced the liberation of nearly 3,000 prisoners (including 86 foreigners from 25 countries)<sup>52</sup>. Alan Gross was not among them.

The enemy is also anyone who, in the eyes of the Cuban authorities, is on the side of foreign powers. According to the Cuban authorities, the US pays individuals to carry out informational operations (propaganda, anti-Cuban comments on Cuban blogs, etc.) aimed at tarnishing the image of the country, its government and its people. Cyberspace is no longer the vector of globalization, but one of globalization

---

51 Cited in <http://som.csudh.edu/fac/lpress/devnat/nations/cuba/cubassy.htm>.

52 “Cuba, libération prochaine de près de 3000 prisonniers”, *Le Monde*, December 24, 2011, (Cuba: forthcoming liberation of nearly 3,000 prisoners). [http://www.lemonde.fr/ameriques/article/2011/12/24/cuba-liberation-de-pres-de-3-000-prisonniers\\_1622576\\_3222.html](http://www.lemonde.fr/ameriques/article/2011/12/24/cuba-liberation-de-pres-de-3-000-prisonniers_1622576_3222.html)

based on incessant plots or maneuvers for destabilization, conceived by capitalist regimes.

The statements of speaker Eduardo Fontes Tato Suarez<sup>53</sup> and the points made in the documentary “Razones de Cuba”<sup>54</sup> (Cuban Reasons) broadcast on March 21, 2011 on Cuban television provide some information on the Cuban perspective on cyber-warfare, and particularly the role played by the American giant in the counter-revolutionary propaganda conveyed in cyberspace. It is clearly in the field of rhetoric that the cyber-conflict between Cuba and its adversaries is played out, rather than the field of hacking *per se*. These statements affirm that:

- Technology itself is not a threat – it is the usage made of it that poses a danger.

- The enemy is American. The situation worsened under the Bush administration, which put more means in place to monitor Cuba. The G. Bush Institute organized a conference to draw up a strategy for cyber-warfare against countries the US considers to be their enemies, including Cuba. Freedom House<sup>55</sup> is an organization supported by the American government to finance the subversion of Cuba. The first cyber-war waged by the US army that we know of took place in Yugoslavia.

- Cyber-warfare against Cuba began when the US decided to keep the island under 24-hour surveillance, similar to that with China and Iran.

- The US is master of the Internet; it has technological domination but, paradoxically, maintains an information block against Cuba.

- The majority of the content of the cyber-war against Cuba consists of demonizing socialism. Within these statements, we can distinguish the theme of an international plot, with multiple ramifications. Communication companies are financed by the US; the Spanish newspaper *El País* maintains an incessant press campaign against Cuba; all the foreign press appears to be allied against Cuba, refusing to tell the truth about the pressure, the war waged by the US against the Cuban people; the deletion of CubaDebate from Facebook<sup>56</sup> was an example of an act of cyber-war. Thus, the speaker assimilates cyber-war and information war, news war, media war (lack of debate, lack of truth, truncated reality, etc.).

---

53 This talk is available on video at the following addresses: <http://observers.france24.com/fr/content/20110218-cours-magistral-cyber-contre-revolution-agent-secret-cubain-fidel-Castro-raul-twitter-fuite> or <http://vimeo.com/19402730>.

54 See the “Ciberguerra” episode in the *Las Razones de Cuba* series broadcast on March 21, 2011: <http://www.cubadebate.cu/noticias/2011/03/21/vea-el-capitulo-ciberguerra-de-la-serie-las-razones-de-cuba-video/>.

55 <http://www.freedomhouse.org/>.

56 <http://www.facebook.com/cubadebate.en>.

– The threat is not merely an external one – the enemy is within as well, in the person of the counter-revolutionary bloggers. The action of these cyber-mercenaries consists of sowing discord within the country using ICTs. They are paid by the US by way of diverse forms of recompense and bonuses. Yoani Sanchez is the figurehead of these mercenary bloggers in the pay of the foreign foe. According to Eduardo Fontes Tato Suarez, the Generación Y blog<sup>57</sup> wishes to prove that its discourse comes from within the country although it is entirely dreamt up abroad. He reproaches the blog for conveying a false image of social reality in Cuba: the blog gives the impression that the populace is on the point of revolt, the country on the point of imploding, its quest is to destroy a project rather than consolidate it. The majority of Cuban bloggers are ones who respect the spirit of the revolution and receive no funding from abroad. The ‘mercenary’ Ernesto Hernandez Busto, Suarez claims, proposed an invasion by the US Army as a solution for Cuba.

The ‘cyber-warfare’ referred to in Cuban political discourse essentially stems from psychological warfare. It concerns the use of ideas space by foreign forces<sup>58</sup> (the American enemy, channeled through its vassals the world over), attempting to place and maneuver their pawns (mercenaries, traitors to the revolutionary project) within a system (Cuban society) in order to destabilize it. It mentions that Cuba is subject to surveillance by the ECHELON network (which has a base in Guantanamo) [STR 09].

## 2.7. Conclusion

Cuba’s policy for the management of cyberspace answers to a logic which has been in place from the very dawn of the Internet in Cuba. Fidel Castro stepped aside for his brother, Raul, to take power in February 2008. The transition was not accompanied by far-reaching reforms in terms of freedom of access to information, which would lead the country a fair way down the road to democracy promulgated by its American neighbor. The new high-capacity link does not guarantee an increase in the number of access points, or the relaxation of the policy of control and surveillance. Hence, restrictions are still in force, as are limitations on the number of access points, control of access by the identification of Internet users and high access costs. Usage restrictions open up the Web to categories that are politically favorable to the regime, and access is mainly limited to public places and institutions, as was the case more than 10 years ago [DRA 00], even from the time of the application of Decree 209 in June 1996, stipulating that Internet access would

---

57 <http://www.desdecuba.com/generaciony/>.

58 A particularly good example of this strategy of influence can be seen in the setting up of Radio Marti in 1985, aimed at the Cuban population. A study conducted in 2009 shows that 2% of Cubans listen to this station. A report on the subject was published by the GAO in 2009 [GAO 09].

be selective, and that priority would be given to institutions that were useful to the country's development [KAL 01].

State control remains complete: the official political line is opposed to total freedom of the press, in the sense that we understand it in Western countries. The State still holds control over industrialists in the domain of new ICTs; and the development of infrastructure and content is guided by the State and not by the law of the market. The Cuban regime is standing in the way of what could constitute a factor of democratization by the introduction of the Internet<sup>59</sup>.

In fact, the Cuban authorities manage to get around the dilemma: they stay away from economic globalization; they do not fully enter into the digital society, and are instrumentalizing technology by way of centralized control (*instrumentalist approach*), although this approach is not as radical as that of North Korea, which forbids the public any access to the Web [KO 09]. Cuba has adopted an intermediary position on the scale of control of the Internet in authoritarian countries: North Korea imposes total blockage of the Internet, China has opened up its Internet although control and surveillance are the order of the day; Cuba is positioned between the two, and may be qualified as a moderate model [KO 09]. We also see in the Cuban model that a State's Internet strategy is not formulated independently. Beyond technological dependence, which most of the world's countries share in, economic and political considerations are such that they will influence choices made in the very long term. Is the Cuban strategy not ultimately an expression of a lack of confidence in the actual stability of the regime?<sup>60</sup> Clearly, the administration does not think itself able to withstand the ideological assaults of the outside world. As long as this uncertainty persists, Cuban cyberspace will remain under-dimensioned and under State control.

---

59 Note, finally, that State interference in the functioning of the Internet, control of the flow of information, cut-off of networks, etc., are not – and have never been – characteristic only of authoritarian regimes. A recent study [HOW 11] indicates that 39% of such 'incidents' can be attributed to democracies, 6% to emerging democracies, and 52% to authoritarian regimes and unstable States, over the period 1995–2011. Over an extended period, it seems that all types of regimes are increasingly tempted to interfere. The reasons proposed are many: protection of political authorities (i.e. of political leaders, institutions, national security, etc.), preservation of the public good (religious morale, culture, social/racial harmony, protection of minors, defense of privacy, fight against crime, etc.). This does not have the effect the authorities had hoped – in fact it results in the strengthening of links between the local and global society, and innovation in the means of getting around the restrictions.

60 Kyngmin Ko *et al.* [KO 09] hypothesize that when a country is confident in the solidity of its regime and its ability to hold power, and displays genuine economic ambitions, it does not deprive itself of Internet, it controls and profits from it. On the other hand, when a country is concerned for its political stability, it takes reactive and defensive measures, to the detriment of economic potential. The first scenario would seem to correspond to China, and the second to Cuba.

The relatively aggressive American discourse about the strategy of democratizing the world using the Internet [CLI 10] would not tend to incite authoritarian regimes to open up further. However, like any restrictive strategy, Cuba's is faced with an inventive or a confrontational spirit from people dreaming up means to circumvent the tools of control and censure, and all forms of limitations (costs and lack of access to technology). In addition, the State is under considerable outside pressure:

- the embargo imposed by the US;
- limiting technological dependence in the absence of any national industry in the field of new ICTs likely to produce genuine solutions of substitution<sup>61</sup>;
- active opponents abroad;
- influential and critical bloggers, even on Cuban soil; and
- accusations of anti-American plotting and of alliance with States that are undesirable in the eyes of democracies.

The international tensions that are becoming increasingly manifest in cyberspace do not spare Cuba, which is accused of participation in the planning of terrorist actions. In early December 2011, the American press<sup>62</sup> hinted at Cuba's involvement in a vast network including Iran, Mexico and Venezuela, intended to carry out cyber-attacks against the US (nuclear installations, the CIA, the White House, the FBI, etc.). The theory of the Iranian Islamist plot, using South America to create a terrorist network, may be part of the new order in international politics, in which the

---

61 Most nations on the planet are now dependent on the technologies, protocols and applications developed in the US, and that form the backbone of cyberspace. For a number of States this situation of dependence is critical, because it involves giving up parts of their national sovereignty. Those States that have not been able to equip themselves with industries they control, both at the levels of software and hardware, find themselves at an *impasse* if they refuse to open their markets to foreign companies to compensate for what they lack. Cuba does not totally refuse, but the decision to open its market is taken grudgingly, and it is at a very slow pace that the country is gaining access to cyberspace. This State strategy, however, has the result of confining the populace a little more to the past. Its leaders admire the virtues of the Internet in the world, but refuse to accept the risks in their own back yard. Yet, as we have seen, this slow advance into the global society of Web 2.0 is not synonymous with a lack of capability in the field of information warfare and cyber-warfare. While Cuba does not actually have all the capabilities and skills, it could undoubtedly acquire them or subcontract part of the task, e.g. as North Korea does with China. Power in the cybernetic domain can be found in a country's alliances, however, this always entails a degree of dependence.

62 A documentary aired by the Hispanic-American channel Univision on December 8, 2012, which describes the organization of an international network headed by Iran, and connecting parties in Mexico, Cuba and Venezuela. Cyber-attacks, according to the documentary, were to be launched from Mexico. The main parties in the plot would be diplomats and university students. Fact or fiction?

cybernetic dimension will have a not insignificant part to play. Is Cuba sufficiently well armed against this new form of conflict facing states in cyberspace?

The concept of active cyber-defense is not ground-breaking in terms of Cuba's defense strategy. Should the training of a new generation of experts (courses at the UCI, the Ciudad Digital Avanzada, etc.) be viewed as the project constituting new defensive forces, or technological emancipation with a view to participating more actively in cyberspace? It should be noted that the army seems to be absent from the debate on cyber-warfare. We are not aware of any official project to create a military cyber-unit, or a strategy or doctrine of cyber-defense.

## 2.8. Bibliography

- [BOA 00] BOAS T.C., "The dictator's dilemma?", in: *The Internet and U.S. Policy toward Cuba, Center for Strategic and International Studies*, MIT, The Washington Quarterly, pp. 57-67, summer 2000, USA.
- [CAS 01] CASTRO F., *Las armas son y siempre serán el arma más importante*, speech, Santiago de Cuba, Cuba, December 2, 2001, available at: <http://usuarios.tinet.cat/mpgp/amigos953.htm>.
- [CAS 03] CASTRO F., *El símbolo de la globalización neoliberal ha recibido un colosal golpe*, speech, Faculty of Law, Buenos Aires, Argentina, May 26, 2003, available at: [http://www.smaldone.com.ar/documentos/docs/fidel\\_argentina.html](http://www.smaldone.com.ar/documentos/docs/fidel_argentina.html).
- [CIA 11] CIA, World Factbook 2011, available at: <https://www.cia.gov/library/publications/the-world-factbook/geos/cu.html>, 2011.
- [CLI 10] Clinton H., speech, January 21, 2010, US Department of State, Washington, USA, available at: <http://www.state.gov/secretary/rm/2010/01/135519.htm>.
- [CRU 11] CRUZ A., *Cuban Hackers Working for Venezuela's Hugo Chavez*, Blog, November 29, 2011, available at: <http://babalublog.com/2011/11/cuban-hackers-working-for-venezuelas-hugo-chavez/>.
- [DRA 00] DRAKE W.J., Kalathil Sh., Cargenie T.B., "Dictatorships in the digital age: some considerations on the Internet in China and Cuba", *The Magazine on Information Impacts*, October 2000.
- [FRE 09] FREEDOM HOUSE, *Freedom on the Net: A Global Assessment of Internet and Digital Media*, Report, Freedom House, USA, April 1, 2009
- [FRE 11] FREEDOM HOUSE, *Freedom on the Net 2011*, Freedom House, USA, 2011, available at: <http://www.freedomhouse.org/images/File/FofN/FOTN2011.pdf>.
- [GAO 09] GENERAL ACCOUNTING OFFICE, *Actions are needed to improve strategy and operations*, Report GAO-09-127, GAO, February 5, 2009, available at: <http://www.gao.gov/assets/290/284998.pdf>