

# Cuban Agent Communications Failure of a Perfect System

DIRK RIJMENANTS

**Abstract** The Cuban Intelligence Service has a long record of broadcasting encrypted numbers messages by shortwave radio to communicate with its clandestine agents abroad. Although it is considered a secure way to communicate covertly, there have been espionage cases where the use of this type of communication provided hard physical evidence, resulting in criminal complaints and convictions.

**Keywords** Cuba, Numbers Stations, cryptography, one-time pad, espionage, “Atencion” radio station, Dirección General de Inteligencia (DGI), Cuban Intelligence Service (CuIS), Federal Bureau of Investigation (FBI), Ana Belen Montes, Carlos and Elsa Alvarez, Walter Kendall Myers, Gwendolyn Myers

## Cuban Intelligence

The United States is the principal foreign target of the Cuban Intelligence Service (CuIS). Therefore, it is no surprise that CuIS officers and agents, recruited and controlled by CuIS in the United States, are important targets of the counter-intelligence efforts of the FBI. In recent years, the FBI has uncovered several important Cuban spy operations.

One common link between all recent spy cases is how these agents received their operational messages. Apparently, the clandestine communication methods, presented in this paper, are standard CuIS procedures. Despite CuIS using a cryptographic system, proven to be unbreakable, the FBI did succeed in reading some of these operational messages and subsequently used them in court.

This paper is based on official FBI documents and the court papers on these espionage cases. It shows procedural and implementation flaws by the CuIS and its agents. These flaws resulted in incriminating evidence that contributed to arrest and the conviction of the clandestine agents.

## The Cases

In 2001, Ana Belen Montes was arrested and charged with espionage while working as a senior US Defense Intelligence Agency (DIA) analyst. The federal prosecutors stated: "Montes communicated with the Cuban Intelligence Service through encrypted messages and received her instructions through encrypted shortwave transmissions from Cuba".<sup>1</sup>

In 2006, Florida International University professor Carlos Alvarez and his wife Elsa Alvarez were charged with espionage and acting as illegal agents for Cuba. The U.S. District Court Florida stated: "defendants would receive assignments via shortwave radio transmissions".<sup>2 3</sup>

In 2009, U.S. State Department official Walter Kendall and his wife Gwendolyn Steingraber Myers were arrested on charges of serving as illegal agents of the Cuban government for nearly 30 years. They acknowledged having received encrypted messages from the Cuban Intelligence via a shortwave radio they possessed.<sup>4 5</sup>

Although these illegal agents had a common method of receiving operational instructions from CuIS, it was not the way they communicated that led to the investigations, surveillance and ultimately, their arrest. As usual, operational errors, their behaviour, their outspoken opinion or thorough profiling by law enforcement raised some red flags with the Federal investigators. A cryptographic system, considered perfectly secure, provided evidence in all cases. These spies were by no means stupid or foolish but educated intellectuals. How does this "perfect" system work and why did it fail?

## Numbers on Shortwave

A common method, used by CuIS to communicate with its agents in the United States, is to broadcast encrypted messages with powerful shortwave transmitters that are located in Cuba. These messages are series of numbers in voice or Morse. The clandestine agent writes down these numbers and decrypts them into readable text, providing him with instructions on gathering intelligence, exchange of information, operational activities or meetings with his so-called handler, the Intelligence Officer, responsible for maintaining personal contact with that agent.<sup>6</sup>

The transmitters that are used for these broadcasts are commonly known as numbers stations and Cuba's most active station is nicknamed "Atencion", named after its prelude, spoken by a Spanish female voice. This prelude enables the agent to precisely tune in on the station. Each message consists of a header with three groups, given during the "Atencion" prelude and repeated for three minutes, followed by 150 groups of five figures, spoken by the synthesized female voice.<sup>7 8</sup>

The advantage of such numbers stations is obvious. Shortwave broadcasts can carry messages over very long distances, to agents far away in foreign countries. Anyone with a simple commercial shortwave receiver can receive these broadcasts. Because it is impossible to find out who is receiving these messages, numbers stations are an ideal way to securely communicate covertly with illegal agents.

Numbers stations were used extensively in the Second World War. The British Special Operations Executive (SOE), the American Office of Strategic Services (OSS) and other intelligence agencies used them to communicate with their espionage and sabotage teams, operating behind enemy lines. During the Cold War, numbers stations remained popular with many intelligence agencies, to send instructions to their agents or agent handlers in foreign countries. Covert communications by shortwave radio has proven very secure and has been used successfully for many decades.<sup>9</sup>

## Encrypted Messages

Before they are broadcast, the operational messages are encrypted into unintelligible series of numbers by applying a crypto algorithm. Usually, such messages are encrypted with a one-time pad, a system that has been proven unbreakable if properly used<sup>10</sup>. The system that is used by the CuLS to encrypt its numbers messages is not revealed in the FBI affidavits. The fact that the agents received diskettes, rather than keys or passwords, and the difficulty the FBI had in deciphering the shortwave messages without access to the proper keys, leads us to the common practice of one-time pad encryption.

The one-time pad system is quite simple and easy to apply with nothing more than a pencil and paper. Both sender and receiver have identical keys, called one-time pads. These pads are series of truly random digits, printed on sheets of a small booklet, microfilm or any other carrier that is easily hidden and destroy. If a pad is used only once, and destroyed immediately after use, the encryption will be mathematically unbreakable.

Before encryption, the plain text must be converted into digits. There are many ways to do this, but a so-called straddling checkerboard is the most economic and common method. In the Ana Belen Montes case, the FBI found a "cheat sheet", provided by Cuban intelligence, which helped Montes to convert the decrypted messages back into plaintext.<sup>11</sup>

Montes' checkerboard

	<b>4</b>	<b>3</b>	<b>6</b>	<b>7</b>	<b>0</b>	<b>1</b>	<b>8</b>
	A	T	I	L	N	E	S
<b>2</b>	B	C	D	F	G	H	J
<b>5</b>	K	M	Ñ	O	P	Q	R
<b>9</b>	U	V	W	X	Y	Z	

To convert the frequently used letters, located in the top row, we take the digit above the letter: "A" = 4, "T" = 3, and so on. The less frequent letters in the other rows are composed with the digit of the row, followed by digit of the column: "B" = 24, "P" = "50" and so on.

Let use convert the message "UN MENSAJE SECRETO" into digits:

U N - M E N S A J E - S E C R E T O  
 94 0 98 53 1 0 8 4 28 1 98 6 1 23 58 1 3 57

After converting the plaintext into groups of digits (the last group is completed with nulls), the one-time pad is subtracted from the plaintext without borrowing (e.g.  $5 - 7 = 15 - 7 = 8$ ).

Plaintext	94098	53108	42819	86123	58135	70000
One-time pad	-58941	23658	86474	02009	32584	87901
Ciphertext	46157	30550	66445	84124	26651	93109

The ciphertext message is broadcast by shortwave radio. The receiving agent writes down the ciphertext. Next, he writes the proper one-time pad underneath the ciphertext and adds ciphertext and one-time pad together without carry (e.g..  $4 + 9 = 3$  and not 13). The agent uses the checkerboard to re-convert the digits into readable text.

As long as both sender and receiver keep their one-time pads secret and destroy these pads after one-time use, the encryption is unbreakable. How did this simple yet solid encryption method go so wrong that it helped to convict the illegal agents who used it?

## Ana Belen Montes

Ana Belen Montes (° 1957) studied at the University of Virginia, earning a degree in Foreign Affairs, and finished a master's at Johns Hopkins University's School of Advanced International Studies. In 1985 she started working at the Department of Justice in Washington. Her outspoken opinion on the U.S. policies towards Latin American countries caught the attention of Cuban officials. Soon after, Montes was recruited by the CuIS. In 1985, Montes applied for a position at the Defense Intelligence Agency (DIA). Over the years, she became the top senior analyst on Cuban matters, with access to secret Sensitive Compartmented Information (SCI)<sup>12</sup>.

In 1996, a DIA colleague reported to a security official that he felt Montes might have contact with Cuban intelligence. The case was filed. However, when four years later the FBI was searching after a Cuban agent in Washington, the official contacted the FBI and an investigation was opened.<sup>13</sup>

That same year, Montes was instructed by the CuIS to purchase a laptop and she received computer diskettes to decipher radio messages and mailings from the CuIS. She used a shortwave radio to listen to messages, broadcast by the Cuban "Atencion" numbers station<sup>14</sup>. The series of numbers were then deciphered on her computer into readable text with the help of the diskettes from CuIS<sup>15</sup>. Each radio message consisted of 150 groups of five figures<sup>16</sup>, the typical "Atencion" format<sup>17</sup>.

Montes also received diskettes to encipher messages or stolen classified information on her home desktop computer and her laptop. The enciphered messages were then stored on other diskettes, which she gave directly or indirectly to her handler<sup>18</sup>. She was also instructed to use a program called "WIPE" (secure file deleting software) every time she deciphered or enciphered something on her laptop.<sup>19</sup> To arrange meetings and exchange of diskettes, she called a pager number using pre-paid calling cards and she used pre-assigned pager codes to convey a particular message.<sup>20</sup>

It is clear that the FBI had no problem in collecting enough evidence. During a surreptitious entry into Montes' residence, the FBI found the laptop and copied its hard drive. During FBI analysis of the hard drive copy, they recovered substantial portions of deleted text<sup>21</sup>. The FBI found fragments of instructions on how to receive ciphered messages. One part stated "Here the program decipheres the message and it retrieves the text onto the screen"<sup>22</sup>. The FBI now knew that Montes received numbers messages and that she deciphered them on her computer. Montes was arrested in September 2001.

How could this operation go wrong? Using an agent's computer to process agent-handler communications was the first major mistake CuIS made. No single computer is secure and information, processed on a computer, is often stored in temporary files or memory swap files. This data resides on a hard drive, even after normal deletion. Although instructed by CuIS to use the WIPE program, she apparently did not use the program consistently or the program did not perform properly. This is not an operational error from her side, but a procedural mistake from CuIS. The CuIS should have implemented fail-safe security measures, rather than assuming that the agent is capable of following strict security procedures. Just because an agent is highly educated, it does not mean that he or she is fully aware of the importance of seemingly futile security measures. Moreover, using a computer for such clandestine purposes is always a bad idea, as truly secure deletion is not always guaranteed. Also, the agent might "clean" his computer, but forget to thoroughly delete some diskette or a thumb drive.

Further analysis revealed a second major mistake by the CuIS. The hard disk contained a series of 150 five-digit groups<sup>23</sup>. With a suspected link to Cuban Intelligence, it was evident

that this was a message, broadcast by a Cuban numbers station. FBI and other agencies archive vast quantities of intercepted communications. The "Atencion" station is one of them. Encrypted message fragments on the hard drive were compared with archived "Atencion" messages and found to be identical with a message, broadcast in 1999 by a Spanish speaking woman at a shortwave frequency<sup>24</sup>.

It is incomprehensible that the CuIS decided to use a software version of a most secure manual enciphering system, instead of instructing its agent to decipher the numbers messages manually. The manual process is an important advantage of one-time pad, as it permits easy and secure destruction (for instance burning) of the one-time pads and sheets that were used to perform the deciphering. A software deciphering method also requires the one-time pads to be stored on diskettes or other digital media. The agent must hide these digital media, just as he would have to do with paper one-time pads. However, such digital media are much harder to destroy or delete without leaving traces. A basic rule of one-time pad is that a key is used only once and properly destroyed after use. Remanence of readable deciphered messages is also an obvious mistake. By using a computer and diskettes, it is inevitable that copies of the deciphering disks or the readable text unintentionally reside on a hard drive and data carriers.

The reason for CuIS using a software version is unclear. Montes had an aid, a checkerboard "cheat sheet", to manually decipher messages<sup>25</sup>. There was no need to process large quantities of text, as each individual message never contained more than 150 groups. The manual deciphering process is very simple and easy to learn. It takes no more than 30 to 40 minutes to decipher a message of 150 groups. Sometimes, codes are used to shorten a message. A short code can replace all kinds of long words or entire phrases. Possibly, the deciphering software contained some additional codebook conversion table that helped to swiftly decipher the digits and convert short codes into readable text. This would require a deciphering diskette that also contains a codebook list. If additional codebook-to-word conversion was required, the agent could just as well use a small hidden codebook on paper instead of hiding a diskette. The only logical reason for using a software one-time pad encryption is convenience and speed, hardly decisive reasons when security is paramount.

The CuIS also instructed Montes to type her messages and reports onto her personal computer and to encipher them with another diskette, provided by CuIS, before handing them directly or indirectly (by brush-pass or dead-drop) to her CuIS handler<sup>26</sup>. Although not directly related to the shortwave messages, this again reveals the irresponsible use of computers and software. In agent-to-handler communications, convenience and speed might indeed have been a reason to use software enciphering, as the quantity of text (information and reports), written by Montes, undoubtedly was much more than the short operational instructions that were sent to her by shortwave. Nevertheless, it was a very bad idea, as the hard disk analysis by the FBI showed.

The information, obtained from the copied hard drive, enabled the FBI to build a case against Ana Belen Montes. If CuIS had instructed Montes to decipher the messages manually and if another method was devised to pass the information from Montes to her handler, there would have hardly been direct physical evidence. Montes never removed any documents from work, electronically or in hard copy. Instead, she kept the details in her head, went home and typed them up on her laptop<sup>27</sup>. Therefore, no compromising classified documents were seized in her house. The use of public pay phones and pre-paid calling cards might seem suspicious, as Montes had a cell phone and telephone at home<sup>28</sup>. However, this doesn't provide hard espionage evidence. Telephone records probably linked the pager number to Cuba affiliated persons, or possibly to Cuban intelligence, but would only prove she had contact with this person.

## Carlos and Elsa Alvarez

Carlos Alvarez (° 1944) and his wife Elsa Alvarez (° 1950) were both born in Cuba. Carlos Alvarez became American citizen in 1972, Elsa in 1979. Carlos Alvarez was an associate professor at Florida International University. He began passing information to the CuIS in 1977. Elsa was a social worker and Florida International University counsellor. Carlos and Elsa married in 1980. Elsa Alvarez began working for the CuIS in 1982 and had been independently spying for the Cuban government before she teamed up with her husband<sup>29</sup>.

They used their academic positions as covers to spy for the Cuban government. The couple transmitted information about the Cuban exile community in Miami on behalf of the Cuban Dirección General de Inteligencia (DGI). CuIS instructed them to gather information on prominent people, community attitudes, political developments and current events of interest to the Cuban government<sup>30</sup>. Only Carlos Alvarez possessed the technical capability to encrypt and decrypt the messages from and to the CuIS. The messages from CuIS contained tasking for both him and his wife, and the messages, encrypted and sent by Carlos Alvarez contained reports of both him and his wife.<sup>31</sup>

Carlos and Elsa Alvarez communicated with the CuIS in a variety of ways. They also received assignments via shortwave radio transmission<sup>32</sup>. These messages were encoded in five-digit groupings. Once received, these messages were deciphered on their home computer with decryption software on a diskette, provided by CuIS. Using a similar diskette, this time equipped with encryption technology, Carlos Alvarez would send coded communiqués back to his supervisors at the Cuban Directorate of Intelligence. This would be accomplished through mailing an encrypted computer diskette to postal mailboxes throughout the United States. Carlos Alvarez was primarily responsible for intercepting and deciphering the shortwave radio messages and would burn notes and other physical evidence of these messages after each transmission. Additionally, Alvarez attempted to erase all electronic or digital evidence from the computer that he used to communicate in code. Carlos and Elsa Alvarez used the codenames David and Deborah.<sup>33</sup>

In 2005, the FBI started monitoring the couple after a tip-off. In June and July 2005 they gave separate confessions to FBI agents about their alleged spying activities<sup>34</sup>. The FBI examined Carlos Alvarez' home computer. During analysis of the computer hard drive, the experts found remnants of coded messages, sent by Carlos Alvarez to CuIS. This home computer was used during the encryption and decryption process of the communications.<sup>35</sup> Series of fragmentary messages, found on the hard drive, were of a format similar to the messages that are known to be sent by CuIS to its agents and agent handlers. The messages used five-digit numbers and were signed "David and Deborah", the codenames of Carlos and Elsa Alvarez. During a search of the Alvarez house, the FBI found a shortwave radio antenna of the type, used by other Cuban operatives. In January 2006, they were arrested for passing information to the Cuban DGI.<sup>36</sup>

The Alvarez case has many similarities with the Ana Belen Montes case. In both cases, the clandestine agents were observed for several months after a tip-off. During these observations, the FBI collected enough evidence to charge them with espionage and search their houses. Carlos Alvarez also use his personal computer and diskettes, provided by CuIS, to decipher the messages he received by shortwave radio. Alvarez was very cautious and made sure to always burn written papers and erase all related files on his computer. Nevertheless, he failed to erase all remnants from his computer<sup>37</sup>. Again, a secure cryptographic method was applied inappropriately on an insecure computer. It is inexplicable why the CuIS still continued to instruct its clandestine agents to use a software version of a secure manual encryption method and, even worse, let them use their own computers to encrypt and decrypt the incoming and outgoing messages.

## Walter Kendall Myers

Walter Kendall Myers (° 1937) served in the Army Security Agency (ASA) from 1959 until 1962, receiving intensive communications training. He went to Brown University and earned a Ph.D. from Johns Hopkins University. In 1977, Kendall Myers began working for the US State Department at the Foreign Service Institute while being a part-time faculty member at Johns Hopkins' School of Advanced International Studies. From 2000 until his retirement in October 2007 he worked as a European analyst in the Bureau of Intelligence and Research (INR). He held a Top Secret/Sensitive Compartmented Information (SCI) security clearance. His wife Gwendolyn Steingraber Myers (° 1938) worked at the Riggs National Bank as an Administrative Analyst in Management Information Systems<sup>38</sup>.

In 1978, Kendall Myers and his wife travelled for personal and academic purposes to Cuba on an invitation from a Cuban government official, belonging to the Cuban Mission to the United States<sup>39</sup>. Kendall Myers expressed a strong affinity towards Cuba and its revolutionary goals, and a negative sentiment toward "American imperialism". An opinion he expressed on several occasions in the public<sup>40</sup>. This trip provided Cuban Intelligence with the opportunity to develop Kendall Myers as a Cuban agent<sup>41</sup>. In 1995, Kendall Myers and his wife travelled to Cuba via Mexico for a clandestine meeting with Fidel Castro<sup>42</sup>. The Myers had regular personal meetings with their CuIS handlers during visits to Trinidad and Tobago, Jamaica, Brazil, Ecuador, Argentina, and Mexico<sup>43</sup>. They held contact with their handlers by e-mail<sup>44</sup>. Kendall Myers, who knew Morse, also received operational instructions through enciphered messages, sent in Morse or in voice, on a portable shortwave radio (the same brand as Ana Belen Montes' shortwave radio)<sup>45</sup>.

Kendall Myers preferred to take classified information from his work at INR by memorizing it or by taking notes<sup>46</sup>. The information was mostly passed hand-to-hand or by a so-called brush-pass, directly or indirectly to their handler.<sup>47</sup> They also received several e-mails from a CuIS contact, an art dealer in Mexico<sup>48</sup>. From January 2002 until 2005 the Myers began meeting CuIS contacts outside the United States. This was probably a precaution by CuIS after the arrest of Ana Belen Montes in September 2001<sup>49</sup>.

Based on general information provided by the FBI, Diplomatic Security (DS) started in 2006 a comprehensive internal investigation that resulted in the identification of Kendall Myers as a probable Cuban agent<sup>50</sup>. In 2009, the FBI started an undercover operation. The Myers were both retired at that time. An FBI undercover source approached the Myers and told them he was sent by a known Cuban Intelligence officer to contact them and get some information<sup>51</sup>. Walter Kendall Myers agreed to meet the undercover source and to provide the requested information. During a series of personal meetings, and believing they were talking to a genuine CuIS officer, they revealed their 30 years of espionage activities for Cuba and various operational details<sup>52</sup>. Among the operational details were the use of a shortwave radio<sup>53</sup>, e-mail communications with their handlers and their own code names<sup>54</sup>.

According to the affidavit, the FBI collected enciphered messages that were sent by shortwave broadcasts from the CuIS in Cuba to CuIS officers and agents abroad. The FBI identified that some of these messages, in the period 1996 – 1997, were broadcast to a CuIS handler of the Myers<sup>55</sup>. The affidavit does not reveal how the FBI succeeded in reading the content of the messages. The numerous deciphered shortwave radio messages contained operational details and indirect references to the Myers<sup>56</sup>. A specific medical problem of an agent codenamed "E-634" in a message coincided with a medical procedure Gwendolyn Myers underwent<sup>57</sup>. In several messages CuIS mentioned the agent codenames "123", "202" and "GOD". During meetings between the undercover source and the Myers, Gwendolyn Myers told the source that her codename was "123" and Walter Kendall Myers confirmed that

his codenames were “202” and “GOD”. In one message, the handler was instructed to train “634” in the use of an IOMEGA data storage device<sup>58</sup>.

The FBI also identified the e-mails from the Mexican art dealer called “Peter” to the Myers’ home e-mail account, sent from December 2008 throughout 2009<sup>59</sup>. During the meetings with the undercover source, Kendall Myers confirmed that “Peter” was one of his contacts with CuIS<sup>60</sup>. An analysis of Kendall Myers’ Department of State work computer also showed that, between August 2006 and October 2007, he had viewed more than 200 classified intelligence reports on Cuba, 75 of them not mentioning the countries Kendall Myers was responsible for<sup>61</sup>. Walter Kendall Myers and Gwendolyn Steingraber Myers were arrested in June 2009. Their arrest was the culmination of a three-year joint FBI/Department of State Diplomatic Security investigation.

The Myers case is an example of connecting the dots and how poor communications security indirectly can lead to the arrest of an illegal agent. The undercover operation and the incriminating talks the Myers had with the undercover source were only to confirm the investigation results. Again, shortwave radio communication was used to receive operational instructions from CuIS. However, in this case, the FBI did not succeed in decrypting or identifying the communications between CuIS and the Myers.

Nevertheless, the FBI did present plaintext excerpts from shortwave radio messages in court. The FBI collects shortwave broadcasted messages from Cuban Intelligence to Cuban officers and their agents. Already in November 2006, some of these messages were identified as destined to a CuIS handler of clandestine agents<sup>62</sup>. This was probably the first important lead, found by Diplomatic Security and the FBI. It is unknown how they obtained these plaintext messages but, in view of the Montes and Alvarez cases, and knowing that the deciphering of the shortwave numbers messages is unlikely without access to the proper decryption diskettes<sup>63</sup>, we can assume that the handler also used his computer in the decryption process (a standard CuIS procedure) and that his messages were seized or surreptitiously retrieved by FBI at some point in the search for a Cuban agent.

The rest of the case is connecting dots. The Myers fitted the profile and personal details, revealed in the handler’s messages. This enabled the FBI to zoom in on the Myers. The failure of communications between CuIS and its handler indirectly lead to the arrest of illegal agents that otherwise might never have been detected. From what we learn from the court documents, the communication between CuIS and the Myers was never compromised and, according to their talks with the undercover source, they were always very cautious in their contacts with CuIS. That is, until they bluntly accepted a stranger they encountered as a Cuban Intelligence Officer.

## **Conclusions**

The Ana Belen Montes case clearly shows how you can turn a perfectly secure pencil-and-paper encryption scheme into an insecure computer application. Decrypting the low volume shortwave messages manually, with one-time pads on paper or microfilm, easy to destroy, would have provide secure communications. Cuban Intelligence obviously did not realize that, by switching from manual to software encryption, they had to consider new and most difficult software security issues. It is a textbook example of not putting together the knowledge of cryptology, software development, security, and operational procedures. The separate solutions were good, but the combination of the different solutions (unbreakable encryption, software and computers) unintentionally produced evidence. The Carlos Alvarez case also shows this false confidence in the application of cryptographic tools on computers. Moreover, it shows that, although the details of the Montes case were publicly available, CuIS did not conclude that it is inappropriate to use normal computers to run cryptographic

software and they did not switch to manual pencil-and-paper deciphering or, less elaborate, secure dedicated computers or electronic cryptographic devices (the latter however difficult to hide). Despite the experience with the Montes and Alvarez case, CuS again showed negligence in its encrypted agent communications with the handler of Kendall Myers, this time indirectly causing the apprehension of one of their longest running agents.

All three cases show that the method of sending one-time pad messages by shortwave radio is very secure. None of the involved agents were caught because they received encrypted messages. None of the messages were decrypted by the FBI and their content was unknown until the seizure of the hard drives or diskettes. All agents came under investigation because of other reasons (tip-offs and indirect leads). As with VENONA, the Cuban numbers messages are mistakenly referred to as a case where one-time pad encryption was broken. They were not. However, bad implementation of a most secure encryption method and operational mistakes were the real reason that law enforcement obtained hard evidence. It is not because one uses a theoretically perfect system that he will use it properly or that he is experienced enough to deal with the corresponding security issues.

v007

---

<sup>1</sup> FBI affidavit in support of complaint and arrest warrant charging Ana Belen Montes, 2001,  
Link: [http://www.fas.org/irp/ops/ci/Montes\\_092101.pdf](http://www.fas.org/irp/ops/ci/Montes_092101.pdf)

Hereinafter FBIMONTES

<sup>2</sup> U.S. District Court Southern District of Florida, The United States vs Carlos Alvarez and Elsa Alvarez, Governments Omnibus Response To Defendants' Pre-trial Detention Appeals,  
Link: <http://www.latinamericanstudies.org/espionage/alvarez-prosecution.pdf>

Hereinafter USALVARES

<sup>3</sup> United States vs Carlos Alvarez and Elsa Alvarez, U.S. Sentencing Memorandum  
Link: <http://www.latinamericanstudies.org/espionage/alvarez-sentence.pdf>

Hereinafter CENTALVAREZ

<sup>4</sup> U.S. District Court for the District of Columbia, The United States vs. Walter Kendall Myers and Gwendolyn Steingraber Myers, 2009

Link: <http://cryptome.org/myers/myers-012.pdf>

Hereinafter USCOLUMBMYERS

<sup>5</sup> FBI affidavit in support of criminal complaint and arrest warrant charging Walter Kendall Myers, 2009

Link: <http://cryptome.org/myers/myers-004.pdf>

Hereinafter FBIMYERS

<sup>6</sup> FBIMONTES, II, A, par 11

<sup>7</sup> Simon Mason, Shortwave Espionage: Cuban Numbers Stations

Link: <http://www.simonmason.karoo.net/page354.htm>

<sup>8</sup> SpyNumbers.com Numbers Stations Monitoring (search database by Attention ENIGMA code "V2" for latest logs)

Link: <http://www.spynumbers.com/enigmaV2.htm>

<sup>9</sup> Dirk Rijmenants, Cipher Machines and Cryptology, Papers: "Spies and Numbers, Here to Stay", 2009

Link: [http://users.telenet.be/d.rijmenants/papers/spies\\_and\\_numbers.pdf](http://users.telenet.be/d.rijmenants/papers/spies_and_numbers.pdf)

<sup>10</sup> Dirk Rijmenants, Cipher Machines and Cryptology, History of One-time Pads

Link: <http://users.telenet.be/d.rijmenants/en/onetimepad.htm>

<sup>11</sup> FBI Headline Archives, 2008. Link: [http://www.fbi.gov/page2/sept08/montes\\_091208.html](http://www.fbi.gov/page2/sept08/montes_091208.html)

<sup>12</sup> FBIMONTES, I, par 10

<sup>13</sup> FBI Headline Archives, 2008. Link: [http://www.fbi.gov/page2/sept08/montes\\_091208.html](http://www.fbi.gov/page2/sept08/montes_091208.html)

<sup>14</sup> FBIMONTES, II, A, par 19

<sup>15</sup> FBIMONTES, II, A, par 18

<sup>16</sup> FBIMONTES, II, A, par 19

<sup>17</sup> Simon Mason, Shortwave Espionage: Cuban Numbers Stations

Link: <http://www.simonmason.karoo.net/page354.htm>

<sup>18</sup> FBIMONTES, II, B, par 20

<sup>19</sup> FBIMONTES, II, A, par 16

<sup>20</sup> FBIMONTES, III, par 24

<sup>21</sup> FBIMONTES, II, A, par 14

- 
- <sup>22</sup> FBIMONTES, II, A, par 18  
<sup>23</sup> FBIMONTES, II, A, par 19  
<sup>24</sup> FBIMONTES, II, A, par 19  
<sup>25</sup> FBI Headline Archives, 2008 Link: [http://www.fbi.gov/page2/sept08/montes\\_091208.html](http://www.fbi.gov/page2/sept08/montes_091208.html)  
<sup>26</sup> FBIMONTES, II, B, par 22  
<sup>27</sup> FBI Headline Archives, 2008 Link: [http://www.fbi.gov/page2/sept08/montes\\_091208.html](http://www.fbi.gov/page2/sept08/montes_091208.html)  
<sup>28</sup> FBIMONTES, III, par 45  
<sup>29</sup> USALVARES, II, Facts, p 3, information based on sealed indictment  
<sup>30</sup> CENTALVAREZ p 3-5  
<sup>31</sup> CENTALVAREZ p 2  
<sup>32</sup> CENTALVAREZ p 2  
<sup>33</sup> USALVARES II, Facts, p 4-5, information based on sealed indictment  
<sup>34</sup> Miami Herald, Jan, 10, 2006 Link: <http://www.latinamericanstudies.org/espionage/alvarez-spies.htm>  
<sup>35</sup> USALVARES, II, Facts, p 6, information based on sealed indictment  
<sup>36</sup> USALVARES, II, Facts, p 2, information based on sealed indictment  
<sup>37</sup> USALVARES, II, Facts, p 4, information based on sealed indictment  
<sup>38</sup> FBIMYERS par 8 - 13  
<sup>39</sup> FBIMYERS par 29  
<sup>40</sup> FBIMYERS par 30  
<sup>41</sup> FBIMYERS par 31  
<sup>42</sup> FBIMYERS par 54  
<sup>43</sup> FBIMYERS par 52  
<sup>44</sup> FBIMYERS par 56  
<sup>45</sup> FBIMYERS par 37, 38  
<sup>46</sup> FBIMYERS par 67  
<sup>47</sup> FBIMYERS par 42  
<sup>48</sup> FBIMYERS par 56, 57  
<sup>49</sup> FBIMYERS par 52  
<sup>50</sup> US Department of State, Press Release on Arrest of Walter Kendall Myers, June 5, 2009  
Link: <http://www.state.gov/r/pa/prs/ps/2009/06a/124404.htm>  
<sup>51</sup> FBIMYERS par 40  
<sup>52</sup> FBIMYERS par 41  
<sup>53</sup> FBIMYERS par 41  
<sup>54</sup> FBIMYERS par 42  
<sup>55</sup> FBIMYERS par 44  
<sup>56</sup> FBIMYERS par 45  
<sup>57</sup> FBIMYERS par 47  
<sup>58</sup> FBIMYERS par 48-51  
<sup>59</sup> FBIMYERS par 56-59  
<sup>60</sup> FBIMYERS par 41, 43  
<sup>61</sup> FBIMYERS par 67  
<sup>62</sup> FBIMYERS par 48  
<sup>63</sup> FBIMONTES, II, A, par 11