How to Hack an Election

Andrés Sepúlveda rigged elections throughout Latin America for almost a decade. He tells his story for the first time.

By Jordan Robertson, Michael Riley, and Andrew Willis | March 31, 2016
Photographs by Juan Arredondo

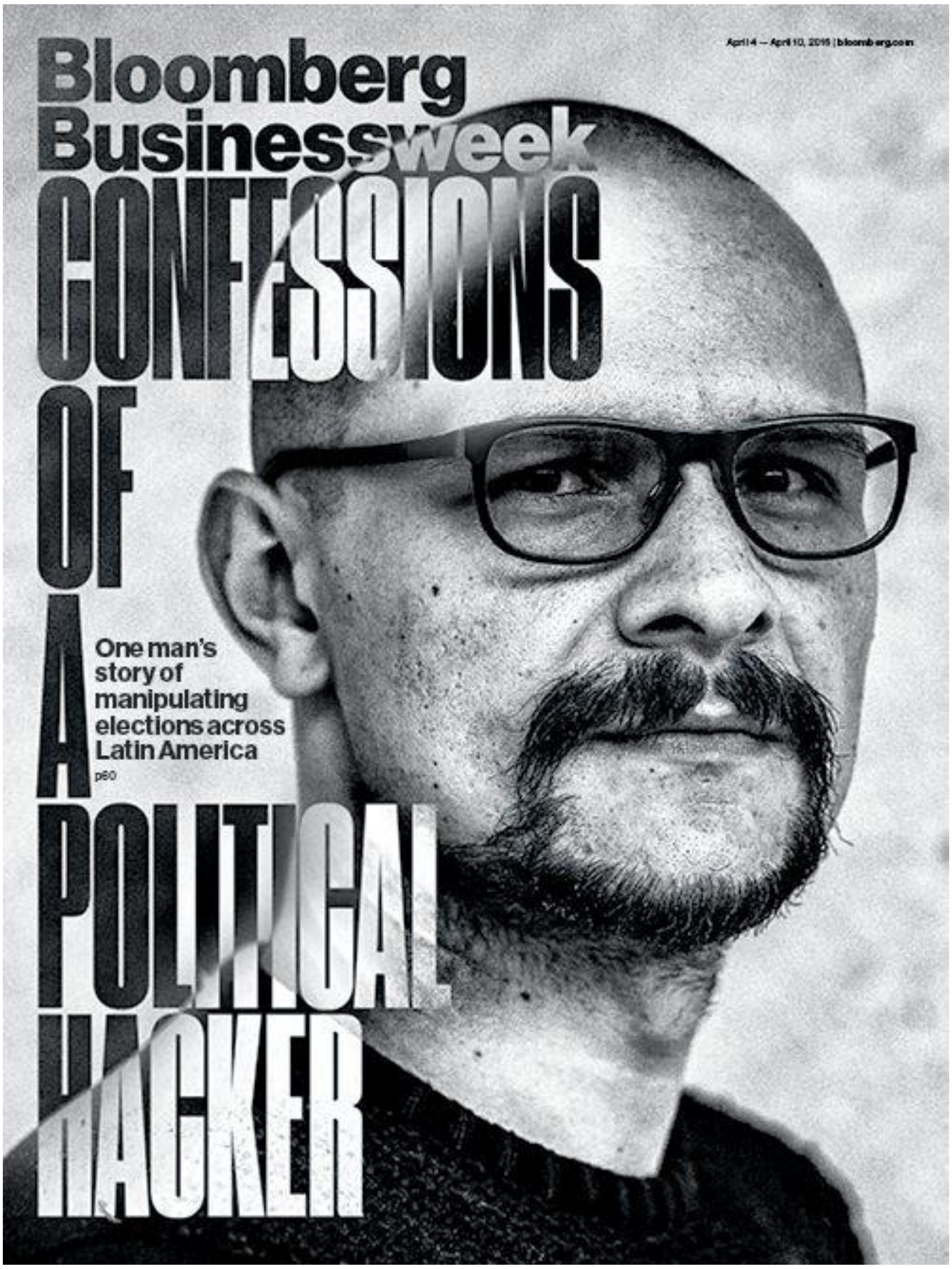
https://www.bloomberg.com/features/2016-how-to-hack-an-election/

From

Versión en español

It was just before midnight when Enrique Peña Nieto declared victory as the newly elected president of Mexico. Peña Nieto was a lawyer and a millionaire, from a family of mayors and governors. His wife was a telenovela star. He beamed as he was showered with red, green, and white confetti at the Mexico City headquarters of the Institutional Revolutionary Party, or PRI, which had ruled for more than 70 years before being forced out in 2000. Returning the party to power on that night in July 2012, Peña Nieto vowed to tame drug violence, fight corruption, and open a more transparent era in Mexican politics.

Two thousand miles away, in an apartment in Bogotá's upscale Chicó Navarra neighborhood, Andrés Sepúlveda sat before six computer screens. Sepúlveda is Colombian, bricklike, with a shaved head, goatee, and a tattoo of a QR code containing an encryption key on the back of his head. On his nape are the words "</head>" and "<body>" stacked atop each other, dark riffs on coding. He was watching a live feed of Peña Nieto's victory party, waiting for an official declaration of the results.


April 4 — April 10, 2016 | bloomberg.com
Bloomberg Businessweek
CONFESSIONS OF A POLITICAL HACKER
One man's story of manipulating elections across Latin America
p60

Featured in *Bloomberg Businessweek*, April 4, 2016. Subscribe now.

When Peña Nieto won, Sepúlveda began destroying evidence. He drilled holes in flash drives, hard drives, and cell phones, fried their circuits in a microwave, then broke them to shards with a hammer. He shredded documents and flushed them down the toilet and erased servers in Russia and Ukraine rented anonymously with Bitcoins. He was dismantling what he says was a secret history of one of the dirtiest Latin American campaigns in recent memory.

For eight years, Sepúlveda, now 31, says he traveled the continent rigging major political campaigns. With a budget of $600,000, the Peña Nieto job was by far his most complex. He led a team of hackers that stole campaign strategies, manipulated social media to create false waves of enthusiasm and derision, and installed spyware in opposition offices, all to help Peña Nieto, a right-of-center candidate, eke out a victory. On that July night, he cracked bottle after bottle of Colón Negra beer in celebration. As usual on election night, he was alone.

Sepúlveda's career began in 2005, and his first jobs were small—mostly defacing campaign websites and breaking into opponents' donor databases. Within a few years he was assembling teams that spied, stole, and smeared on behalf of presidential campaigns across Latin America. He wasn't cheap, but his services were extensive. For $12,000 a month, a customer hired a crew that could hack smartphones, spoof and clone Web pages, and send mass e-mails and texts. The premium package, at $20,000 a month, also included a full range of digital interception, attack, decryption, and defense. The jobs were carefully laundered through layers of middlemen and consultants. Sepúlveda says many of the candidates he helped might not even have known about his role; he says he met only a few.

His teams worked on presidential elections in Nicaragua, Panama, Honduras, El Salvador, Colombia, Mexico, Costa Rica, Guatemala, and Venezuela. Campaigns mentioned in this story were contacted through former and current spokespeople; none but Mexico's PRI and the campaign of Guatemala's National Advancement Party would comment.

As a child, he witnessed the violence of Colombia's Marxist guerrillas. As an adult, he allied with a right wing emerging across Latin America. He believed his hacking was no more diabolical than the tactics of those he opposed, such as Hugo Chávez and Daniel Ortega.

Many of Sepúlveda's efforts were unsuccessful, but he has enough wins that he might be able to claim as much influence over the political direction of modern Latin America as anyone in the 21st century. "My job was to do actions of dirty war and psychological operations, black propaganda, rumors—the whole dark side of politics that nobody knows exists but everyone can see," he says in Spanish, while sitting at a small plastic table in an outdoor courtyard deep within the heavily fortified offices of Colombia's attorney general's office. He's serving 10 years in prison for charges including use of malicious software, conspiracy to commit crime, violation of personal data, and espionage, related to hacking during Colombia's 2014 presidential election. He has agreed to tell his full story for the first time, hoping to convince the public that he's rehabilitated—and gather support for a reduced sentence.

Usually, he says, he was on the payroll of Juan José Rendón, a Miami-based political consultant who's been called the Karl Rove of Latin America. Rendón denies using Sepúlveda for anything illegal, and categorically disputes the account Sepúlveda gave *Bloomberg Businessweek* of their relationship, but admits knowing him and using

him to do website design. “If I talked to him maybe once or twice, it was in a group session about that, about the Web,” he says. “I don’t do illegal stuff at all. There is negative campaigning. They don’t like it—OK. But if it’s legal, I’m gonna do it. I’m not a saint, but I’m not a criminal.” While Sepúlveda’s policy was to destroy all data at the completion of a job, he left some documents with members of his hacking teams and other trusted third parties as a secret “insurance policy.”
Sepúlveda provided *Bloomberg Businessweek* with what he says are e-mails showing conversations between him, Rendón, and Rendón’s consulting firm concerning hacking and the progress of campaign-related cyber attacks. Rendón says the e-mails are fake. An analysis by an independent computer security firm said a sample of the e-mails they examined appeared authentic. Some of Sepúlveda’s descriptions of his actions match published accounts of events during various election campaigns, but other details couldn’t be independently verified. One person working on the campaign in Mexico, who asked not to be identified out of fear for his safety, substantially confirmed Sepúlveda’s accounts of his and Rendón’s roles in that election.

Sepúlveda says he was offered several political jobs in Spain, which he says he turned down because he was too busy. On the question of whether the U.S. presidential campaign is being tampered with, he is unequivocal. “I’m 100 percent sure it is,” he says.

Sepúlveda grew up poor in Bucaramanga, eight hours north of Bogotá by car. His mother was a secretary. His father was an activist, helping farmers find better crops to grow than coca plants, and the family moved constantly because of death threats from drug traffickers. His parents divorced, and by the age of 15, after failing school, he went to live with his father in Bogotá and used a computer for the first time. He later enrolled in a local technology school and, through a friend there, learned to code.

In 2005, Sepúlveda’s older brother, a publicist, was helping with the congressional campaigns of a party aligned with then-Colombian President Alvaro Uribe. Uribe was a hero of the brothers, a U.S. ally who strengthened the military to fight the Revolutionary Armed Forces of Colombia (FARC). During a visit to party headquarters, Sepúlveda took out his laptop and began scanning the office’s wireless network. He easily tapped into the computer of Rendón, the party’s strategist, and downloaded Uribe’s work schedule and upcoming speeches. Sepúlveda says Rendón was furious—then hired him on the spot. Rendón says this never happened.

For decades, Latin American elections were rigged, not won, and the methods were pretty straightforward. Local fixers would hand out everything from small appliances to cash in exchange for votes. But in the 1990s, electoral reforms swept the region. Voters were issued tamper-proof ID cards, and nonpartisan institutes ran the elections in several countries. The modern campaign, at least a version North Americans might recognize, had arrived in Latin America.

Rendón had already begun a successful career based partly, according to his critics—and more than one lawsuit—on a mastery of dirty tricks and rumormongering. (In 2014, El Salvador's then-President Carlos Mauricio Funes accused Rendón of orchestrating dirty war campaigns throughout Latin America. Rendón sued in Florida for defamation, but the court dismissed the case on the grounds that Funes couldn't be sued for his official acts.) The son of democracy activists, he studied psychology and worked in advertising before advising presidential candidates in his native Venezuela. After accusing then-President Chávez of vote rigging in 2004, he left and never went back.

Sepúlveda's first hacking job, he says, was breaking into an Uribe rival's website, stealing a database of e-mail addresses, and spamming the accounts with disinformation. He was paid $15,000 in cash for a month's work, five times as much as he made in his previous job designing websites.

Sepúlveda was dazzled by Rendón, who owned a fleet of luxury cars, wore big flashy watches, and spent thousands on tailored coats. Like Sepúlveda, he was a perfectionist. His staff was expected to arrive early and work late. "I was very young," Sepúlveda says. "I did what I liked, I was paid well and traveled. It was the perfect job." But more than anything, their right-wing politics aligned. Sepúlveda says he saw Rendón as a genius and a mentor. A devout Buddhist and practitioner of martial arts, according to his own website, Rendón cultivated an image of mystery and menace, wearing only all-black in public, including the occasional samurai robe. On his website he calls himself the political consultant who is the "best paid, feared the most, attacked the most, and also the most demanded and most efficient." Sepúlveda would have a hand in that.

Rendón, says Sepúlveda, saw that hackers could be completely integrated into a modern political operation, running attack ads, researching the opposition, and finding ways to suppress a foe's turnout. As for Sepúlveda, his insight was to understand that voters trusted what they thought were spontaneous expressions of real people on social media more than they did experts on television and in newspapers. He knew that accounts could be faked and social media trends fabricated, all relatively cheaply. He wrote a software program, now called Social Media Predator, to manage and direct a virtual army of fake Twitter accounts. The software let him quickly change names, profile pictures, and biographies to fit any need. Eventually, he discovered, he could manipulate the public debate as easily as moving pieces on a chessboard—or, as he puts it, "When I realized that people believe what the Internet says more than reality, I discovered that I had the power to make people believe almost anything.”

Sepúlveda's head. The upper tattoo is a QR code containing an encryption key.

According to Sepúlveda, his payments were made in cash, half upfront. When he traveled, he used a fake passport and stayed alone in a hotel, far from campaign staff. No one could bring a smartphone or camera into his room.

Most jobs were initiated in person. Sepúlveda says Rendón would give him a piece of paper with target names, e-mail addresses, and phone numbers. Sepúlveda would take the note to his hotel, enter the data into an encrypted file, then burn the page or flush it down the toilet. If Rendón needed to send an e-mail, he used coded language. To "caress" meant to attack; to "listen to music" meant to intercept a target's phone calls.

Rendón and Sepúlveda took pains not to be seen together. They communicated over encrypted phones, which they replaced every two months. Sepúlveda says he sent daily progress reports and intelligence briefings from throwaway e-mail accounts to a go-between in Rendón's consulting firm.

Each job ended with a specific, color-coded destruct sequence. On election day, Sepúlveda would purge all data classified as "red." Those were files that could send him and his handlers to prison: intercepted phone calls and e-mails, lists of hacking victims, and confidential briefings he prepared for the campaigns. All phones, hard drives, flash drives, and computer servers were physically destroyed. Less-sensitive "yellow" data—travel schedules, salary spreadsheets, fundraising plans—were saved to an encrypted thumb drive and given to the campaigns for one final review. A week later it, too, would be destroyed.

For most jobs, Sepúlveda assembled a crew and operated out of rental homes and apartments in Bogotá. He had a rotating group of 7 to 15 hackers brought in from across Latin America, drawing on the various regions' specialties. Brazilians, in his view, develop the best malware. Venezuelans and Ecuadoreans are superb at scanning systems and software for vulnerabilities. Argentines are mobile intercept artists. Mexicans are masterly hackers in general but talk too much. Sepúlveda used them only in emergencies.

The assignments lasted anywhere from a few days to several months. In Honduras, Sepúlveda defended the communications and computer systems of presidential candidate Porfirio Lobo Sosa from hackers employed by his competitors. In Guatemala, he digitally eavesdropped on six political and business figures, and says he delivered the data to Rendón on encrypted flash drives at dead drops. (Sepúlveda says it was a small job for a client of Rendón's who has ties to the right-wing National Advancement Party, or PAN.

The PAN says it never hired Rendón and has no knowledge of any of his claimed activities.) In Nicaragua in 2011, Sepúlveda attacked Ortega, who was running for his third presidential term. In one of the rare jobs in which he was working for a client other than Rendón, he broke into the e-mail account of Rosario Murillo, Ortega's wife and the government's chief spokeswoman, and stole a trove of personal and government secrets.

In Venezuela in 2012, the team abandoned its usual caution, animated by disgust with Chávez. With Chávez running for his fourth term, Sepúlveda posted an anonymized YouTube clip of himself rifling through the e-mail of one of the most powerful people in Venezuela, Diosdado Cabello, then president of the National Assembly. He also went outside his tight circle of trusted hackers and rallied Anonymous, the hacktivist group, to attack Chávez's website.

Dirty Work

Colombia

Supported reelection of Alvaro Uribe for president, 2006; congressional elections, 2006; failed campaign of Oscar Iván Zuluaga for president, 2014

Honduras

Supported Porfirio Lobo Sosa, elected president 2009

Nicaragua

Against Daniel Ortega, 2011

Mexico

Supported Enrique Peña Nieto, over a three-year period

Venezuela

Against Chávez and Maduro in 2012 and 2013

Costa Rica

Supported Johnny Araya, failed presidential candidate for center-left National Liberation Party, 2014 election

Panama

Supported Juan Carlos Navarro, presidental candidate for the center-left Democratic Revolutionary Party, 2014 election

After Sepúlveda hacked Cabello's Twitter account, Rendón seemed to congratulate him. "*Eres noticia* :)"—you're news—he wrote in a Sept. 9, 2012, e-mail, linking to a story about the breach. (Rendón says he never sent such an e-mail.) Sepúlveda provided screen shots of a dozen e-mails, and many of the original e-mails, showing that from November 2011 to September 2012 Sepúlveda sent long lists of government websites he hacked for various campaigns to a senior member of Rendón's consulting firm, lacing them with hacker slang ("Owned!" read one). Two weeks before Venezuela's presidential election, Sepúlveda sent screen shots showing how he'd hacked Chávez's website and could turn it on and off at will.

Chávez won but died five months later of cancer, triggering an emergency election, won by Nicolás Maduro. The day before Maduro claimed victory, Sepúlveda hacked his Twitter account and posted allegations of election fraud. Blaming "conspiracy hackings from

abroad," the government of Venezuela disabled the Internet across the entire country for 20 minutes.
In Mexico, Sepúlveda's technical mastery and Rendón's grand vision for a ruthless political machine fully came together, fueled by the huge resources of the PRI. The years under President Felipe Calderón and the National Action Party (also, as in Partido Acción Nacional, PAN) were plagued by a grinding war against the drug cartels, which made kidnappings, street assassinations, and beheadings ordinary. As 2012 approached, the PRI offered the youthful energy of Peña Nieto, who'd just finished a successful term as governor.

Sepúlveda didn't like the idea of working in Mexico, a dangerous country for involvement in public life. But Rendón persuaded him to travel there for short trips, starting in 2008, often flying him in on his private jet. Working at one point in Tabasco, on the sweltering Gulf of Mexico, Sepúlveda hacked a political boss who turned out to have connections to a drug cartel. After Rendón's security team learned of a plan to kill Sepúlveda, he spent a night in an armored Chevy Suburban before returning to Mexico City.

Mexico is effectively a three-party system, and Peña Nieto faced opponents from both right and left. On the right, the ruling PAN nominated Josefina Vázquez Mota, its first female presidential candidate. On the left, the Democratic Revolution Party, or PRD, chose Andrés Manuel López Obrador, a former Mexico City mayor.

Early polls showed Peña Nieto 20 points ahead, but his supporters weren't taking chances. Sepúlveda's team installed malware in routers in the headquarters of the PRD candidate, which let him tap the phones and computers of anyone using the network, including the candidate. He took similar steps against PAN's Vázquez Mota. When the candidates' teams prepared policy speeches, Sepúlveda had the details as soon as a speechwriter's fingers hit the keyboard. Sepúlveda saw the opponents' upcoming meetings and campaign schedules before their own teams did.

Money was no problem. At one point, Sepúlveda spent $50,000 on high-end Russian software that made quick work of tapping Apple, BlackBerry, and Android phones. He also splurged on the very best fake Twitter profiles; they'd been maintained for at least a year, giving them a patina of believability.

Sepúlveda managed thousands of such fake profiles and used the accounts to shape discussion around topics such as Peña Nieto's plan to end drug violence, priming the social media pump with views that real users would mimic. For less nuanced work, he had a larger army of 30,000 Twitter bots, automatic posters that could create trends. One conversation he started stoked fear that the more López Obrador rose in the polls, the lower the peso would sink. Sepúlveda knew the currency issue was a major vulnerability; he'd read it in the candidate's own internal staff memos.

Just about anything the digital dark arts could offer to Peña Nieto's campaign or important local allies, Sepúlveda and his team provided. On election night, he had computers call tens of thousands of voters with prerecorded phone messages at 3 a.m. in the critical swing state of Jalisco. The calls appeared to come from the campaign of popular left-wing gubernatorial candidate Enrique Alfaro Ramírez. That angered voters—that was the point—and Alfaro lost by a slim margin. In another governor's race, in Tabasco, Sepúlveda set up fake Facebook accounts of gay men claiming to back a conservative Catholic candidate representing the PAN, a stunt designed to alienate his base. "I always suspected something was off," the candidate, Gerardo Priego, said recently when told how Sepúlveda's team manipulated social media in the campaign.

In May, Peña Nieto visited Mexico City's Ibero-American University and was bombarded by angry chants and boos from students. The rattled candidate retreated with his bodyguards into an adjacent building, hiding, according to some social media posts, in a bathroom. The images were a disaster. López Obrador soared.

The PRI was able to recover after one of López Obrador's consultants was caught on tape asking businessmen for $6 million to fund his candidate's broke campaign, in possible violation of Mexican laws. Although the hacker says he doesn't know the origin of that particular recording, Sepúlveda and his team had been intercepting the communications of the consultant, Luis Costa Bonino, for months. (On Feb. 2, 2012, Rendón appears to have sent him three e-mail addresses and a cell phone number belonging to Costa Bonino in an e-mail called "Job.") Sepúlveda's team disabled the consultant's personal website and directed journalists to a clone site. There they posted what looked like a long defense written by Costa Bonino, which casually raised questions about whether his Uruguayan roots violated Mexican restrictions on foreigners in elections. Costa Bonino left the campaign a few days later. He indicated recently that he knew he was being spied on, he just didn't know how. It goes with the trade in Latin America: "Having a phone hacked by the opposition is not a novelty. When I work on a campaign, the assumption is that everything I talk about on the phone will be heard by the opponents."

The press office for Peña Nieto declined to comment. A spokesman for the PRI said the party has no knowledge of Rendón working for Peña Nieto's or any other PRI campaign. Rendón says he has worked on behalf of PRI candidates in Mexico for 16 years, from August 2000 until today.

Juan José Rendón, political consultant.

Photographer: El Comercio/GDA/ZUMA PRESS

In 2012, Colombian President Juan Manuel Santos, Uribe's successor, unexpectedly restarted peace talks with the FARC, hoping to end a 50-year war. Furious, Uribe, whose father was killed by FARC guerrillas, created a party and backed an alternative candidate, Oscar Iván Zuluaga, who opposed the talks.

Rendón, who was working for Santos, wanted Sepúlveda to join his team, but Sepúlveda turned him down. He considered Rendón's willingness to work for a candidate supporting peace with the FARC a betrayal and suspected the consultant was going soft, choosing money over principles. Sepúlveda says he was motivated by ideology first and money second, and that if he wanted to get rich he could have made a lot more hacking financial systems than elections. For the first time, he decided to oppose his mentor.

Sepúlveda went to work for the opposition, reporting directly to Zuluaga's campaign manager, Luis Alfonso Hoyos. (Zuluaga denies any knowledge of hacking; Hoyos couldn't be reached for comment.) Together, Sepúlveda says, they came up with a plan to discredit the president by showing that the guerrillas continued to traffic in drugs and violence even as they talked about peace. Within months, Sepúlveda hacked the phones and e-mail accounts of more than 100 militants, including the FARC's leader, Rodrigo Londoño, also known as Timochenko. After assembling a thick file on the FARC, including evidence of the group's suppression of peasant votes in the countryside, Sepúlveda agreed to accompany Hoyos to the offices of a Bogotá TV news program and present the evidence.

It may not have been wise to work so doggedly and publicly against a party in power. A month later, Sepúlveda was smoking on the terrace of his Bogotá office when he saw a caravan of police vehicles pull up. Forty black-clad commandos raided the office to arrest him. Sepúlveda blamed his carelessness at the TV station for the arrest. He believes someone there turned him in. In court, he wore a bulletproof vest and sat surrounded by guards with bomb shields. In the back of the courtroom, men held up pictures of his family, making a slashing gesture across their throats or holding a hand over their mouths—stay silent or else. Abandoned by former allies, he eventually pleaded guilty to espionage, hacking, and other crimes in exchange for a 10-year sentence.

Three days after arriving at Bogotá's La Picota prison, he went to the dentist and was ambushed by men with knives and razors, but was saved by guards. A week later, guards woke him and rushed him from his cell, saying they had heard about a plot to shoot him with a silenced pistol as he slept. After national police intercepted phone calls revealing yet another plot, he's now in solitary confinement at a maximum-security facility in a rundown area of central Bogotá. He sleeps with a bulletproof blanket and vest at his bedside, behind bombproof doors. Guards check on him every hour. As part of his plea deal, he says, he's turned government witness, helping investigators assess possible cases against the former candidate, Zuluaga, and his strategist, Hoyos. Authorities issued an indictment for the arrest of Hoyos, but according to Colombian press reports he's fled to Miami.

When Sepúlveda leaves for meetings with prosecutors at the Bunker, the attorney general's Bogotá headquarters, he travels in an armed caravan including six motorcycles speeding through the capital at 60 mph, jamming cell phone signals as they go to block tracking of his movements or detonation of roadside bombs.

In July 2015, Sepúlveda sat in the small courtyard of the Bunker, poured himself a cup of coffee from a thermos, and took out a pack of Marlboro cigarettes. He says he wants to tell his story because the public doesn't grasp the power hackers exert over modern elections or the specialized skills needed to stop them. "I worked with presidents, public figures with great power, and did many things with absolutely no regrets because I did it with full conviction and under a clear objective, to end dictatorship and socialist governments in Latin America," he says. "I have always said that there are two types of politics—what people see and what really makes things happen. I worked in politics that are not seen."

Sepúlveda says he's allowed a computer and a monitored Internet connection as part of an agreement to help the attorney general's office track and disrupt drug cartels using a version of his Social Media Predator software. The government will not confirm or deny that he has access to a computer, or what he's using it for. He says he has modified Social Media Predator to counteract the kind of sabotage he used to specialize in, including jamming candidates' Facebook walls and Twitter feeds. He's used it to scan 700,000 tweets from pro-Islamic State accounts to learn what makes a good terror recruiter. Sepúlveda says the program has been able to identify ISIS recruiters minutes after they create Twitter accounts and start posting, and he hopes to share the information with the U.S. or other countries fighting the Islamist group. Samples of Sepúlveda's code evaluated by an independent company found it authentic and substantially original.

Sepúlveda's contention that operations like his happen on every continent is plausible, says David Maynor, who runs a security testing company in Atlanta called Errata Security. Maynor says he occasionally gets inquiries for campaign-related jobs. His company has been asked to obtain e-mails and other documents from candidates' computers and phones, though the ultimate client is never disclosed. "Those activities do happen in the U.S., and they happen all the time," he says.

In one case, Maynor was asked to steal data as a security test, but the individual couldn't show an actual connection to the campaign whose security he wanted to test. In another, a potential client asked for a detailed briefing on how a candidate's movements could be tracked by switching out the user's iPhone for a bugged clone. "For obvious reasons, we always turned them down," says Maynor, who declines to name the candidates involved.

Three weeks before Sepúlveda's arrest, Rendón was forced to resign from Santos's campaign amid allegations in the press that he took $12 million from drug traffickers and passed part of it on to the candidate, something he denies.

According to Rendón, Colombian officials interviewed him shortly afterward in Miami, where he keeps a home. Rendón says that Colombian investigators asked him about Sepúlveda and that he told them Sepúlveda's role was limited to Web development.

Rendón denies working with Sepúlveda in any meaningful capacity. "He says he worked with me in 20 places, and the truth is he didn't," Rendón says. "I never paid Andrés Sepúlveda a peso."

Last year, based on anonymous sources, the Colombian media reported that Rendón was working for Donald Trump's presidential campaign. Rendón calls the reports untrue. The campaign did approach him, he says, but he turned them down because he dislikes Trump. “To my knowledge we are not familiar with this individual,” says Trump’s spokeswoman, Hope Hicks. “I have never heard of him, and the same goes for other senior staff members.” But Rendón says he’s in talks with another leading U.S. presidential campaign—he wouldn’t say which—to begin working for it once the primaries wrap up and the general election begins.

—With Carlos Manuel Rodríguez and Matthew Bristow