**Cyberwar for Sale - The New York Times**

On the morning of May 18, 2014, Violeta Lagunes was perplexed by a series of strange messages that appeared in her Gmail inbox. It was Election Day to choose the leadership of Mexicos Partido Accin Nacional, or PAN, and Lagunes, a former federal congresswoman, was holding a strategy meeting in her office in Puebla city. The emails seemed harmless, at least at first. One appeared to come from the account of a trusted colleague. It asked her to download and review a document. Lagunes clicked on the link, but it seemed to be broken, so she wrote back to her colleague and asked him to send it again. Elsewhere in her inbox was an email from Google warning her that someone had tried to log in to her account. Meanwhile, she began to receive phone calls from PAN allies, who claimed that they had received emails from Laguness account that she did not remember sending. Now Lagunes was worried. Around 1 oclock, she called the colleague who appeared to have emailed her. She reached him at a restaurant, where he was finishing lunch with other campaign allies. I did not send you an email, he insisted. A consultant with the campaign ” who asked to remain anonymous in order to preserve his relationships with other candidates ” overheard the conversation. He knew of other campaign workers who had been receiving similar messages: emails with vague subject lines, asking the recipient to review a document or click a link. The campaign, he realized, had been hacked. In the vote for party leader, Lagunes and her allies in Puebla ” a drive southeast from Mexico City ” were supporting the challenger, a senator who promised to return the party to its conservative roots. But the incumbent was backed by Pueblas powerful governor, Rafael Moreno Valle. One of Mexicos rising political stars, Moreno Valle is close to Mexicos president, Enrique Pe±a Nieto, and has forged an alliance between PAN and Nietos centrist Partido Revolucionario Institucional, or PRI, long the dominant force in Mexican politics. Since winning the governorship in 2010, Moreno Valles opponents say, his ambitions have grown, and he has resorted to increasingly harsh measures to keep Puebla state ” including members of his own party ” under control. In the beginning, the governor was and respectful, Rafael Micalco, a former leader of PAN in Puebla state, told me. When he became governor, he transformed. Now he controls the party through threats. This race to retain control of the party leadership in 2014 was a crucial test for the governor, who was rumored to be considering a run for Mexicos presidency in 2018. (This past September, Moreno Valle publicly announced his intent to run.) Clashes between the two camps were especially intense in Puebla, where backers of the challenger, Ernesto Cordero, claimed that the governor was using public money to support the incumbent, Gustavo Madero, though the governors office has denied these charges. Shortly before the election, Maderos campaign manager said that Corderos side was trying to undermine the legitimacy of the process. Their strategy is clear from the outset, he said in an interview with a Mexican magazine. u2009˜If I win, good. If not, I was cheated. u2009 After Laguness call on Election Day, her colleagues rushed from the restaurant back to their local headquarters, a hotel conference room that they had nicknamed the bunker. All morning, they had been trying to reach their field network, a group of 40 Cordero canvassers who were working to get out the vote in Puebla state. But the field network seemed to have gone dark. Few of the canvassers were even answering their phones. Hackers, the team concluded, must have found the list of the canvassers names and phone numbers ” widely circulated by email within the campaign ” and begun to intimidate them. The day before, the consultant told me, the field network was motivated and eager to do this work. After the hack, it was very hard to reach them. The few who did answer said that they had received phone calls saying that their lives were at stake. They were worried that if they went out, they or their families would get hurt. According to another worker on Corderos campaign, who also requested anonymity, citing fear of reprisal, the message to the canvassers was simple and direct: We know who you are. If you dont want any trouble, shut down your cellphone and stop your activity. The worker added: Its an authoritarian regime. Madero won the election, with 57 percent of the 162, 792 votes cast over all. In Puebla, his margin was substantially larger, roughly 74 percent. Corderos team decided not to contest the result. They had suspicions about how they were hacked. But it would be another year before any evidence emerged. Their political enemies, leaked documents seemed to show, had built a spying operation using software made by an Italian firm called Hacking Team ” just one of many private companies that, largely below public notice, have sprung up to aid governments in surveilling the private lives of individual citizens. The industry claims that its products comply with local laws and are used to fight crime and terror. But in many countries around the world, these tools have proved to be equally adept at political espionage. On average, an American office worker sends and receives roughly 120 emails per day, a number that grows with each passing year. The ubiquity and utility of email has turned it into a record of our lives, rich with mundane and potentially embarrassing details, stored in a perpetual archive, accessible from anywhere on earth and protected, in some cases, by nothing more than a single password. In the case of Violeta Lagunes, her email login represented a point of vulnerability, a seam where the digital walls protecting her campaign were at the mercy of her human judgment ” specifically, whether she could determine if a message from an apparently reputable source was real or fake. Nearly two years later, John Podesta, chairman of Hillary Clintons campaign, was faced with a similar judgment call. An email warned him that someone in Ukraine had tried to access his Gmail account and asked him to click on a button and reset his password. His senior adviser forwarded the email to one of the campaigns technology experts. This is a legitimate email, he replied, in what the expert later would clarify was a simple typing error on his part he meant to say it was not legitimate. The gmail one is REAL, the senior adviser wrote to Podesta and another aide. And so, like Lagunes, Podesta fell into a trap. The button appeared to lead to an official Google page, but it was in fact a meticulously personalized fake, with a domain address linked to a remote cluster of atolls in the South Pacific. The details were designed to trick Podesta into entering his password. This technique is known as spear phishing. It is an especially potent weapon against companies and political organizations because it needs to succeed only one time, against one target. After that, attackers can use the trusted identity of the first compromised account to more easily lure colleagues into opening infected attachments or clicking on malicious links. Not only will a working email password yield years of intraoffice chatter, invoices, bills and confidential memos it can often be leveraged into control of other personal accounts ” Twitter, Facebook, Amazon ” and even access to company servers and internet domains. The Podesta and Lagunes episodes are far from the only cases in which hackers have used information from stolen emails as a weapon against an entire institution. The 2009 Climategate incident, which exposed troves of emails from prominent climate researchers, began when hackers remotely broke into servers at a British university with the help of illicitly obtained passwords. The 2014 hack of internal Sony files, which American officials attributed to the North Korean government, began with a series of emails that attackers then used to dig deeper into Sonys servers. Each hack yielded the most private thoughts and deeds from the members of each respective organization: their blunt insults, their quashed dissents, their plans, their smarmy flattery, all chronicled in time down to the hundredth of the second when the author clicked send. In an earlier era, the hackers might have had to engage in riskier behavior, like bribery or burglary. Now, in many cases, all they had to do was send along a link. The White House, C. I. A. and F. B. I. have all claimed that, based on classified evidence, they can trace the hacks of Podestas email account (and other hacks of people close to the Clinton campaign) back to the Russian government. But with the rise of private firms like Hacking Team, penetrating the email accounts of political opponents does not require the kind of money and expertise available to major powers. A website called Insider Surveillance lists more than a dozen companies selling ethical malware, including Hacking Team and the German firms FinFisher and Trovicor. Compared with conventional arms, surveillance software is subject to few trade controls a recent attempt by the United States to regulate it under a pact called the Wassenaar Arrangement failed. The technology is morally neutral, says Joel Brenner, a former inspector general of the National Security Agency. The same program that you use to monitor your babysitter might be used by Bashar Assad or Abdel Fattah to keep track of whomever they dont like. Hacking Team has fewer than 50 employees, but it has customers all over the world. According to internal documents, its espionage tool, which is called the Remote Control System, or R. C. S. can be licensed for as little as $200, 000 a year ” well within the budget of a provincial strongman. After it has been surreptitiously installed on a targets computer or phone, the Remote Control System can invisibly eavesdrop on everything: text messages, emails, phone and Skype calls, location data and so on. Whereas the N. S. A. s programs grab data in transit from switching rooms and undersea cables, the R. C. S. acquires it at the source, right off a targets device, before it can be encrypted. It carries out an invisible, digitized equivalent of a . The United States government is almost certainly the worlds most formidable repository of hacking talent, but its most powerful cyberweapons are generally reserved for intelligence agencies and the military. This might explain why, according to company documents, at least two federal agencies have been Hacking Team clients: the F. B. I. beginning in 2011, and the Drug Enforcement Administration, beginning in 2012. The F. B. I. contract paid Hacking Team more than $700, 000 the D. E. A. appears to have used the software to go after targets in Colombia. Documents show that the company has also sold its software to some of the worlds most repressive governments. Some, like those of Honduras, Ethiopia, Bahrain, Morocco, Egypt and Saudi Arabia, are Western allies. Other countries, like Uzbekistan and Turkey, have a more troubled relationship. A few are openly hostile to the West. Between 2012 and 2014, Hacking Team was paid nearly one million euros by the government of Sudan, a United state sponsor of terrorism. Even more notable, in light of recent events, is the relationship that Hacking Team carried on with the F. S. B. one of Russias main intelligence agencies. As with Puebla, Hacking Team used a middleman, a research agency called Kvant, to handle its sales to Russia. Between 2012 and 2014, the agency paid Hacking Team 451, 000 euros to license the Remote Control System. Hacking Team claims that it draws the line at customers who commit gross abuses and that it sells exclusively to governments operating within the laws of their own countries. In at least one case, David Vincenzetti, Hacking Teams founder and chief executive, told a salesman to hold off on a potential Mexican client. We sell to official, governmental LEAs ” agencies ” and security agencies ONLY, Vincenzetti wrote in an email. But at other times, a more casual attitude prevailed inside the company. If one sells sandwiches to Sudan, he is not subject, as far as my knowledge goes, to the law, one Hacking Team lawyer wrote in an internal email. Hacking Team should be treated like a sandwich vendor. When asked about its arrangements in various countries, the company responded that it does not comment on confidential business dealings. Its American spokesman, Eric Rabe, did tell me that neither Russia nor Sudan is a current Hacking Team customer. (The relationships, Rabe wrote, ended in 2014, Russia because the Putin government evolved from one considered friendly to the West to a more hostile regime and Sudan because of concerns about the countrys ability to use the system in accordance with the H. T. contract. ) Separately, the company confirmed that the state of Puebla was, in fact, a former client. Until recently, most of what was known about the world of private surveillance companies was a matter of hearsay and speculation. Industry players kept a low profile, operating discreetly from rented offices and meeting potential customers in person a few times a year at carefully screened trade shows. This is why it was so notable when, in July 2015, an unusual tweet appeared in Hacking Teams Twitter feed. Since we have nothing to hide, it read, were publishing all our emails, files and source code. Then came another tweet, with links to a downloadable file called Hacked Team. The file was huge, 420 gigabytes of material scraped from Hacking Teams internal servers. Inside were 33 folders containing the companys contracts, payroll documents, invoices, legal memos, records and a cache of email correspondence from the chief executive on down. Hacking Team had itself been hacked. WikiLeaks pounced on the breach and quickly uploaded the emails into a searchable database. Anyone with an internet connection could now read the chief executive joking about how his company was in the business of selling the evilest technology on earth. You could browse Hacking Teams source code, including one line using bomb\_blueprints. pdf as a placeholder for files that might be found on a targets device. On Reddit, an online peanut gallery formed around the online habits of one Hacking Team engineer and his own notably weak passwords ” HTPassword! P4ssword, Passw0rd. But the most damaging exposures in the leak by far were Hacking Teams client list and the names of some of the clients targets. In South Korea, newspapers focused on evidence suggesting that Hacking Teams software had helped the nations intelligence service rig an election after the leak, one agent who had reportedly used the system there committed suicide. In Ecuador, a magazine found an email with seven phone numbers that the government appeared to have targeted with the R. C. S. Three belonged to lawmakers a fourth to the mayor of Quito all four were members of the opposition party. With the source code for the Remote Control System now public, the company and its clients had to stop using it temporarily. By the end of the year, though, Hacking Team had updated its product and was trying to rebuild its reputation. I was curious whether a company that profited from online breaches could recover from its own. Eric Rabe, the American spokesman, sounded eager to meet me for coffee in Philadelphia. A grandfather and former anchor, he exudes credibility. If you disagree with someone on the internet, he said, of the Hacked Team files, with a wave of his hand, theres no need to have a debate. Just go destroy them. A couple of months later, I went to Milan to visit Hacking Teams headquarters, a stately gray apartment building with boxes of limp flowers adorning a few of its sooty sills. Waiting to demonstrate the companys software were Rabe Philippe Vinci, a company vice president and Alessandro Scarafile, a young engineer. Scarafile had gathered a Dell desktop computer and three smartphones: iPhone, BlackBerry and Android. The screen from his own laptop, which represented the console of a client intelligence agency, was projected on the wall. Several icons represented the various streams of data that could potentially be acquired by gaining control of the targets computer: images from cameras, sound from mikes, screenshots, detailed records of applications opened and bitcoins transferred, a continuous log of location with latitude and longitude, and logs of address books, calendars, phone calls, Skype calls and passwords, as well as websites visited. A key logger recorded every key that was pressed. It was a lot to keep track of. Two other views, called line of events and line of actions, assembled the information into chronological order. Scarafile, who was playing both the customer and the target, or bad guy, turned on the Dell. Judging by the background on the desktop, a gothic scene framed by castlelike silhouettes, our target seemed to be planning a terrorist attack from Transylvania. There are three methods, Scarafile explained, for getting the Remote Control System onto a targets device. Customers can gain physical access to the device and then infect it with a USB stick or memory card. They can beam the R. C. S. in over a network. Or they can send the customer an email and get him to click on an infected attachment ” usually a file from a program like Microsoft Word or PowerPoint. Scarafile did not mention a fourth method, one described by Hacking Teams critics and referred to in its internal emails: the installation of the R. C. S. through a more elaborate process called network injection, which is said to involve pinpointing the targets exact location on the internet, observing the person as he orders up, say, a YouTube cat video, and then serving up a doctored version of the same page, one with the desired cat video playing in the foreground ” YouTube logo and all ” as the R. C. S. discreetly rolls in past the digital gates. Whatever the method of infection, the malicious code, known as an agent, then communicates with its masters anonymously, its dispatches routed through a series of dedicated servers scattered around the world. Even if the target gets suspicious and figures out that something is wrong, this chain of servers makes it nearly impossible for him to figure out exactly who is using Hacking Teams product to spy on him. For the demo, Scarafile opted for the third method, which he referred to as a bit of social engineering. Using the customers computer, he sent the target an email with a Word file attached. Then he returned to the targets computer and on it, just as Lagunes had clicked on the link in her inbox. From now on, he said, this system is currently infected, or monitored, by the Remote Control System. It would remain so even if the suspect turned off his machine or logged out. On the timeline, the target appeared as a stubbly lout in an undershirt, named Jimmy Page . .. head of the terrorist cell. Using Jimmy Pages Dell, Scarafile logged into Pages Gmail, Facebook and Twitter. He opened up Skype, perused Pages criminal colleagues (Don Corleone, Harry Potter, Keyser Soze) and left one of them a voice mail message from Pages phone. Accessing a USB drive attached to the infected computer, Scarafile opened an encrypted file that turned out to contain an order to kill David Vincenzetti. R. C. S. captured it all, including periodic snapshots of Scarafile, as Page, at work. I dont like the words ˜inject and ˜infect,u2009 Vinci, the vice president, said. R. C. S. is deploying the agent into the device of the target because you want to monitor some of his activities. Exactly the way that law enforcement is listening to some of your phone calls, right? Rabe had told me that Vincenzetti was a fighter, and his combative side was apparent from a collage of magazine clippings and printouts taped to the wall beside his desk ” a sort of mood board, like those used in the advertising industry to gather inspiration before the unveiling of a new brand. Vincenzettis mood board, though, wasnt about sneakers or cola. It was about the global struggle for power, which he seemed to envision as one big conflict, a battle between the good guys and the bad guys. On the good side was a photo of the bell that aspiring Navy SEALs can ring should they want to quit the program during Hell Week, and a quote from another entrepreneur that business is war. On the bad side, Vincenzetti had taped up a satellite image showing one of the hottest zones of international tension, the artificial islands rising in the South China Sea, a line of terrestrial pawns advancing Chinas sphere of influence. Beside it was a chart about Iran, depicting how the country could continue to advance its nuclear program despite the recent deal. I think the Iran deal is just terrible, Vincenzetti said, and then added, sarcastically, Oh, its such a very peaceful expansion. Very peaceful. That is not an official company position, Rabe interjected. Vincenzetti, now 48, is a familiar type ” a ferociously competitive, driven entrepreneur whose existence is organized around his work. He has a wife, who was born in Morocco, and no children. His small, eyes can make him seem sleepily blas©. On the morning we met at Hacking Teams offices, he wore jeans, a cardigan and a striped shirt, unbuttoned to midchest. He seemed more comfortable on his feet than sitting down. As we talked in a conference room, he periodically leapt to his feet and stalked around the table, considering in turn the espresso machine, the view from the window, a case of bottled water. If I wanted to break into this room, how would I do it? he asked. There is a door, and there are two windows. He pressed his hands against the glass panes. The perimeter is the first thing you must secure, he continued. Securing data was what he did earlier in his career. Now he had moved on. If you cannot break into a bank, you cannot protect a bank. So when you are in security, really there is no difference between thinking offensively and defensively. In the Vincenzettis parents, a salesman and a schoolteacher, bought him a Commodore 64, one of the earliest personal computers. He soon created a clone, a Tron game and a adventure game. As a student at the University of Milan in the 90s, he became fascinated by cryptography he corresponded with programmers around the world about new cryptographic theories and wrote code for email encryption. In his senior year, he was appointed to administer the universitys internal network, a post that was usually reserved for a graduate student. Vincenzetti remembers these early days as a time when everything was free and no one was trying to harm you. We were wide open and accessible. All the best were called hackers, and I was a hacker. Vincenzetti left university early and founded three companies, all of them focused on defensive cybersecurity. After he founded Hacking Team in 2003, he tried to sell his services to Italian police agencies but found them skeptical that Mafiosi and other criminals would ever bother to encrypt their communications. In Italy, the police were also used to getting whatever they needed through wiretaps, arranged with varying degrees of formality through their contacts at telecommunications firms. But after the 2004 Madrid train bombings, which were coordinated via cellphones and the internet, police officers and intelligence agents not just in Italy but all across Europe became interested in contracting with vendors, part of an emerging arms race over encryption. The growth of Skype made it easy for users to encrypt their communications, and the authorities were eager to pay for countermeasures like the Remote Control System. Singapore, Hacking Teams first client, signed on in 2008. The companys Middle Eastern business took off in 2011, a boom that coincided with the beginning of the Arab Spring. By then, Hacking Team had entered a growth phase, its business driven in part by demand among governments for surveillance tools. According to two former employees, the company held talks with Col. Muammar s chief security officer, who wanted to build a countrywide scheme that could be embedded in every Libyan cellphone. (Rabe would not confirm or deny that this meeting occurred, and added: The company often receives requests to provide services that it does not have available or would sell. ) The United Nations, which prohibits the export of electronic weaponry to Sudan, has investigated Hacking Teams activities there. Nineteen members of the Italian Parliament signed a petition raising the question of whether the Egyptian government might have used the R. C. S. to track Giulio Regeni, a Italian student who appears to have been under government surveillance and whose mutilated body turned up on the side of a road in Egypt last year. Hacking Teams software has not been connected to the case, but the company has done business with the current Egyptian regime. As part of the controversy, the Italian government temporarily revoked Hacking Teams global export license, so that for several months the company had to file a separate application for each of its customers outside the European Union. (When I brought up the Regeni case with Rabe, he called the dead student this Italian national who got himself killed in Egypt. He cited Hacking Teams official policy ” the company neither knows nor desires to know the identities of the people its customers choose to target. There is no evidence that Hacking Teams software had anything to do with Regenis demise, Rabe said.) All Hacking Team customers sign contracts agreeing to comply with local laws. The company says that it vets potential customers and studies reports from journalists and groups, looking for objective evidence or credible concerns that its products are being abused. But when it comes to Hacking Teams own interactions with customers, leaked documents suggest that employees have sometimes turned a blind eye. In the case of the Puebla government and other Latin American customers, Hacking Team employees appeared to ignore warnings suggesting that the Remote Control System was being used to gather intelligence on the political opposition. On multiple occasions, customers emailed Hacking Team attachments with content, including polling data, party registration forms and invitations addressed to and signed by elected officials. Rather than ask what these files had to do with fighting crime and drug trafficking, Hacking Team members simply emailed them back, as requested, with an embedded exploit, turning the document into a surveillance tool to be used against whomever it was sent on to. Asked about these cases, Rabe replied that customers are not supposed to be using it for political purposes, but I dont think its reasonable to expect that an Italian computer programmer, i. e. a support technician, would have seen these files and known what was going on. . .. I think thats a stretch, that an Italian software guy could know that an individual is a dissident. Hacking Teams most persistent critic is Citizen Lab, a research group at the University of Torontos Munk School of Global Affairs. Before the Hacked Team leak, Citizen Lab documented cases in which Hacking Team software turned up on the devices of activists in Morocco and the United Arab Emirates, as well as an journalist in Alexandria, Va. Ronald Deibert, Citizen Labs director, told me that Hacking Team is a company that appears to have no internal controls on abuse of its products. When I asked Vincenzetti about this, he said that Citizen Lab was motivated by money, noting that the group won a grant a week after publishing a report on Hacking Teams sales to Ethiopia. Their identity, he said, is: ˜I am the defender of free speech, I am the defender of liberty and democracy. O. K. So am I. So is every rational guy. If Citizen Lab really cared about good and evil, he said, it would be fighting China and Iran. Almost immediately after the Hacked Team documents went online, they were being pored over by R3D, a Mexico group. Luis Fernando Garc­a, R3Ds director, says that intimidation and online surveillance have increased under Pe±a Nietos presidency, and he took notice when Citizen Lab, in 2014, released a report that traced a chain of servers associated with Hacking Team that routed data through Hong Kong, London, Amsterdam and Atlanta before terminating somewhere inside Mexico. Exactly who was on the receiving end of the traffic and what they were doing with it was unknown at the time, but now R3Ds team recognized that this could be their chance to find out. Shortly thereafter, R3D published three invoices from the Hacked Team cache showing that one state government ” that of Jalisco, on the Pacific Coast ” had paid the company nearly half a million euros for the Remote Control System. Soon other documents were found in the leak to implicate several more states, including Puebla, though most of the states denied ever using the software. (Jalisco later admitted to purchasing the system, which it claimed was for its prosecutors office.) The story failed to get much traction in the Mexican press, except in Puebla, after R3D connected with Lado B, a small collective there. The sites name translates to B Side, as in the back of a hit single ” symbolizing its dedication to telling stories that would otherwise go untold. Lado Bs editor, Ernesto Aroche, was not surprised that Pueblas government had been using the Remote Control System. In Moreno Valles six years as governor there, he has spent lavishly on new surveillance systems, including multiple security arches, structures that scrutinize traffic with video cameras and and whose cost had raised some questions in the local press. Beginning in 2013, Aroche began noticing solicitations on the website for hidden cameras and other spying equipment. When he filed a request about them, the governments form response indicated that these orders had never been filled, but Aroche was skeptical, given the mounting evidence that Moreno Valles administration had begun using its security apparatus for political purposes. There were periodic of homes belonging to dissident politicians and journalists, with the burglars sometimes taking little besides their victims laptops. Politicians would answer calls from unknown numbers, only to hear their own taped conversations played back to them. Another journalist, Fernando Maldonado, received an unmarked envelope full of what were purportedly transcripts of 400 private phone calls made by Puebla politicians. As Aroche and R3D sifted through the Hacked Team file dump, they discovered that the files on Puebla had more detail than those dealing with Hacking Teams other Mexican accounts. The Puebla client often wrote emails asking for help with infecting a particular document with a malicious virus. Some of these came from an account ” soporteuiamx@gmail. com ” that also appears in many of Hacking Teams internal support tickets. One of those tickets documents a clients request for help in infecting an attachment: an invitation to attend an event for a Mexican political organization, signed by Violeta Lagunes and addressed to another party colleague opposed to the governor. Aroche interviewed politicians and journalists who were on the receiving end of the infected emails contained in the Hacked Team trove. According to a 2015 article that Lado B published in conjunction with a politics website, the Puebla group sent Hacking Team at least 47 requests to infect specific files that it would then forward on to their targets. Almost all of those fil

**Mattathias Schwartz**

**2017**