Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260
Herausgegeben von Stefan Schumacher
Erschienen im Magdeburger Institut für Sicherheitsforschung

This article appears in the special edition »In Depth Security – Proceedings of the DeepSec Conferences«.
Edited by Stefan Schumacher and René Pfeiffer

A Death in Athens

The Inherent Vulnerability of »Lawful Intercept«

James Bamford

I will discuss the »Athens Affair,« the subject of a recent investigation by me in The Intercept. In 2004, the NSA and CIA worked secretly with the Greek government to subvert Vodafone and other telecom companies in order to conduct widespread eavesdropping during the 2004 Athens Summer Olympics. The NSA agreed, however, to remove the spyware once the games were over. But rather than remove it, they instead secretly turned it on the top members of the Greek government and members of the Greek public, including journalists. When the covert operation was accidentally discovered, however, a Vodafone engineer involved was found dead, either by suicide or murder, and the death was officially connected to the bugging operation. I will show how the operation was pulled off, by recruiting an inside person, then subverting the company's »lawful intercept« program, and transferring the data back to NSA headquarters at Fort Meade. The episode demonstrates the enormous vulnerability of widespread »lawful intercept« programs, and government backdoors in general, and also how the NSA often uses a »bait and switch« in its operations – promising to help find terrorists, but really spying on the host government and local population instead.

This paper is a transcript of the talk held at DeepSec 2015

Citation: Bamford, J. (2016). A Death in Athens: The Inherent Vulnerability of »Lawful Intercept«. *Magdeburger Journal zur Sicherheitsforschung*, *12*, 725–741. Retrieved September 2, 2016, from http://www.sicherheitsforschung-magdeburg.de/publikationen/journal.html

SLIDE 1

Thanks very much, it's great being here. I love being in Vienna, it's a terrific place to do a talk.

I used to come here a lot when I was covering the cold war for ABC News. My job was chasing spies here in Vienna. And one of my most memorable times was being arrested by the Secret Police and then interrogated for two hours.

SLIDE 2

I was after this guy: Zoltan Szabo. He was one of the most wanted American spies. He was running a big spy ring here in Vienna, he was a former US Army officer and I wanted an interview with him. So it took me about a week to find him, he was hiding out, but I found him and I wanted to follow him around Vienna for about half a day, just to see where he went before I'd approach him for an interview. What I didn't know was that the Austrian secret police where also following him and they couldn't understand who I was - So, after about an hour or two, they pulled me over and pulled me out of my car and took me down. They thought I was an assassin from the communist countries, trying to assassinate Szabo, who had defected to the West here to Austria. So, anyway that was my last experience here in Vienna, so I'm happy to be here not under interrogation and to give my little talk.

SLIDE 3

One of the reasons that I'm giving this talk here today is I did a piece for the Intercept Magazine a few months ago, basically on this case in Athens, and I've always been fascinated by it for years. There was this event in Athens, where this huge bugging operation was discovered. It was an enormous scandal in Athens, it was basically like Watergate in Athens. It was discovered that somehow, someway, somebody was bugging the major acteurs of the government, the prime minister, his wife, the Mayor of Athens, most of the top officials in Greece. That was back in 2004 during the Olympics there. It became a big scandal, but nobody knew what to do with it, because nobody knew who did the bugging. I mean they did a number of investigations in Greece but they didn't come up with much evidence. Well, I interviewed Ed Snowden last summer, I spent three days with him in Moscow, hanging out with him when I did the cover story for Wired. So, in addition to interviewing him I also got access to Snowdens documents, and going through them I saw documents that dealt with the bugging of the Greek government and the bugging of the Greek telecom system, that never have been revealed before. So, I really started to look into it and I found a number of sources in Washington - that's sort of what I do, I specialize in Intelligence. So I had some top NSA, CIA officials I talked to and one of them told me that yes, it was an NSA bugging operation, not only that, it was a rogue operation: It was an operation that was done without the permission of the CIA Chief of Station in Athens.

Just recently I did a piece on the attack in Paris. It just came out a couple of days ago in Time.

One of the things that the Director of the CIA came out with this week was to basically blame Snowden for the fact that the US failed in it's attempt to discover this attempt before it happened. So I wrote a piece basically saying it had nothing to do with Snowden, it was just bad intelligence. The NSA has missed firstly every intelligent or every terrorist incident since the beginning, so it wasn't really any big surprise.

SLIDE 4

This is the person that was involved in the Athens affair: Costas Tsalikidis was a really interesting guy, he had his masters degree in Electrical Engineering, he got that in the UK, he was about to be married, he was happy, he was living a very good life in Athens - And then he was found hanged. He was hanging in his apartment, from the ceiling leading into the bathroom. What had happened was, the day before the CEO of Vodafone, the big wireless company in Greece, discovered malware, a huge piece of malware, and they had it removed. And the next day Costas was found dead. So, obviously this led to questions. How did this happen? What was Costas connection? And again, there was no answer because there were no leaks from the US, nothing came out, and again, this was one of the reasons I decided to look into this.

SLIDE 5

Here's one of the documents, and, what this article I did does - I've been writing about NSA forever - but this is one of the very few times where you can trace an NSA operation from the very beginning to the very end and show exactly how the whole thing worked. So the very first thing is, - you know, this should be a wake up call for the governments in Europe or actually anywhere around the world, South America and other places - is the NSA will come into a country and they'll say: »Look, you gonna have the World Cup, or you gonna have the Olympics, or you gonna have some big event: You need us, because we can tell you when there's gonna be a terrorist event, because we can search through all the communications, so have us come in, have us bug your whole telecom system and we can help you. You know, we're here to help you.«

So, that's what they did, they got the permission from the Greek government to come in and do the bugging and what this document here from the Snowden archive talks about is they've been doing this for years. The NSA has been going around to various Olympic venues saying »We're here to help.« and »Let us come in, bug all your phones and when the event's over we'll disappear and you'll never hear from us again.« So that's pretty much what NSAs pitch was to the Greek government.

SLIDE 6

So, that's the agreement. This was from one of my Intelligence sources: »The Greeks identified terrorist nets, so NSA put these devices in there and they told the Greeks, »Ok, when it's done we'll turn it off.«

So, my information is coming from both Snowden documents and also from Senior NSA Officials.

SLIDE 7

One of the key things, and this is something that's very rarely discussed, especially by NSA or the CIA, is, when they wanna do this kind of operation, you can do a fair amount remotely, but if you really want to get in there and get a lot of intercept done you really prefer to have an inside person. Somebody in the country, who works for the telecom system. In this case it's the CIA that actually goes in there and recruits a spy, that's their job. CIA is Human Intelligence, NSA is technical. So they had a CIA person that went in there and this is what my Intelligence source said. You can just read it on the Slide.

SLIDE 8

NSA collects the technical side but they need the human aspect so they really need the CIA to do that. So, the CIA comes up with a recruiter. This was the recruiter. He looks like Santa Claus, actually this was one of the few public shots of Basil. Basil was never known until I did the story. I found out who he was and I did a lot of investigation about who he was and where he came from and how he did his work and everything for my article. He was the chief recruiter in Athens for the CIA, recruiting local Greek citizens to spy for the US. He had one picture taken for Facebook and he put this phony beard on, I think it's glued on or whatever, to hide his face. His family was on either side, so I've managed to find that picture, and here's a picture I've got from the Greek government, it was his passport picture. Here's another picture of him from a visa, and this is a picture I found: His daughter got married in Greece and I managed to find the photos of the wedding. He was trying to hide from the photographer. You can see as soon as he saw the photographer he put his head down, he don't wanted any pictures taken. So, this is the CIA official that was involved in the case. Again, he wasn't really known until he was exposed in this story here. One of the things that made Basil really useful was his parents were born in Greece, his been back and forth to Greece a great deal, he spoke Greek fluently like a native, he knew everything about the culture.

SLIDE 9

This is Basil as a young kid, over when his father got re-married on one of the Greek islands, we got that from one of his relatives. So, and this was his business card, he was posing - that's his cover title - as a Secretary of Regional Affairs for the Embassy, in reality he was a CIA covered officer.

SLIDE 10

So Costas was the perfect inside person, if the CIA wanted to recruit somebody. He was a 39 year old telecom engineer, he was a network planer, manager, he'd risen up the ranks, he's been there, I think, a dozen years - So, if someone wants to recruit somebody - that's Costas, inside the Vodafone facility - he would be a perfect person to do.

SLIDE 11

That's his brother. I interviewed his brother and he said Costas was living a happy life, he was doing very well right up until the time they found his body hanging. Nobody could understand why he would commit suicide, there was no real reason, he was fine financially, about to get married, he had a nice living, but ironically he was found dead the day after the bugging was discovered.

SLIDE 12

So, once you recruit the inside person, the next thing is to develop the malware to take control of the system, to take control of the network basically, to take control of Vodafone, of all of the cell phones in Greece, that are using the Vodafone system, and that was the biggest system there.

NSA developed a procedure, known as Lawful Intercept. Well, let me backup. Lawful Intercept is a program that goes with most telecom systems. If you're Vodafone and you're buying a big system, the company you're buying it from, in this case it was Ericsson, will also supply you with a program known as Lawful Intercept. A program, that if the government wants to monitor somebody's phone, a suspects phone, legitimate monitoring of criminal activity or whatever, has the technical capability of doing that. It's called the Lawful Intercept System.

So it comes as a package. Vodafone got it from Ericsson, Costas actually was the person who signed for it. The problem was the Greek government didn't have any capability for doing eavesdropping. All they had was a very rudimentary alligator clip type of bugging system, they didn't have any very wide-spread system for eavesdropping, so they never needed the Lawful Intercept Program, so Vodafone never bought it, or they had it, but they never paid for the digital key to turn it on.

It costs tens of thousands of Euros to pay to Ericsson to actually turn it on, so they never turned it on. So that was the perfect opportunity for NSA. NSA developed malware. You see the document on this Slide here, the one that reads »Top Secret // (S//SI//REL) TO USA, FVEY. Exploiting Foreign Lawful Intercept (LI) Roundtable« - This was the NSAs program, and this is one of the top secret slides from Snowden. This was the NSAs basic internal round table about how to turn Lawful Intercept Programs to their use.The way the system worked was the NSA developed this malware that they put into the system that would not activate the – actually let me go to the next slide, i think it will reveal a little bit more -

SLIDE 13

There are two parts of the Lawful Intercept System. The first one is the Intercept Management System and that basically creates an audit trail. If you're the Greek government, you wanna come in, you wanna eavesdrop on James Bamford, cause you think he's a spy, then you turn that over to Vodafone and Vodafone will put my name and my phone number into that first program, the Intercept Management System, the IMS. That will keep a record of the Intercept.

The second part, the RIS, will actually initiate the taping, that's actually doing the tap. So the malware that NSA came up with bypassed the first part and secretly turned on the second part, without ever notifying Ericsson that they were turning on the system, without the key or whatever. If anyone looked at it it would seem that there is no activity, when in reality they are doing a great deal of eavesdropping. That was the way NSA has been using the system in countries around the world, countries who don't necessarily use the Lawful Intercept Program, or even do. The NSA would come in there and secretly turn that system to their own use.

SLIDE 14

And this again is from another slide from Snowden, it shows all the different places the NSA used this technique of Lawful Intercept.

SLIDE 15

That's one way into the system. The NSA uses a variety and Duncan (Campbell) did a really excellent job to lower my work for me by explaining how these others systems work.

So in addition to eavesdropping, using the system I just mentioned, subverting the Lawful Intercept, they have other ways.

FORNSAT, that is foreign satellite interception – these are all top secret slides from Snowden – the map on the right shows where all these FORNSAT locations are, those are big satellite dishes intercepting satellite communications.

Microwave (F6), that was the system that Duncan mentioned, the Special Collection Service, those little huts on the top of Embassies. What they do is they collect the Microwaves passing through the city. So they getting all the local communication. And because the embassy is usually along an embassy row or in an embassy area you're getting a lot of foreign embassy communications as well as federal or national government communications. So, F6 is the internal code for Special Collection Service.

Special Source Operations, SSO, is the section of the NSA that works with the telecom companies. In other words they would work with AT&T to secretly get AT&T to eavesdrop on US communications, in this case they probably worked with Vodafone to get access.

TAO, Tailored Access Operations - these are the ones who would actually do the malware, they are the ones who would have created it. So all these groups, according to the Snowden documents that I had, people from all these groups were sent to Athens to do this work.

SLIDE 16

So basically, now you've got the agreement of the government, you've got the inside person, you've got the malware, you've got the external intercept operations going, what now was needed was some way to get the information after it's been collected, after it's been intercepted basically, in Vodafone. Now as phone calls will come in from the targets, a duplicate will be made of those signals and the duplicate signal will be sent out to an NSA facility. So you need some way to get that signal out and normally, in a normal case they would go out to the law enforcement agency of Greece or whatever, if this was a legitimate wire tap. But since it wasn't a legitimate wire tap NSA had to find another way to do that. So they came up with a whole bunch of - basically they are called shadow phones, phones that are untraceable. They go round to a lot places to buy this phones that are untraceable and then the signals get transmitted to these phones.

And once they are transmitted to these phones, the phones then transmit them to another location, which is NSAs secret location, where they have the ability to store and analyze the communications. But if anybody did trace them, if anybody did follow the signals, they only would go to these untraceable cell phones and go no further. So this was a very good set up: You got the agreement of the government, you put them in there, look for terrorists during the Olympics, keep everybody happy, get an inside person there, you get the malware, then you exfiltrate the intercepted communications to these untraceable cell phones and they transmit it to the NSA.

SLIDE 17

So what happens now. The Olympics are all over. You know they have a closing ceremony, that was supposed to be the end of the operation, the NSA was supposed to take it all out, fly back to Fort Meade and say goodbye to the Greek government and the Greek telecom system. The problem was, according to my confidential source, they never removed it, all they did is they turned it off for a day and then they turned it back on again. But now instead of going after the terrorists, which was the whole raison d'être for the operation in the first place, now they secretly turning it on the Greek government, they turning it on the prime minister, his wife - I don't know why, but they did - , the Mayor of Athens - that will keep us safe by knowing what the Mayor of Athens is telling us. This is total overreach by the NSA, but this is what they do, this is one, just one little example, you can extend this around the world to other places. I mean it came out that in Germany they have been bugging Angela Merkel and so forth, and so, this is just standard operation procedure on a mission according to a senior NSA source. I asked »You know, is this unusual or what?« And he laughed and said »They never remove it. Are you kidding? Once you got it in there you leave it in there.« So that's just standard operation procedure for NSA.

SLIDE 18

Then, everything is going fine, the Olympics are over, the NSA doing their illegal eavesdropping and then something happened. Somebody made a reboot or some change in the Vodafone system or updated the System, a routine update or whatever, but because of that it screwed up the NSA system. And as a result of that it stopped a number of text messages from going out, so Vodafone began getting complaints from

customers, that weren't getting text messages. That set of something like an burglar alarm at Vodafone, you know, all of a sudden the system isn' working, so they sent all their data to Ericsson for a technical analysis. On March 8th Ericsson sent back the Vodafone report saying »Sorry Folks, but you got a huge bug in your system there. 6500 lines of a piece of code of malware. So you got a huge problem, you got a very big bug in your system for some reason.« Then the CEO of Vodafone made a bad mistake, if he did it on purpose or not nobody can know at this point, but he immediately got rid of that malware. The problem with doing that is - I mean, the good thing is you get the malware out, the bad thing is there's no way to do a forensic analysis now. You can't figure out where it came from, you can't trace it back very well, it's like destroying the evidence. Anyway, the next day Costas was found dead. Costas brother was going to Costas apartment and he walked in and saw his brother hanging from the ceiling. A horrible, horrible event.

SLIDE 19

So then there were a few pieces of technical details that the Greeks could trace back. And they were able to trace the signals, some of the signals being sent to some of the phones, the supposedly untraceable cell phones. And what they did was, they saw the signals all went in the direction of the US Embassy. So you know, there's a fairly big clue there. But there was no smoking gun. Again, they didn't have the Snowden documents that I had, they didn't have the sources I had, that told me these things, all they had were diagrams that told them were the signals were going.

SLIDE 20

So, after a decade of on-again and off-again investigations - the Greeks, to give them credit, they were really trying to find this out, but you know, how do you find these invisible signals? It's really, really difficult. One of the things, they were able to find though, was that some of the cell phones were bought from a particular cell phone store. They were able to trace them back and find out who purchased them. The owner of the cell phone store actually recognized, when the Greek investigators showed him pictures, Basils wife as the person who purchased those shadow phones. Well, there's a big clue right there. That's how Basil came into the picture in terms of the Greek investigation. In addition to that they were very sloppy. The CIA, it's not what you see on television, it's a very sloppy organization most of the time. They used some of these untraceable cell phones to make calls to Maryland were NSA is, to the Embassy and all that. So they were able to see that these shadow phones, bought by the CIA officers wife, were actually being used not only to collect the intercepted signals but then to make phone calls to the Embassy and even to Maryland, even to the place were Basil used to live, near NSA. So this was very sloppy and as a result there's now an arrest warrant out for Santa Claus. He hasn't come back to Greece since and that's really sad for him actually, because he has a house on a little island in Greece, his wife's actually living in Athens. His wife is ethnically Greek also, and he, according to documents I found, planned to retire in Athens. Well, that's out of the window right now, unless he wants to spend his retirement in a Greek jail. So the Greeks are after him, he hasn't surfaced, I found him, his location is in the US of all places, and sent e-mails and phone calls to him and all of his relatives, his wife, his son, his daughter and everybody, but he never got back to me, big surprise. So he's disappeared to some place in the US and if he ever goes back to Greece there will be an arrest, there will be a trial, and the trial will be very interesting, because all of this will come out, which is exactly is why he will never go back to Greece and why the US won't send him back.

SLIDE 21

Anyway Costas family is still hoping for answers. Hopefully, maybe there will be some answers send from the US government, but I really doubt it. And one of the things they did in 2011, they asked some coroners to re-examine some of the documents that the original medical examiners produced. Among the people they asked was a pathologist from the United States, from San Francisco, somebody, who has a lot of medical experience in terms of looking into causes of death and so forth. He went to Athens, looked into it all and he thought the whole original examination was very, very sloppy. He didn't actually think that there was a suicide, he thought, you know, it might be murder. So, I'm not big on conspiracy theories, but there it is, there's a medical examiner from San Francisco, who did say, that, from looking at the photos and the autopsy report, he didn't think it was suicide, he thought it could be murder or some external cause.

So what are the possibilities? There are a couple of possibilities here. One is Costas was the inside person and he thinks he's doing something very patriotic. He's bugging the system to find terrorists. Because somebody either from Greek Intelligence or Basil posing at what they call a false flag, pretending he's from the Greek Intelligence said to him »We're trying to catch terrorists, so you're doing something very patriotic here.« And then all of a sudden he discovers they're not looking for terrorists, they're bugging the top people of the government. It' d be like me or somebody from the US working for AT&T, just trying to do something honorable, suddenly discovering they're bugging President Obama, his wife and everybody else from the top members of government.

Can you imagine the scandal? I mean facing your family, the public, everybody after it is discovered that you're the guy who put the malware in there that caused that?

I mean that would be a good excuse for a suicide.

On the other hand he may not have been the inside person, there are other people who could have been the inside person, and Costas could have been the person, who discovered the malware and wanted to report it to the press or the public or expose it somehow, and someone didn't want him to expose it and ex-

plain that Vodafone was bugging all this senior member of government. I mean that would have been a good reason to bump him off. So, these are questions that haven't been answered, but at least we're moved down the road quite a bit to show how it happened, who's responsible, why it happened and so forth.

SLIDE 22

Anyway that was my talk, and we have ten minutes left, so if anybody has some questions left I'm happy to take them.

1 About the Speaker

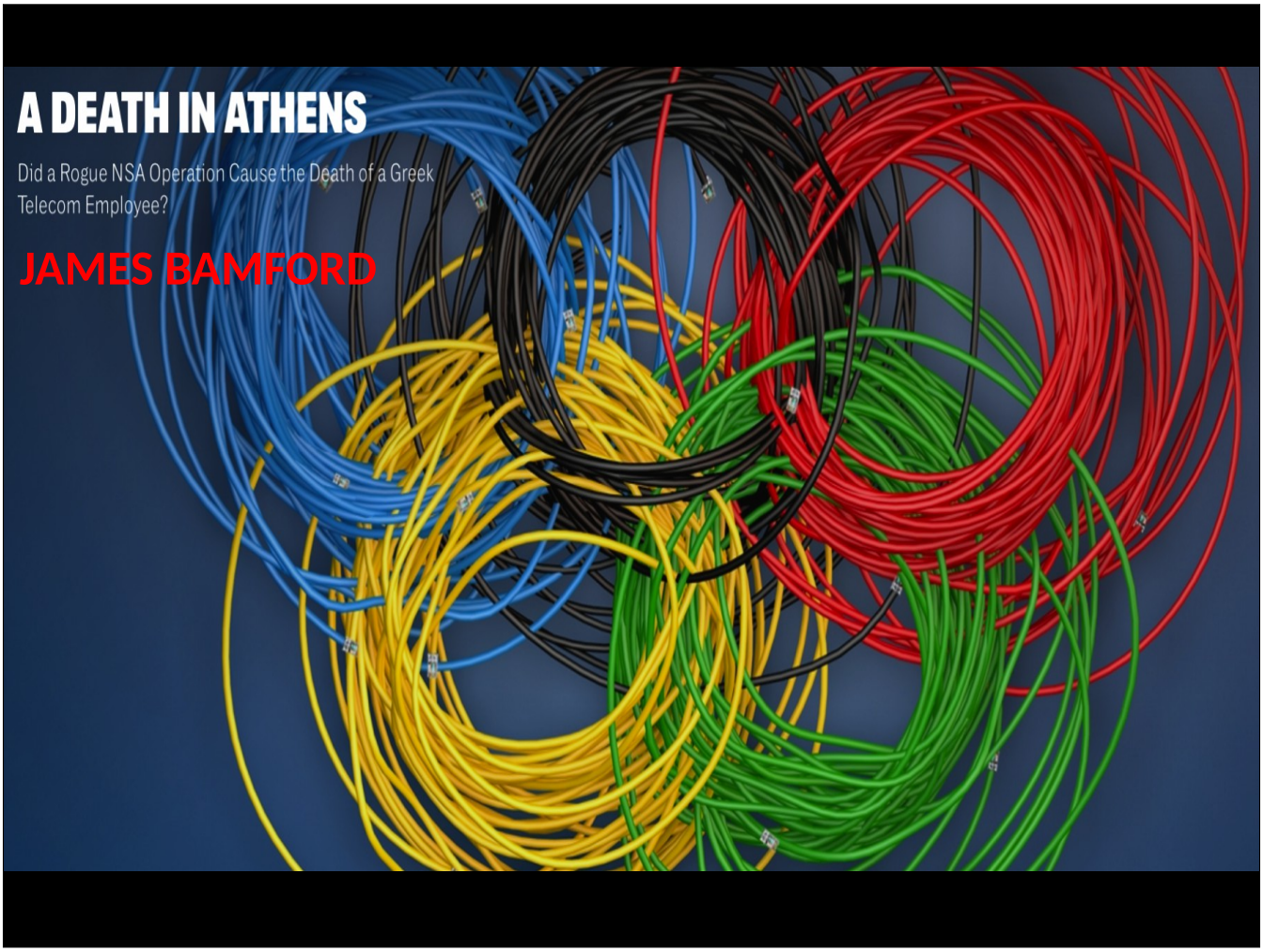
James Bamford is a columnist for Foreign Policy Magazine, a contributor to Wired magazine, a documentary producer for PBS, and a bestselling author. He is widely noted for his writing about the United States intelligence agencies, especially the highly secretive National Security Agency. The New York Times has called him "the nation's premier journalist on the subject of the National Security Agency." And in a lengthy profile, The New Yorker referred to him as "the NSA's chief chronicler." His most recent book, The Shadow Factory: The Ultra-Secret NSA From 9/11 to The Eavesdropping on America, became a New York Times bestseller and was named by The Washington Post as one of "The Best Books of the Year." It is the third in a trilogy by Mr. Bamford on the NSA, following The Puzzle Palace (1982) and Body of Secrets (2001), also New York Times bestsellers.

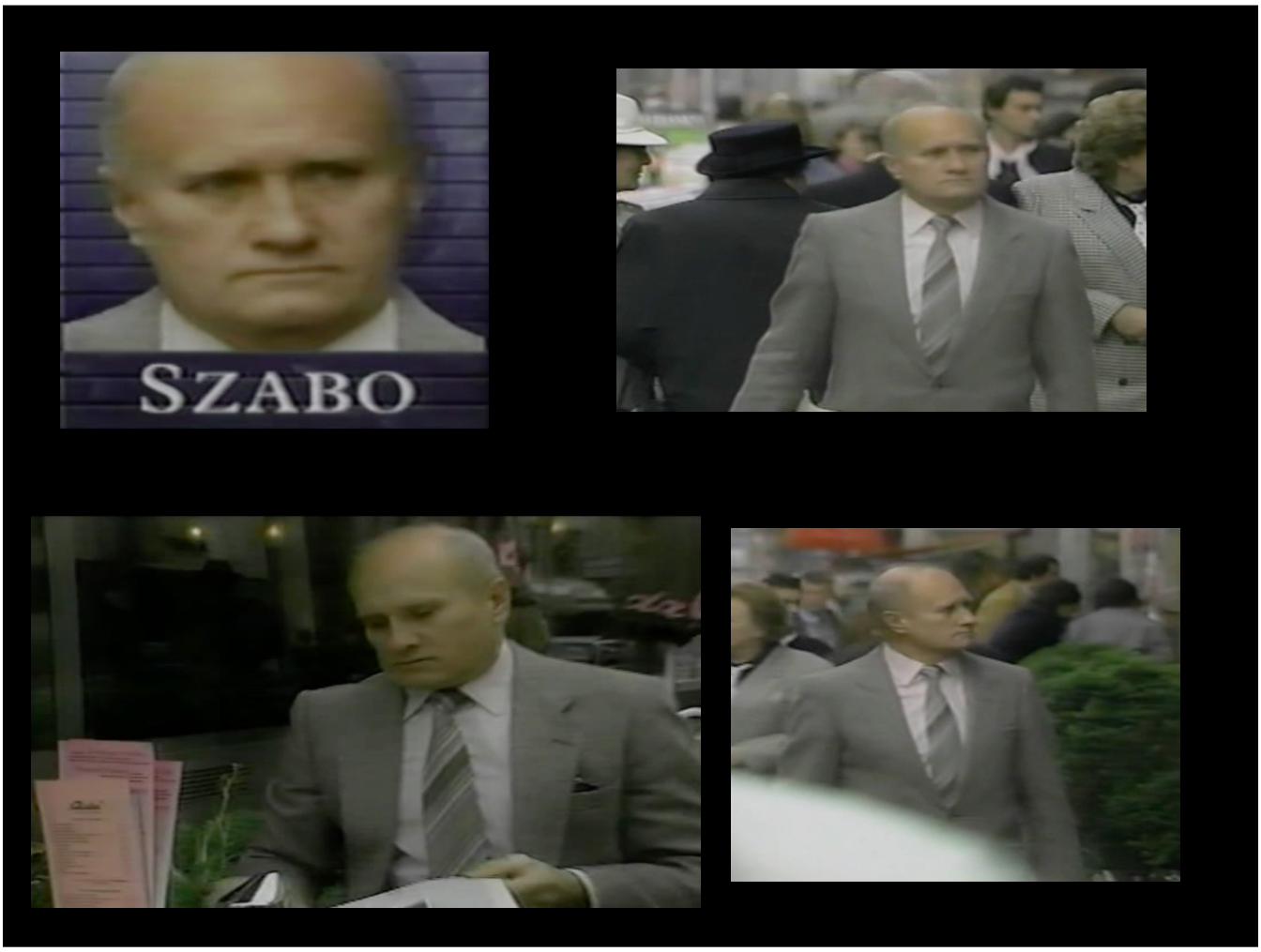
In September 2014 he wrote a cover story for Wired magazine based on his three days in Moscow with fugitive NSA whistleblower Edward Snowden, the longest any journalist has spent with him there. In addition, he has written for the New York Review of Books, New York Times Magazine, The Atlantic, Harpers, Rolling Stone, and many other publications. In 2006, he won the National Magazine Award for Reporting, the highest honor in the magazine industry, for his writing in Rolling Stone on the war in Iraq. He also writes and produces documentaries for PBS, including The Spy Factory, based of his most recent book, which was nominated for an Academy Award in 2010. His most recent documentary for PBS, Cyber War Threat, aired on October 14, 2015.

Throughout the 1990s, Mr. Bamford served as the Washington Investigative Producer for ABC's World News Tonight with Peter Jennings where he won a number of journalism awards for his coverage of national security issues. In 2005, he released A Pretext for War: 9/11, Iraq and The Abuse of America's Intelligence Agencies, an examination of the intelligence community from the attacks of September 11 to the war in Iraq and was also a bestseller.

Mr. Bamford holds a Juris Doctor degree; was awarded a Polymer fellowship at Yale Law School; received a postgraduate diploma in International Law from the Institute on International and Comparative Law, Université Panthéon Sorbonne; and taught at the University of California, Berkeley's Goldman School of Public Policy as a distinguished visiting professor. He has been a member of the defense team in a variety of high profile espionage and whistleblower cases, including the case involved NSA whistleblower Thomas Drake. He currently lives in Washington, DC after four years in London.

Email: WashWriter@gmail.com, Facebook: james.bamford2@facebook.com, Twitter: @WashAuthor


A DEATH IN ATHENS
Did a Rogue NSA Operation Cause the Death of a Greek Telecom Employee?
JAMES BAMFORD


SZABO

ON MARCH 8, 2005, THE CEO OF VODAFONE GREECE ORDERED THAT A NEWLY DISCOVERED PIECE OF MALWARE, A LARGE AND SOPHISTICATED BUG, PLANTED BY PERSONS UNKNOWN, BE REMOVED

THE NEXT DAY ONE OF THE COMPANY'S SENIOR MANAGERS, COSTAS TSALIKIDIS, WAS FOUND HANGED IN HIS ATHENS APARTMENT. THERE WAS NO SUICIDE NOTE







COSTAS IN HAPPIER TIMES

A DECADE LATER, WITH THE HELP OF PREVIOUSLY UNPUBLISHED SNOWDEN DOCUMENTS AND INTERVIEWS WITH FORMER SENIOR INTELLIGENCE OFFICIALS, I WAS ABLE TO SHOW HOW THE NSA AND CIA WERE RESPONSIBLE FOR THE MYSTERIOUS BUGGING OPERATION THAT LED TO COSTAS' DEATH AND WHAT BECAME KNOWN AS "THE ATHENS AFFAIR"



WORKING WITH GREEK JOURNALIST AGGELOS PETROPOULOS, THE ARTICLE APPEARED IN THE INTERCEPT LAST MONTH AND RESULTED IN HEADLINES IN GREECE

ACCORDING TO PREVIOUSLY UNRELEASED SNOWDEN DOCUMENTS, THE NSA HAS HAD A LONG HISTORY OF SPYING DURING OLYMPIC GAMES, BEGINNING MORE THAN 30 YEARS AGO



DYNAMIC PAGE -- HIGHEST POSSIBLE CLASSIFICATION IS
TOP SECRET // SI / TK // REL TO USA AUS CAN GBR NZL

(U//FOUO) SID Trains for Athens Olympics

FROM: [redacted] USAF
SIGINT Communications
Run Date: 08/15/2003

(U//FOUO) In just over a year the torch will be lit, and thus will kick off the 2004 Summer Olympic Games in Athens, Greece, home to the first Olympic Games. Although the first race, dive, and somersault are still a year away, the Intelligence Community is already in full "training mode" for the event. In truth, NSA has been gearing up for the 2004 Olympics for quite some time, in anticipation of playing a larger role than ever before at the international games.

(U) Prior Games

(S) The first phase of preparation actually began years ago through the involvement of NSA with the Olympic Games in other cities. NSA has had an active role in the Olympics since the 1984 Los Angeles games, and has seen its involvement increase with the recent games in Atlanta, Sydney, and Salt Lake City. During the 2002 Winter Olympics in Salt Lake City, the focus was on counterterrorism, and NSA acted largely in support of the FBI in a fusion cell known as the Olympics Intelligence Center (OIC). The mission of the OIC was to fuse foreign intelligence and law enforcement information to provide threat warning and situation awareness before and during the games. NSA's support to the 2004 Olympics in Athens will be much more complicated.

(U) The Athens Outlook

(S//SI) Several factors will make the Athens Olympics vastly different, not the least of which is the fact these Olympics will not be held at a domestic location. Also different is that the security organization that NSA will support is the EYP, or Greek National Intelligence Service. NSA will gather information and tip off the EYP of possible terrorist or criminal actions. Without a doubt, the communication between NSA and EYP will take some coordination, and for that reason preparations are



THE SECRET AGREEMENT

INTELLIGENCE SOURCE: "THE GREEKS IDENTIFIED TERRORIST NETS, SO NSA PUT THESE DEVICES IN THERE AND THEY TOLD THE GREEKS, 'OK, WHEN IT'S DONE WE'LL TURN IT OFF.'"

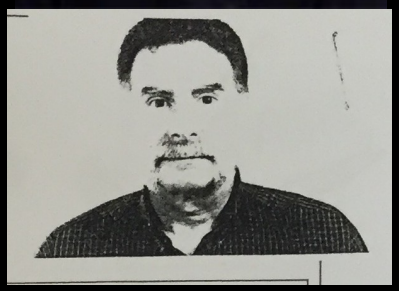
RECRUITING AN INSIDE PERSON

- **INTELLIGENCE SOURCE:** "WHAT THE NSA REALLY DOESN'T LIKE TO ADMIT, ABOUT 70 PERCENT OF NSA'S EXPLOITATION IS HUMAN ENABLED. FOR EXAMPLE, AT A FOREIGN MINISTRY OF POST AND TELECOMMUNICATIONS, IF NSA DETERMINES IT NEEDS TO GET ACCESS TO THAT SYSTEM, NSA AND/OR THE CIA IN COORDINATION WOULD COME UP WITH A MECHANISM THAT WOULD ALLOW THEM TO REPLICATE THE EXISTING SWITCH TO BE SWAPPED OUT. THE CIA WOULD THEN GO AND SEEK OUT THE PERSON WHO HAD ACCESS TO THAT SWITCH — LIKE A NORTEL SWITCH OR A ROUTER — GO IN THERE, AND THEN IT WOULD BE THE CIA THAT WOULD EFFECT THE OPERATION. AND THEN THE TAKE FROM IT WOULD BE EXPLOITED BY THE NSA."

- **SNOWDEN DOCUMENT:** A HIGHLY SECRET PROGRAM CODENAMED "SENTRY OWL" DEALS WITH "FOREIGN COMMERCIAL PLATFORMS" AND "HUMAN ASSETS COOPERATING WITH NSA."

- **INTERVIEW WITH GEN. MICHAEL HAYDEN:** "HUMAN INTELLIGENCE GUYS CAN PROVIDE SOMETIMES THE NEEDED PHYSICAL ACCESS WITHOUT WHICH YOU JUSTCAN'T DO THE SIGNALS INTELLIGENCE ACTIVITY.





THE CIA RECRUITER

- THE MANY FACES OF WILLIAM GEORGE BASIL, A CIA CASE OFFICER AT THE U.S. EMBASSY, ATHENS

- **CIA SOURCE IN ATHENS:** "HE WAS THE BEST RECRUITER THE STATION HAD, THE BEST."





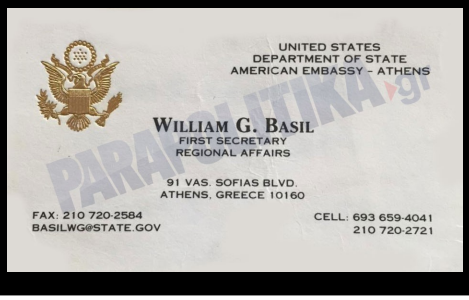
- ONE OF THE THINGS THAT MADE HIM THE EMBASSY'S BEST RECRUITER WAS HIS ETHNIC HERITAGE

- HIS PARENTS WERE GREEK AND HE GREW UP PARTLY IN GREECE AND PARTLY IN THE BALTIMORE AREA

- HE SPENT ABOUT TWENTY YEARS AS A CIA POLYGRAPH OPERATIOR AND THEN JOINED THE DIRECTORATE OF OPERATIONS AS A CLANDESTINE OFFICER

- HIS COVER TITLE: FIRST SECRETARY, REGIONAL AFFAIRS SECTION





THE POSSIBLE INSIDE PERSON

COSTAS TSALIKIDIS







- A 39 YEAR OLD TELECOM ENGINEER, COSTAS WAS A NETWORK PLANNING MANAGER FOR VODAFONE GREECE, THE COUNTRY'S LARGEST MOBILE PHONE COMPANY,WHERE HE HAD WORKED FOR THE LAST ELEVEN YEARS.

- HE EARNED A DEGREE IN ELECTRICAL ENGINEERING FROM THE NATIONAL TECHNICAL UNIVERSITY OF ATHENS AND A MASTERS IN COMPUTER SCIENCE IN ENGLAND.

- LIKE MOST EVERYONE ELSE, HE WORKED EXTRA-LONG HOURS DURING THE OLYMPICS

- ACCORDING TO HIS BROTHER, PANAGIOTIS, UP UNTIL THE LAST FEW MONTHS OF HIS LIFE, COSTAS WAS VERY HAPPY AND ABOUT TO GET MARRIED.
- PANAGIOTIS: "HE HAD MET THE WOMAN OF HIS LIFE AND THEY WERE PLANNING TO GET MARRIED REALLY SOON. AND FOR THAT REASON, THEY WERE LOOKING TO GET A HOUSE AND THEY HAD ALREADY STARTED BUYING THINGS THAT THEY COULD USE IN THEIR NEW HOUSEHOLD. COSTAS WAS HAPPY AND OPTIMISTIC AND THINGS HAD BEEN WORKING OUT REALLY GOOD FOR HIM."



PANAGIOTIS TSALIKIDIS

THE MALWARE



- THE KEY TO OPERATION WAS HIJACKING A PARTICULAR PIECE OF SOFTWARE, ERICSSON'S "LAWFUL INTERCEPT" PROGRAM. IT WAS A COMMON TECHNIQUE FOR NSA


TOP SECRET//SI//REL TO USA, FVEY

(S//SI//REL) Exploiting Foreign Lawful Intercept (LI) Roundtable

[redacted] S31122

TOP SECRET//SI//REL TO USA, FVEY

- INSTALLED IN MOST MODERN TELECOM SYSTEMS
- GIVES A TELECOM COMPANY THE TECHNICAL CAPABILITY TO RESPOND TO A LEGAL WARRANT FROM THE LOCAL GOVERNMENT TO MONITOR A SUSPECT'S COMMUNICATIONS



ERICSSON'S AEX MOBILE PHONE SWITCH



THE LAWFUL INTERCEPT PROGRAM CONSISTS OF TWO PARTS:

1. THE INTERCEPT MANAGEMENT SYSTEM (IMS) CREATES AN AUDIT OF THE INTERCEPT

2. THE REMOTE CONTROL EQUIP SUBSYSTEM (RES) INITIATES THE INTERCEPT

- **VODAFONE HAD BOTH SYSTEMS, BUT BECAUSE EVEN OFFICIAL WIRETAPPING WAS ILLEGAL IN GREECE, VODAFONE NEVER PURCHASED THE KEY FROM ERICSSON TO TURN ON THE IMS AUDIT PROGRAM**



- **NSA KNEW THIS AND, WITH THE HELP OF THEIR INSIDE PERSON, INSTALLED MALWARE TO SECRETLY ACTIVATE THE "RES" SYSTEM AND INSTALL THE NUMBERS TO BE TAPPED. BUT BECAUSE THE "IMS" SYSTEM WAS NEVER ACTIVATED, THERE WOULD BE NO RECORD OR INDICATION OF THE TAPPING**

- **COSTAS ACCEPTED AN UPGRADE TO THE SYSTEM**

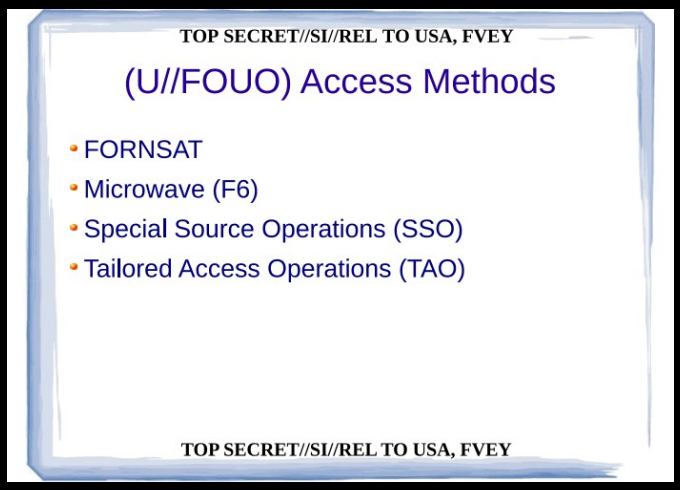
BESIDES GREECE, THE NSA HAS SUBVERTED THE LAWFUL INTERCEPT PROGRAM IN MANY COUNTRIES, AS THIS SLIDE FROM SNOWDEN SHOWS



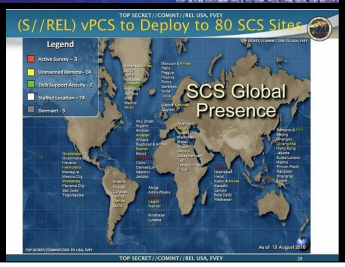
- ALSO ACCORDING TO THE SNOWDEN DOCUMENTS, GAINING ACCESS TO THE GREEK TELECOM SYSTEMS INVOLVED SENDING TO ATHENS PERSONNEL FROM THE KEY OFFICIES INVOLVED IN LAWFUL INTERCEPT TAPPING
- THESE INCLUDED THE SPECIAL COLLECTION SERVICE (F6), SPECIAL SOURCE OPERATIONS (SSO), AND TAILORED ACCESS OPERATIONS (TAO)
- SNOWDEN DOCUMENT: MEMBERS OF THE TAO "PERFORMED CNE [COMPUTER NETWORK EXPLOITATION] OPERATIONS AGAINST GREEK COMMUNICATIONS PROVIDERS" AS PART OF THE PREPARATIONS FOR THE OLYMPICS











THE "SHADOW" PHONES

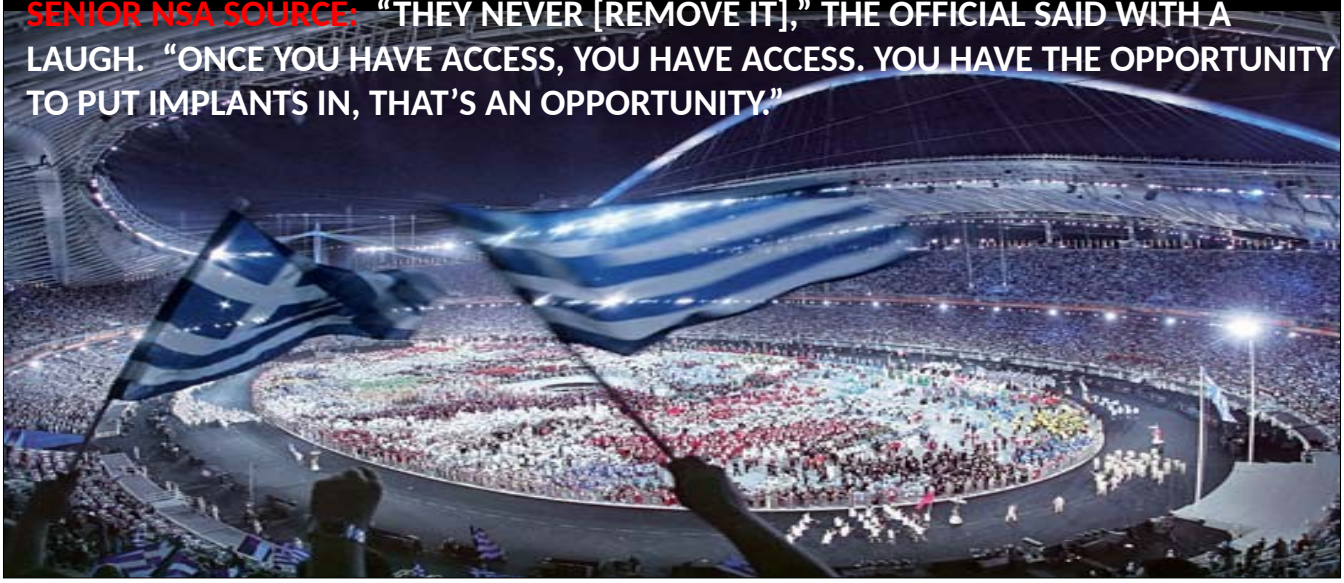
- ALL THAT WAS LEFT WAS TO DEVELOP A SYSTEM TO SECRETLY TRANSMIT THE WIRETAPPED CALLS FROM VODAFONE TO NSA
- THIS INVOLVED PURCHASING A DOZEN UNTRACEABLE "SHADOW" CELL PHONES
- THEN PROGRAMING THE "RES" SYSTEM TO TRANSMIT DUPLICATES OF THE TARGET CALLS TO THE SHADOW PHONES
- THE SHADOW PHONES WOULD IN TURN BE PROGRAMED TO RETRANSMIT THE CALLS TO LOCAL NSA COMPUTERS WHERE THEY COULD BE ANALYZED AND THEN SENT ON TO NSA HEADQUARTERS FOR FURTHER ANALYSIS AND STORAGE



AUGUST 29, 2004: THE CLOSING CEREMONY OF THE 2004 OLYMPICS

SENIOR INTELLIGENCE SOURCE: "WE HAD A HUGE PROBLEM RIGHT AFTER THE GREEK OLYMPICS. THEY [NSA] SAID WHEN THE OLYMPICS IS OVER, WE'LL TURN IT OFF AND TAKE IT AWAY. AND AFTER THE OLYMPICS THEY TURNED IT OFF BUT THEY DIDN'T TAKE IT AWAY AND THEY TURNED IT BACK ON AND THE GREEKS DISCOVERED IT. THEY TRIANGULATED SOME SIGNALS, ANONYMOUS SIGNALS, AND IT ALL POINTED BACK TO THE EMBASSY."

SENIOR NSA SOURCE: "THEY NEVER [REMOVE IT]," THE OFFICIAL SAID WITH A LAUGH. "ONCE YOU HAVE ACCESS, YOU HAVE ACCESS. YOU HAVE THE OPPORTUNITY TO PUT IMPLANTS IN, THAT'S AN OPPORTUNITY."



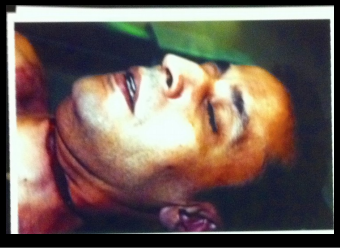
THE GLITCH

- AT 7:56 P.M. ON JANUARY 24, 2005, SOMEONE INSTALLED A ROUTINE UPDATE IN THE NSA'S BUGGING SOFTWARE AT VODAFONE'S FACILITY IN THE PAIANIA SECTION OF ATHENS. IT WOULD TURN OUT TO BE ANYTHING BUT ROUTINE.

- WITHIN SECONDS, ERRORS APPEARED, WHICH CAUSED HUNDREDS OF TEXT MESSAGES FROM CUSTOMERS TO GO UNDELIVERED, AND PEOPLE BEGAN COMPLAINING.

- ON MARCH 8, FOLLOWING A TECHNICAL ANALYSIS BY ERICSSON THAT UNCOVERED A HEAFTY 6,500 LINES OF MALWARE – EVIDENCE OF A LARGE BUGGING OPERATION – THE CEO OF VODAFONE ORDERED IT REMOVED.

- THE NEXT MORNING, COSTAS, ENGAGED TO BE MARRIED, WAS FOUND HANGED IN HIS APARTMENT BY HIS BROTHER PANAGIOTIS.



GREEK INVESTIGATORS TRACED THE SIGNALS BACK TO THE U.S. EMBASSY



- AFTER A DECADE OF ON AGAIN OFF AGAIN INVESTIGATION, THE GREEK INVESTIGATORS FINALLY POINT A FINGER DIRECTLY AT WILLIAM GEORGE BASIL, THE FORMER CIA CLANDESTINE OFFICER AT THE ATHENS EMBASSY.

- AS A RESULT OF SLOPPY CIA TRADECRAFT, INVESTIGATORS TRACED THE PURCHASE OF SEVERAL OF THE SHADOW PHONES TO BASEL'S WIFE. AND CALLS FROM THOSE PHONES WERE TRACED BACK TO THE EMBASSY AND ALSO TO MARYLAND, NEAR NSA.

- EARLIER THIS YEAR, IN A VERY RARE MOVE FOR AN ALLY, THE GREEK GOVERNMENT RECENTLY ISSUED AN INTERNATIONAL ARREST WARRANT FOR BASIL BUT HE IS NOW BACK IN THE U.S.





- AND COSTAS' FAMILY IS STILL HOPING FOR ANSWERS FROM THE U.S. ABOUT WHAT HAPPENED TO HIM, BUT THE U.S. HAS THUS FAR STONEWALLED ALL INVESTIGATIONS.
- IN 2011, THE FAMILY ASKED TWO CORONERS TO REEXAMINE THE MEDICAL RECORDS, INCLUDING DR. STEVEN KARCH, A FORENSIC PATHOLOGIST AND FORMER MEDICAL EXAMINER IN SAN FRANCISCO. KARCH CALLED THE ORIGINAL AUTOPSY "FARCICAL" AND THE TWO CORONERS CONCLUDED THAT THE MARKS TO COSTAS' NECK COULDN'T HAVE COME FROM SIMPLY JUMPING OFF THE CHAIR. "SOMETHING WAS DONE TO HIM PRIOR," KARCH SAID.
- I QUESTIONED GEN. MICHAEL HAYDEN, WHO WAS DIRECTOR OF NSA AT THE TIME. HIS RESPONSE: "NOT ANYTHING WE'RE GOING TO TALK ABOUT HERE," HE SAID. "NOT SOMETHING I CAN TALK ABOUT."





Many Thanks

Please feel free to contact me

@WashAuthor

WashWriter@gmail.com

