History of espionage Part 2

Midnight Facts for Insomniacs

Podcast Transcript

(Note: transcript consists of episode outline)

At its most basic, espionage involves the covert acquisition of information. If you’re trying to keep your own secrets while stealing someone else’s, you’re engaged in some level of espionage. And you have a variety of techniques at your disposal. Those can be as simple as whispering, or passing notes. Every third grade classroom is a hotbed of espionage. Most of us probably practiced pig Latin, or developed secret languages or code words with friends. Even inside-jokes are a kind of covert language. As we mentioned in the previous episode, the instinct to keep secrets is encoded in our genes, we're all a bunch of sneaky sneakersons, but very few humans are genuinely skilled at subterfuge. Most of us lie, and most of us get caught. If you want evidence of how bad we are at keeping secrets, tell your friend a secret, like that you had sex with his wife, and I guarantee everyone is going to know about it in a couple days. It seems like discretion is dead.

From the early days of human history we’ve relied on technology, however primitive, to help us keep and/or transmit our secrets.

So this episode is all about the evolving technology of espionage.

The most primitive method for protecting information is to make that information physically difficult to obtain. So, hide it. Conceal the information in an unexpected location. Hollow out a tooth, cut a hole in the pages of a book, pour out the soda from a Pepsi can…empty items, very popular in the spy game. Spies are enemies of solidity. A famous spy saying: “When in doubt, hollow it out.” That’s not true but it should be. Spies, you’re welcome. you can keep that. Steganography is the science of concealing the existence of a message, usually in plain sight. For instance, in Ancient Greece one method was to shave a slave’s head, tattoo a message in his/her scalp, and let the hair grow back. This is great if your message is not super urgent. This is the long game.

“Your house is on fire:” not a great scalp message. More like your house WAS on fire, my bad, I ‘m not good at making toast, it was a whole toast debacle, I’m very far away by now. Don’t bother looking for me. You can keep the slave, I realize it’s not as valuable as a house, because this is a terrible time in history, I mean we’re tattooing peoples heads which is still a thing that happens, but only voluntarily by people are angry at their parents. It reminds me of Johnny mnemonic, where a corporation imprints information into a guy’s brain and only a certain phrase can unlock it. The hair thing is the most primitive version of imprinting information in the brain area. Ok now that I think about it it’s nothing like that at all.

So concealment devices were some of the earliest forms of spying technology. And if you want to share secret information with only one specific person, concealment devices can be great for that. you reveal the location to your compatriot, and he or she retrieves the information, and now you’ve created what is known in the spy industry as a “dead drop.” Kind of a grim name for a place to hide stuff. “I put the documents in a carnage box. A murder hole. Yeah, its a soda can.” A murder hole, I guess that’s just a grave. But the name sort of makes sense, because it contrasts with an alternate method for transferring information, a live drop, which is when two agents exchange the info in person. This is risky, because the spies are in the same place at the same time and thus can be “made” or identified by their actions, or by their association with each other. If one of you was already a suspected spy, and you were being tailed, now you’re both suspects. but a dead drop is also risky, in different ways. Once you’ve placed the item or info in a dead drop,

it’s no longer under your control...if anyone tries to drink that pepsi they’re going to get a mouthful of secrets. So there are benefits and drawbacks to each. A live drop is risky because If one of you was followed, now you’re both caught; on the other hand, if one spy is followed to a dead drop, the information is compromised but the other spy remains Anonymous. In a live drop you control the information throughout the process.
A common hiding place for secrets in World War One was ammunition. Take a bullet, pour out the propellant, replace it with a little tightly wrapped piece of paper. This is Another staple of the spy game: tiny paper, with tiny writing. Also tiny electronics. Spying...not for size queens. If you’re a

male spy, you have to be super secure in your masculinity. Or maybe the opposite. Maybe male spies enjoy carrying around tiny phones and tiny paper and tiny cameras because of the contrast. A tiny camera makes your junk seem massive. At least, next to the camera. Taking pictures of your junk with a tiny camera doesn't make your junk look any bigger in the pictures. Pro tip.

A secret compartment in a vehicle btw is called a "trap." And some modern traps are extremely complex. "one trap found in the airbag compartment of a U.S. car in 2012 would only open if a driver was in the seat, all doors were closed...the defroster was turned on and a magnetic card was swiped over a sensor hidden in an airconditioning vent” interesting post script… that particular spy’s airbag-concealment method was eventually foiled by his own stupidity. His airbag had been manufactured by takata, and he had ignored repeated recall notices. The airbag exploded, blasting state secrets and his brains all over the upholstery. He wasn’t using those brains anyway. So the airbag was real, and that is an extremely complicated method of concealment, but we’ve been concealing messages for years in clever if much more simple ways. One of my favorite is the “mask letter.“ this is a letter that is carefully crafted so that certain words are deliberately placed in specific areas, and when the recipient receives the letter, he or she places a carved design made of wood or paper over the letter, which blocks out all of the irrelevant words and only reveals the words that fall in the carved portions of the pattern, which together create a message. I like this because it takes a ton of planning and creativity. You have to be a real wordsmith to somehow fit "kill the king" in a letter without sounding any alarms. You're like, "I've been walking all day, my feet are really killing me. This is the absolute king of foot pain. I'm Experiencing stabbing sensations all the way up to my heart."

Another popular early form of steganography is invisible ink, otherwise known as the sympathetic stain. George Washington called it that. I don’t know why, maybe during the American revolution both sympathetic and stain meant things other than what they mean today. Maybe sympathy meant like useful, and stain meant “not at all a stain.” it is in fact the exact opposite of a stain. A stain appears when you don’t want it to, and is very visible, whereas invisible ink won’t show up until you summon it. Maybe that’s why it’s a sympathetic stain, it’s like “oh, you need to see me now? I understand. Here I am.” Invisible ink dates as far back as the fourth century BCE. I didn’t know this, but there are tons of substances you can use as invisible ink…for instance, if you write with lemon juice it’s completely transparent when diluted with a small amount of water, but turns brown when heated by a candle or even a lightbulb. George Washington’s Culper ring, made famous by starring in our last episode, and probably also for being instrumental in defeating the British, but mostly from being mentioned on this podcast, used a special formulation of oak gall ink, with various salts and oak apples. This was a version of the most popular ink of the day—you may have heard of oak gall ink, if you’re a history buff, or kind of a weirdo—but the invisible version of oak gall ink was invented by founding father James Jay. The way it worked was that you would write a letter with normal ink and then write an invisible message beneath it with the invisible solution and the recipient would then introduce a second solution which would reveal the invisible message. The letters usually contained content that was too dangerous to say out loud like, the “we attack the British at dawn,” or “what the hell is going on with George Washington’s teeth? Why did we bother leaving England if we’re just gonna be worshipping another snaggletoothed white-haired rich dude in the new world? Based on his dental situation, that guy definitely has British sympathies.” We have some very sensitive BRITs in the discord, so I like to throw fuel on the fire.

So hiding information is the most primitive method of concealing info, and a dead drop may be the most primitive method for covertly transmitting it, but what if you want to conceal information in plain sight? I don’t want to have to worry about someone opening the wrong book in my library and accidentally reading my secret recipe for spicy honey-glazed chicken wings. Instead, I want to leave that recipe smack in the middle of a busy town, secure in the knowledge that no one will be able to decipher the exact amount of cayenne pepper that gives my wings the perfect mixture of zest and tang. Secret recipes are weird. I guess I can understand if it’s a patented recipe, like Coca Cola, but there are people who have secret family recipes, and that’s just greedy and mean spirited. Because why would I want anyone to enjoy the same level of deliciousness that I myself get to experience? I’m not sharing this with the world. I’m not some kind of culinary mother Theresa. Create your own recipes, chicken wing freeloaders!

So Enter cryptography.

In ancient Greek, kryptos is “secret” and “Graph” is to write. At its most basic cryptography is all about creating protocols and techniques that conceal the content of private communications from adversaries.

The first versions of cryptography were based on encryption, which is the art and science of converting legible messages into unintelligible gibberish that can then be reconverted to decipherable text. The most basic might be the substitution cypher, in which you simply substitute letters for other letters. But these can be easily broken by analyzing the frequency distribution of certain letters. For instance, If you have a long enough substitution cypher written in English it becomes obvious that the most common letter in the cipher is standing in for the most common letter in the English language—e—etc.

A transposition cypher, on the other hand, can be encrypted and decrypted using a grid, in which you write the original message in a certain pattern on the grid, and then use that same grid and pattern to decrypt it.

There have been cipher texts discovered dating back from ancient Egypt. One archaic version of cryptology technology is a scytale, which is kind of a brilliantly simple device. You take a ribbon or long strip of leather, and wrap it around a rod in a candystripe pattern, like a barbershop pole. You then write a message across the ribbon, one letter on each coil, continuing around the rod. Then you unwind the ribbon, and it becomes just a jumble of letters. The receiver of the message possesses a rod of the exact same width, so that when he or she wraps the ribbon around the rod using that same candy cane method, the letters once again align and the message is decipherable. But if you were to use a rod of any other width, it would again be gibberish. Very clever.

Speaking of clever inventions, two inventions in particular would revolutionize the espionage game. Radio, and the camera. And this is where the Russians really shine when it comes to being the sneakiest of sneakersons.

Let’s start with cameras. Photographic Camera technology has been around since The 1700s, when it was discovered that certain substances, such as silver salts, darken when exposed to light. Holy hell that was a lot of alliteration. Holy hell. Also alliteration. Cool.

But those first cameras were giant boxes, like the classic daguerreotypes (dug arrow types) of the 18th century. But in 1936, a German from Russia who was living in Estonia—it's confusing—named Walter Zapp told his wife "honey I shrunk the camera" when he built and marketed the Minox, the first ever subminiature camera. Subminiature may be a bit of an exaggeration... It's small. For a camera of that day. But I'd say it's probably about the size of a kind of elongated Swiss Army knife. You're not hiding this thing in a pen or your watch or something. Basically you had to be in a situation where you were unobserved, and then you could whip this thing out and take some photos with it, but it wasn't particularly discreet. The camera could be used with a variety of creative and sometimes comedic attachments, my favorite is the full size pair of binoculars, it looks just as ridiculous as you’re thinking it looks. Tiny camera, giant binoculars, but hey, it got the job done. Maybe. Or you just looked stupid and super conspicuous with your dumb ass tiny camera attached to a giant pair of binoculars. If you’re using a giant pair of binoculars, you’re clearly far away, why do you care if the camera is visible or not? Just use a big ass camera with a long ass lens. But apparently this was somehow a selling point for the Minox. These cameras were utilized by spies in both the east and west, they were very popular and are still highly prized by the espionage-nostalgia crowd. The company is still around, and now makes a digital version. If for some reason you want to carry another small digital camera in addition to the small digital camera that we all carry in our pockets at all times. Another interesting blip in spy camera technology: the pigeon cam. There are a few contenders for “most ridiculous object attached to a camera,” we’ve already met one: the full sized pair of binoculars. But the pigeon cam may be more ridiculous and is undeniably more adorable. The first pigeon cameras were developed in 1907 by German, Julius Neubronner.   homing pigeons Have long been used as Messenger carriers because of their unique ability to find their way home over incredibly long distances. So Julius fitted some homing pigeons with a bad ass looking leather harness and a time delayed camera. These things were cumbersome and I had no idea pigeons could heft an entire goddam Nikon into the sky. Pigeons were used by various armies in both world wars, though they were quickly eclipsed by actual spy plane technology. But I still love the fact that if you were a soldier in World wars one or two, you could have smiled at the sky every once in a while in the hopes of having a few heroic action shots snapped by some burly, camera-hauling pigeon photographers.

A more high-tech form of camera-based Espionage, the microdot camera could take a photo of a message, and shrink it down drastically on film so that a detailed message could literally fit into the period at the end of a written sentence. Microdot messages could be hidden anywhere from a hollow coin to a postcard—as mentioned, they could be literally embedded on a postcard as the period at the end of a sentence—and once received were read via the use of microscopes or even tiny lenses that themselves would fit into a ring or locket.

Let’s switch over to the other cornerstone of spy tech, the radio transmitter. Or maybe I should be more generic and say, just radio waves harnessed in numerous ways.

The first radio transmitters don’t show up until the late 1800s, developed by another German, Heinrich Hertz. Germans, killing it with the technology. Maybe that’s a bad way to put it. But sneaky sneakersons indeed. Anyway, Hertz, that name may ring a bell. The original versions of radio transmitters, so- called spark gap transmitters, didn’t send discernible audio information, they just transmitted pulses of radio waves, which could be used to communicate via Morse code. But in 1906 an American— represent!— named Lee de forest invented the vacuum tube, and radio finally found a voice. Or many voices. To be completely transparent, Lee De forest didn’t fully understand how his invention worked, but that doesn’t make it any less useful. I don’t understand how this microphone works, but that doesn’t stop us from recording our utterly useless and nonsensical musings every week. Not understanding how things work is not an impediment to using them. It also doesn’t stop me from being super judgmental when things don’t work exactly the way I want them to. “Dammit, microphone, why do I not sound like a radio announcer? Use your audio wizardry and all the magical soundiness that you contain to make my voice authoritative and worthy of respect!” Vacuum tube led to amplitude modulation, or a.m. radio, which in turn led to the superior practical frequency modulation or FM radio. Radio waves are especially useful if you’re a spy, or if you have a long morning commute and enjoy either music or dudes yelling. A lot of the most popular radio programs involve dudes yelling, for some reason. Along with microphones, radiowave technology would allow the recording and transmitting of conversations over large distances. And all of us are familiar with an espionage device for recording and transmitting audio, aka a covert listening device, aka a bug. The tricky element of bugs is that you have to find a way to smuggle them into a sensitive location and make them small enough to be undetected once they've been "planted." Another problem is power: the power source has to be tiny, which typically doesn't bode well for long-term operation. Enter The Thing, aka the Great Seal bug, which sounds like an amazing animal mashup but is in fact A legendary piece of spying tech that would lead directly to a common and very underrated piece of technology that we use on a daily basis.

So as World War 2 drew to a close, the Soviet Union's *Vladimir Lenin All-Union Pioneer organization* presented a wonderful gift to their war-time ally, the United States of America. Specifically it was presented to US Ambassador Averell Harriman and the gift took the form of a large, wooden carving of the Great Seal of the United States, which is unfortunately not an adorable aqua-puppy but instead is an image of an Eagle with his legs spread to an obscene degree, clutching an olive branch and some arrows. Have you ever really looked at this thing…I had not, and let me tell you, it’s like eagle porn. I didn’t understand the term “spread-eagle” before taking a closer look at this carving. That eagle appears to be laying on its back, fully exposed and ready to rock. The eagle is down to F, and might stab you with an arrow or give you some olives, it depends on your performance. Also, how amazing would it have been if the Great Seal of The United States was in fact a seal or sea lion, I can’t tell the difference. It has to do with their ears. But that would be so cool if the seal were a seal. Even a mediocre one, it doesn’t have to be a great seal of the United States.

I’d settle for a middling seal. I just love that it would sound like we’re a bunch of seal worshippers. It’s like the Wizard of Oz… we’re off to see the Great Seal of the United States. He’ll give me a heart, and Duncan a brain. That was so mean, I apologize.

So it turns out that if you are a large and powerful country exiting a massive global conflict, and you receive a gift from a supposed ally that is also a rival superpower vying for world domination, that gesture of goodwill should raise some alarms. It’s a little sus. Maybe don’t hang that gift in your office where you conduct shady American government business. Hindsight is 20/20 but this seems like diplomat protocol 101. Have we learned nothing from the Trojan Horse?

Harriman did in fact have the seal scanned for bugs and radio transmitters, but here’s the kicker: all previous versions of bugs had required a power source, and so it was fairly easy to detect them if you knew where to look. But this bug was special. It had been developed by a Russian engineer named Leon Theremin, maker of the Theremin musical instrument, an instrument that doesn’t require physical contact to play--it senses the hand position of the musician and emits annoying tones of varying frequencies that could never be confused with music. The theremin never gained much popularity--mostly because it’s terrible--but it did bring attention to Theremin himself, who as a result of his low-grade fame was locked in a Russian Gulag and forced to create spy technology. I would never say that any innocent person deserved that particular fate, but did I mention that the theremin is really annoying? Musical Karma. Anyway, much like the Theremin, this device didn’t require a physical connection to make it work. Instead, it was a small passive device, nothing more than a long but extremely thin antenna and also a small membrane; the tiny device was inlaid into the mouth-area of the eagle, and it was activated and powered by electromagnetic pulses. The Soviets simply had to direct a radio beam at Harriman’s office, and the Thing would be “illuminated,” AKA activated, and immediately begin transmitting any audio that it detected. As soon as the Soviets switched off the energy beam, the Thing would shut down, and once again be undetectable.

The Thing was finally discovered by accident in 1951. It had been hanging on the wall of the American embassy in Moscow, and a nearby British radio operator noticed that he was suddenly receiving random American conversations through his equipment. He alerted the American state department, and they were eventually able to track down the bug. And then I imagine that diplomatic meetings were a bit frosty and awkward for a few months.

The Thing and devices like it would eventually become known as High-Frequency Radio Bugs, and the technology that allowed them to function essentially endlessly without any internal power source would lead directly to what we know today as RFID, or radio frequency identification devices. If you have a cat or dog that has been chipped, you're benefitting from RFID technology. The transmitters can be the size of a grain of rice, and do not require batteries; as mentioned they are powered by an electromagnetic radio beam that is used to illuminate them. RFID is everywhere: in retail stores to track items and for self-checkout, for contactless payments and ID badges etc. So, thanks, Russian spies!

We already discussed one of the most notorious espionage-uses of radio technology. Way back in our first episode about unexplained phenomena, we covered numbers stations. These are fascinating, and I encourage you to check out that episode. while they have never been conclusively and definitively acknowledged by all of the world's major governments, it's also not entirely accurate to refer to them as "unexplained," because we know what they are. They are radio stations—many of them operating to this day—that continuously broadcast encrypted (and, I think it would be fair to say, cryptic) coded language or messages in order to communicate with spies in the field. Even though we now know what they are, they’re still creepy as hell. The broadcasts often consist either a young girl’s voice, or a robotic voice simply reading a series of numbers, preceded or followed by audible tones that sound a lot like a theremin. Numbers stations are weird, and have been freaking people out for years. Imagine tuning through radio stations back when that was still something people did, and coming across a random broadcast of a young girl reading strings of unintelligible numbers. We played an example of one in our first episode and it raised the hairs on my neck. But the way numbers stations actually work is very simple. There is a spy out in the field tuning in with a radio, and decrypting the messages using what’s called a one-time pad. The pad is literally a pad of paper, with different encryption keys on each page. The first portion of the radio message—often the tone—indicates which page of the pad is being used, and the spy simply flips to that page and uses that particular key to decrypt the rest of the message and then—this is critical—discards that page. Since the key is only used once, and the messages tend to be short, messages from numbers stations are essentially impossible to decrypt, and they provide a convenient method for conveying sensitive information to spies without worrying about a letter being intercepted or a phone call being recorded etc. It’s basically another case of hiding information in plain sight.

Many of the most famous versions of spying technology have been dead-ends in the actual espionage game, but either led to other common technologies today and/or entered into pop culture. Here are some of the most famous examples (famous among spy-stans)

The insectothopter. In the 1970s, the CIA built a dragonfly. Technically un unmanned aerial vehicle, basically an early drone, the insectothopter was flying tiny bug-robot, painted like a dragonfly and with wings that could flap. It used gas propellant to power the wings, but the tiny drone was too light to handle crosswinds, so eventually it was scrapped. No word on how many of them were swallowed by surprised frogs and birds. Less functional than a real dragonfly, and probably far less delicious. Crunchier than expected.

In the international spying museum in Washington DC you'll find the notorious Dog-poop radio transmitter. Which is just what it sounds like. Seems ridiculous but if you want to ensure that no one touches your transmitter, it's a way to go. Until someone picks it up with a plastic bag and tosses it into the trash.
Sticking with a similar theme, the rectal toolkit. A smooth lozenge-shaped container filled with

various tools of the spying trade. Espionage isn’t always glamorous. It can be uncomfortable. Weird that the rectal toolkit was omitted from all of the 007 films. I wonder how often James Bond was packin. Here’s a rule of thumb: if you ever see someone shuffling around, looking uncomfortable, there’s a 99% chance that it is a spy with a toolkit up his ass. That’s just math.

The 1960s introduced the lipstick pistol, also known as the kiss of death, a hollow lipstick tube capable of firing a single 4.5mm round. So, I guess some advice for female spies…don’t miss. I’m not a fan of these one-and-done weapons, because I am not that confident in my aim. How awkward is that. “Did you just shoot at me from that tube of lipstick? Oh. Very clever. I’m gonna kill you now.” There was also the flashlight gun, the glove gun, the umbrella gun… name a household item, and a spy has probably used it to shoot someone. Speaking of umbrellas. Did you want to take this one? I’m thinking we should actually save it for the next episode, because we’re going to follow up with at least one more installment of the espionage series, focused on famous spies in media and reality, plus notorious turncoats and spying capers

And of course we can’t end this episode without addressing that staple of pop-culture espionage, the shoe phone. Which wasn’t actually a phone, but it was an actual device. Made famous by the satirical 1960s television show “Get Smart,” in which agent Maxwell Smart would frequently have full-on conversations by yanking off his shoe and speaking into the heel, the shoe-phone was based on an actual piece of KGB spying technology, the heel-transmitter. It wasn’t technically a phone, and it wasn’t meant to be worn, but it WAS basically a radio station implanted in the hollowed-out heel of a shoe. The shoe would be hidden in the home or office of the target to record conversations. So much spying technology comes down to a billion variations of the same theme: the heel-transmitter is just a bug. It’s like: Listening device in poop, listening device in shoe, listening device in Great American Seal, listening device in anus, Gun in lipstick, gun in flashlight, gun in anus, camera in lipstick, camera in… etc.

So we’re not going to delve into the espionage technology of the 2000s in this episode for a couple reasons: one, modern espionage is almost exclusively digital. It’s all about decryption, hacking and cracking, it’s all internet or at least computer-based, and while I AM fascinated with computer technology, typing on a keyboard isn’t quite as sexy as slinking around with a lipstick pistol, or planting a dogpoop transmitter. I guess sexy is subjective. Plus, we’re going to cover cryptography and hacking and all of the juicy online espionage in future episodes devoted to those subjects. As I mentioned, next episode in this series will be all about famous spying capers, as well as famous (or infamous) spies in the media and in the real world.

21 Top Secret Devices From The Dangerous World Of Spies (buzzfeed.com)

Shoe Transmitter | Encyclopedia.com

https://crypto.interactive-maths.com/rail-fence-cipher.html

https://www.google.com/amp/s/

amp.interestingengineering.com/an-inside-look-at-the-spy-technology-of-the-future

https://www.google.com/amp/s/amp.interestingengineering.com/the-history-of-spy-gadgets-and-our-fascination-with-007

https://en.m.wikipedia.org/wiki/Espionage

https://www.mountvernon.org/george-washington/the-revolutionary-war/spying-and-espionage/spy-techniques-of-the-revolutionary-war/

https://www.google.com/amp/s/www.bbc.com/

news/business-48859331.amp

https://www.spyequipmentuk.co.uk/spy-cameras-through-history/

https://www.cbsnews.com/pictures/secret-cia-spy-gadgets-go-public/11/