DOWNLOAD PDF SURVEILLANCE DETECTION

Chapter 1 : How to Run A Surveillance Detection Route - Spy Escape and Evasion

The presence of hostiles in the field is the Surveillance Detection Agent's (SDAs) or Surveillance Detection Enabled Agent's (SDEAs) opportunity to detect them prior to the actual attack, and thus disrupt the attack before it happens.

The computers running the database are contained in an underground facility about the size of two American football fields. Surveillance aircraft Micro Air Vehicle with attached surveillance camera Aerial surveillance is the gathering of surveillance, usually visual imagery or video, from an airborne vehicleâ€”such as an unmanned aerial vehicle , helicopter , or spy plane. Military surveillance aircraft use a range of sensors e. Digital imaging technology, miniaturized computers, and numerous other technological advances over the past decade have contributed to rapid advances in aerial surveillance hardware such as micro-aerial vehicles , forward-looking infrared , and high-resolution imagery capable of identifying objects at extremely long distances. For instance, the MQ-9 Reaper , [87] a U. They have developed systems consisting of large teams drone planes that pilot themselves, automatically decide who is "suspicious" and how to go about monitoring them, coordinate their activities with other drones nearby, and notify human operators if something suspicious is occurring. This greatly increases the amount of area that can be continuously monitored, while reducing the number of human operators required. Thus a swarm of automated, self-directing drones can automatically patrol a city and track suspicious individuals, reporting their activities back to a centralized monitoring station. Data profiling can be an extremely powerful tool for psychological and social network analysis. A skilled analyst can discover facts about a person that they might not even be consciously aware of themselves. In the past, this data was documented in paper records, leaving a " paper trail ", or was simply not documented at all. Correlation of paper-based records was a laborious processâ€”it required human intelligence operators to manually dig through documents, which was time-consuming and incomplete, at best. But today many of these records are electronic, resulting in an " electronic trail ". Every use of a bank machine, payment by credit card, use of a phone card, call from home, checked out library book, rented video, or otherwise complete recorded transaction generates an electronic record. Public recordsâ€”such as birth, court, tax and other recordsâ€”are increasily being digitized and made available online. In addition, due to laws like CALEA , web traffic and online purchases are also available for profiling. Electronic record-keeping makes data easily collectable, storable, and accessibleâ€”so that high-volume, efficient aggregation and analysis is possible at significantly lower costs. Information relating to many of these individual transactions is often easily available because it is generally not guarded in isolation, since the information, such as the title of a movie a person has rented, might not seem sensitive. However, when many such transactions are aggregated they can be used to assemble a detailed profile revealing the actions, habits, beliefs, locations frequented, social connections , and preferences of the individual. The centers will collect and analyze vast amounts of data on U. Miller , data held by third parties is generally not subject to Fourth Amendment warrant requirements. The data collected is most often used for marketing purposes or sold to other corporations, but is also regularly shared with government agencies. Although there is a common belief that monitoring can increase productivity, it can also create consequences such as increasing chances of deviant behavior and creating punishments that are not equitable to their actions. It can be used for direct marketing purposes, such as targeted advertisements on Google and Yahoo. These ads are tailored to the individual user of the search engine by analyzing their search history and emails [] if they use free webmail services , which is kept in a database. An IP address and the search phrase used are stored in a database for up to 18 months. Their revenue model is based on receiving payments from advertisers for each page-visit resulting from a visitor clicking on a Google AdWords ad, hosted either on a Google service or a third-party website. This information, along with the information from their email accounts, and search engine histories, is stored by Google to use for building a profile of the user to deliver better-targeted advertising. In addition, most companies use software to block non-work related websites such as sexual or pornographic sites, game sites, social networking sites, entertainment sites, shopping sites, and sport sites. The American Management Association and the ePolicy Institute also stress that companies "tracking content, keystrokes, and time spent at the keyboard The Department of Homeland

Security has openly stated that it uses data collected from consumer credit and direct marketing agenciesâ€”such as Googleâ€”for augmenting the profiles of individuals whom it is monitoring. Nevertheless, human infiltrators are still common today. For instance, in documents surfaced showing that the FBI was planning to field a total of 15, undercover agents and informants in response to an anti-terrorism directive sent out by George W. Reconnaissance satellite On May 25, the U. Director of National Intelligence Michael McConnell authorized the National Applications Office NAO of the Department of Homeland Security to allow local, state, and domestic Federal agencies to access imagery from military intelligence Reconnaissance satellites and Reconnaissance aircraft sensors which can now be used to observe the activities of U. The satellites and aircraft sensors will be able to penetrate cloud cover, detect chemical traces, and identify objects in buildings and "underground bunkers", and will provide real-time video at much higher resolutions than the still-images produced by programs such as Google Earth. Some nations have an identity card system to aid identification, whilst others are considering it but face public opposition. In this case it may create an electronic trail when it is checked and scanned, which can be used in profiling, as mentioned above. RFID and geolocation devices[edit] Hand with planned insertion point for Verichip device RFID tagging[edit] Radio Frequency Identification RFID tagging is the use of very small electronic devices called "RFID tags" which are applied to or incorporated into a product, animal, or person for the purpose of identification and tracking using radio waves. The tags can be read from several meters away. They are extremely inexpensive, costing a few cents per piece, so they can be inserted into many types of everyday products without significantly increasing the price, and can be used to track and identify these objects for a variety of purposes. Verichip is slightly larger than a grain of rice, and is injected under the skin. The injection reportedly feels similar to receiving a shot. The chip is encased in glass, and stores a "VeriChip Subscriber Number" which the scanner uses to access their personal information, via the Internet, from Verichip Inc. Thousands of people have already had them inserted. This information could be used for identification, tracking, or targeted marketing. As of [update] , this has largely not come to pass. GPS tracking In the U. The geographical location of a mobile phone and thus the person carrying it can be determined easily whether it is being used or not , using a technique known multilateration to calculate the differences in time for a signal to travel from the cell phone to each of several cell towers near the owner of the phone. Victor Kappeler [] of Eastern Kentucky University indicates that police surveillance is a strong concern, stating the following statistics from Of the , law enforcement requests made to Verizon, 54, of these requests were for "content" or "location" informationâ€”not just cell phone numbers or IP addresses. Content information included the actual text of messages, emails and the wiretapping of voice or messaging content in real-time. A comparatively new off-the-shelf surveillance device is an IMSI-catcher , a telephone eavesdropping device used to intercept mobile phone traffic and track the movement of mobile phone users. IMSI-catchers are used in some countries by law enforcement and intelligence agencies , but their use has raised significant civil liberty and privacy concerns and is strictly regulated in some countries. Microchip implant human A human microchip implant is an identifying integrated circuit device or RFID transponder encased in silicate glass and implanted in the body of a human being. A subdermal implant typically contains a unique ID number that can be linked to information contained in an external database, such as personal identification, medical history, medications, allergies, and contact information. Several types of microchips have been developed in order to control and monitor certain types of people, such as criminals, political figures and spies,[clarification needed] a "killer" tracking chip patent was filed at the German Patent and Trademark Office DPMA around May

Chapter 2 : Chapter 11 Surveillance Detection - Surveillance Tradecraft

Counter Surveillance equipment is used to help you find out if someone is listening to your conversations or video recording you without your knowledge. While we specialize in covert video and voice recorders we do so with the intent that everything we sell will be used in a legal and ethical manner.

Twitter Advertisement If you have reason to be suspicious of a partner or employer, or they have reason good or bad to be suspicious of you, and you fear they might be filming you with a hidden surveillance camera, what can you do about it, other than use some futuristic, James Bond-style The Best Bond Gadgets Of All Time The Best Bond Gadgets Of All Time James Bonds gadgets are legendary. In this article, we run down some of the most futuristic gadgets from the films, and see how they stand up in the era of the iWatch. Read More camera detection device? Well, you could use a modern day, smartphone-style camera detection device. You Are Being Watched Someone is watching you. This is pretty much irrefutable in the post-Snowden era. But digital surveillance of emails and telephone records is a little less hair-raising than someone actually observing your movements via a hidden surveillance camera. But what about closer to home? Without being made aware of such surveillance in advance, you could find yourself being recorded, your movements and actions tracked, judged, no doubt misinterpreted. This intrusion might be performed using professionally manufactured security cameras, or custom built ones, perhaps using a webcam with an old PC, or a Raspberry Pi Build a Motion Capture Security System Using a Raspberry Pi Build a Motion Capture Security System Using a Raspberry Pi Of the many projects that you can build with the Raspberry Pi, one of the most interesting and permanently useful is the motion capture security system. What can you do about this? In general, two common methods are used to achieve this. The first is by using the smartphone hardware to detect electromagnetic fields Is Electromagnetic Radiation Dangerous? How To Protect Yourself? Is Electromagnetic Radiation Dangerous? Can cell phones cause cancer after all? The media certainly knows how to screw with facts. How does radiation emitted by electronics really affect your body? With the installation of a single app, you can move your phone around the area you suspect a camera to be hidden, and if a strong field is detected, you can be sure there is a camera secreted within the wall or object. Another way that smartphones can be used is by detecting light reflecting from a lens. You can also check out Glint Finder for visible lens detection. Remember that other options are available. If you have access to an infrared camera, for instance, this should detect a hidden camera, while low-cost devices using wireless networking may well appear in the list of nearby Wi-Fi devices Wireless Networking Simplified: The Terms You Should Know Do you know the difference between an "access point" and an "ad hoc network? What is a "wireless repeater" and how can it improve your home network? Read More in your home. With the app running on your device, finding the hidden camera should be straightforward, thanks to the radiation detection. Ready to use when you load the app, the detector software will display a red glow when the smartphone is in the proximity of a camera. However, it will also glow when near other types of hardware, so keep an eye on the number displayed in the middle of the screen, as this will exceed when a camera is detected. For added camera detection magic, Hidden Camera Detector also features an IR mode limited to portrait orientation with which you can find cameras that have so far eluded you. This is done by pointing the smartphone at an area where a camera might be hidden and looking for a bright white disc. The disc indicates the presence of a hidden camera. But what should you do about it? Well, you could always take it to a higher authority, but in the meantime, you might wish to take action. Note, however, that the problem with this is as soon as you do this, you may well alert the observer to your realization. For cameras possibly hidden high up, in lightbulbs or smoke detectors, staying out of sight can be difficult. Try these hidden cameras for around the home. Read More , they could use these tips to find it. Do you suspect unauthorized surveillance of your movements? Have you been filmed without your knowledge? Tell us about it in the comments below.

Chapter 3 : Surveillance - Wikipedia

There are many types of surveillance detection and today we'll be continuing to apply concepts and tactics used by Personal Security Detail (PSD) teams, with ways to detect static and mobile surveillance along your routes.

Data Analyst , Surveillance detection Executive protection providers and clients have recently experienced an upsurge of interest in surveillance detection SD. AS Solution has provided surveillance detection SD agents for a number of our clients for years. We also hold SD training courses for agents working in both the private and public sectors. This blog is not an SD how-to; there are already plenty of those on the web, some accurate, many less so. Rather, we aim to address the ten most common questions we hear about SD, especially as it concerns executive protection efforts in the US private sector. SD is a series of covert procedures and tactics that are designed and implemented in order to confirm or deny whether there is hostile surveillance of a principal, place or event. SD takes place over a given period of time and, where relevant, over distance. The aim of SD is to prevent a hostile act before it happens by identifying the surveillants and thus enabling disruption of the attack in the planning phase. Most attacks require pre-attack information to succeed. Any object persons, fixed sites, events, etc. Often, SD activities are added to traditional corporate EP programs on an ad hoc basis due to heightened risk scenarios. The addition of SD to a protective detail is particular to each assignment, so divulging the precise variables that warrant it should be considered an OPSEC violation. At the risk of splitting hairs, not exactly. SD is responsible for actively discovering hostile surveillance, whereas counter surveillance CS is tasked with actively preventing hostile surveillance as well as conducting surveillance operations on the hostiles themselves. In other words, SD strives to detect hostile surveillance while CS aims to negate hostile surveillance. So while there is indeed some crossover, SD is more passive than CS. Counter Surveillance Agents, on the other hand, often attempt to control or modify the environment to one extent or another in order to prevent hostile surveillance. Covert protection refers to tactics used to protect the principal, place or event while concealing the true function of the agent. While the covert protection agents should indeed be aware of surveillance, they are primarily concerned with preventing a hostile act. Should an attack be imminent, they act as an interdictory force to create time and distance between a threat and the protected object. I have come across some private sector details who refer to SD as CS as covert protection. This can be confusing to principals, detail managers, team leads and the agents themselves. Whereas a Surveillance Detection Enabled protection detail has the skillset and knowhow to conduct SD operations, an SD agent is not equipped to, nor responsible for conducting protective operations as an interdiction force. In the private sector, however, there is only a small handful of dedicated SDUs. Unfortunately, we also see private sector SD operations carried out by agents with no dedicated training; of course, such operations are largely ineffective against a genuine threat. The dedicated SD agent is typically distanced from the principal, and observes the red zone from the outside in. This is in order to detect surveillance from outside the red zone, where surveillants may be. As such, the SDA is typically not in a position to react to imminent threats in an interdictory manner. Protective agents whether they are covert, low-profile or overt who are SD-enabled are trained to detect correlations over time and distance which may indicate hostile surveillance. They may detect surveillance while working in a close protection role, or they may be moved from a close protection role to outside the red zone if circumstances dictate. In other words, they are trained both to look outward to detect potential threats, and to look from the outside in as required. The data analyst is key in mapping correlations which may indicate hostile surveillance. The data analyst may be a dedicated function within the unit, or it may be a field agent with additional responsibility. Consider the field agents as those tasked with bringing all the ingredients to the kitchen and the data analyst as the chef who knows how to transform the raw materials into a finished product. Data analysis is the missing link of private sector SD. SD should be taught by former or current SD field agents with field and teaching experience. SD employs a highly specialized skillset that cannot effectively be learned from instructors that have not actually worked a significant amount of SD assignments, had successes and made mistakes. Knowing how to impart knowledge â€” combined with the experience of success and failures in the filed â€” makes an effective SD

instructor. SD is not the end all and be all of protection strategies Protective strategies should be the outcome of thorough risk, threat and vulnerability analyses RTVAs. There is no one-size-fits-all solution, and certainly no one has an unlimited budget. The Security Master Plan is the document which describes in detail both the strategy and the tactics to be used in order to mitigate identified risks as identified in the RTVA. SD may be a part of the Security Master Plan, but it is only one component of the overall strategy â€" and very seldom the entire strategy. When used as an integrated element in corporate EP, corporate campus security or corporate events, however, the SD function can be a powerful means of enhancing the overall security of the principal.

Chapter 4 : TSCM AmericaÂ® National Eavesdropping Bug Sweeps Service Provider

This article will introduce a number of techniques to detect if someone is conducting surveillance on you. Before we get started, I want to make it clear that my knowledge and experience in this come from the private sector, and not from any clandestine government agency work. Though the principles.

It might be as simple as some crack head at your local mall watching the exit as you leave. If they think you look like an easy victim they may follow you to your car and try to rob or carjack you. This is what I do when someone hires my investigations company, Global Protection and Intelligence. First, we plan a surveillance detection route for our client. Example surveillance detection route For example, we would have them leave their house at Next, they would go to their third Cover Stop, which would be their gym and they would spend one hour there. On their way home from the gym, they would stop at the grocery store and pick up a few items, spending 20 minutes there. After the grocery store, they would head home. While our client is running their errands, my surveillance team is following the client to see if anyone is following them. We make sure to get pictures and license plates and we find out who the people are and begin to build a case. Also, make sure that you time the entire SDR. What I mean is, you need to know that you leave the house at Hopefully, you never have an ex-spouse or lover who you think may be following you, but if you do, plan a surveillance detection route to make sure. You mentioned having a lantern and flashlight in your car for emergencies. They might be a good thing to mention. Thanks for all of your good information. You are correct, these are great to have and I do have a few of them myself. The tactical pen is a great item, but how about some training to use the thing? I created a DVD that gives you training on how to use the pen in several different situations. You talk about how you carry a Ruger, is this the same gun you use for home protection? I often carry a Ruger LCP in my front, right pocket. I personally would not and do not use this gun for home defense. I purchased your retirement gun dealers information. Very good and informative. I am serious about perusing this but seem to be missing some things. All I got was the e-book but none of the marketing and additional info I was expecting. Could you give me some guidance on how to get that information. All of the information you mentioned is right underneath where you accessed the book itself. There you will see all of the marketing information and the audio interviews. I will have someone contact you to assist you in accessing these items. Click here to see the Retirement Gun Guide. How can I work for the CIA?

Chapter 5 : SURVEILLANCE DETECTION - AS Solution

Surveillance Detection Units (SDU) are organizations belonging to the US Government that have conducted secret surveillance that potentially broke national laws in various European countries.

A spectrum of specific, well-rehearsed actions and techniques that a properly trained person can perform to expose any surveillance team. If you were being followed, would you know it? Could you determine if you were under surveillance? Why does it matter? When a criminal organization is making heavy profits off their illegal activity, they will do anything to protect their operation. They have the funds and resources to collect intelligence on those who pose a threat to their existence. Surveillance Detection is complex. Anyone can make aggressive u-turns and cut through parking lots to make a determination whether or not someone is following them. This is important because if a surveillance team knows you are trying to lose them or identify them, they are going to change their tactics. Physical surveillance of a person can occur no matter how they choose to travel, so he or she must be able to perform surveillance detection while walking, driving and on all forms of transportation. You can benefit from the Surveillance Detection Training Course in two ways: With proper training, you can always determine your surveillance status. A rising trend for criminal organizations is to collect intelligence on those who seek to dismantle their operations. All persons involved in criminal investigations, intelligence operations or national security should be properly trained in counter surveillance and surveillance detection. Surveillance Ops offers counter surveillance training with the law enforcement and retail investigator in mind. We have developed an easy to learn course of instruction. As with all our courses, we start in the classroom and quickly progress to the street for realistic practical exercises. Topics we cover in our curriculum: Operating in the Red Zone. Where is the Red Zone?

Chapter 6 : Surveillance Detection Unit - Wikipedia

Example surveillance detection route For example, we would have them leave their house at am and go to their first Cover Stop, which would be Starbucks. They would stay at Starbucks for 15 minutes and then drive to their next Cover Stop, which would be Macy's to look at clothes.

Chapter 7 : How to Use Your Phone to Detect Hidden Surveillance Cameras at Home

During this day Technical Surveillance Detection and Countermeasure course students will learn numerous techniques to detect and defeat surveillance through electronic means and tradecraft. Detecting surveillance is the front line defense in protecting diplomats, government officials and other high value principals.

Chapter 8 : Surveillance Detection - 10 Things You Need To Know

Detection and surveillance technologies help to protect the public and ensure officer safety. Criminal justice practitioners use detection and surveillance technologies to manage and monitor crime scenes and to keep prisons, courts, schools and public areas safe.

Chapter 9 : Surveillance Detection/Counter Surveillance â€“ Surveillance Ops

Counter surveillance tools are designed to help users detect and prevent unlawful and unwanted monitoring, whether that means detecting hidden cameras, scrambling unseen signals, or creating white noise masking that prevents recording devices from capturing voices.