AS SOLUTION™
FORWARD THINKING

Tech tools for executive protection

A whitepaper for practitioners

Keeping our clients safe, happy and productive™

Tech tools for executive protection: A **whitepaper** for practitioners

TABLE OF CONTENTS

Communication tools for corporate executive protection

By Christian West

Technology can help the corporate executive protection team to improve the quality and speed of its communication as well as its responsiveness, resourcefulness and coverage. Let's look at the most commonly used tools of our trade.

Smart phones

Smart phones are the go-to tool for most executive protection communication and a lot of navigation.

These days, practically everyone carries an iPhone, Android or Windows smart phone. Executive protection teams are no different. As ubiquitous as they are convenient and cheap to use, smart phones come with plenty of useful apps – including our very own **ADVANCE productivity app and ODIN geolocation app** developed especially for executive protection use. Practically all smart phones feature GPS, so they can be used for navigation as well as location tracking.

When tracking, phone batteries drain more quickly than does the charge in dedicated GPS trackers. However, cell phones have the advantage of convenience: Most folks already have a phone that they need to remember to bring along and charge; they won't have to do the same with an additional GPS tracking device.

The downsides of cell phones are predictable—and manageable—in most situations:

- Batteries run out (make sure you have extra chargers and battery packs)
- They can break down (bring a spare or buy a "burner")
- Coverage can be unreliable in many locations (boosters are available, but some signal must be available to boost)
- Cell phones can be hacked

Important note: Natural disasters such as hurricanes can easily put cell phones out of commission due to power outages, flooding or heavy winds. And, as many of us have experienced in situations that cause cell phone usage to suddenly spike (anything from New Year's Eve to a big football game) they can be unreliable when you need them most because so many others are on the grid at the same time.

Two-way radios

Radios are great for executive protection teams conducting local communication and have a number of advantages compared to phones:

- They're rugged and made to take a beating.
- They're relatively inexpensive.
- They use "one-to-many" comms, so everyone on the team can get the same message at the same time.
- They don't depend on the phone network, so they can be more reliable than cell phones in times of crisis.
- They're simple to set up and use.

But radios also have their limitations:

- They work for voice only, and can't be used for text messages, emails or data transmission.

- They only work locally and not across great distances. Depending on the system you use, this can be anywhere between 1-5 miles (more if you add infrastructure such as repeaters, antennae and power stations, but loss of power might render repeaters and power stations inoperable). This can still be plenty of coverage for use on corporate campuses, between cars driving together, at events, etc.

- You don't need to be a skilled hacker to listen in. Anyone with a radio scanner can hear what's going on.

Satellite phones and modems

Satellite phones and modems are great for emergency situations and for communication when you're off the beaten track. If you've got your own electrical supply (battery, solar, generator, etc.), they'll work right through power grid outages. And some providers can deliver a coverage footprint that will keep you connected anywhere on the planet as long as you are outside and not in the middle of a dense rainforest. We like Iridium's low Earth orbit system, which provides coverage every place we've been so far. Satmodems have all the advantages of sat phones – and connect you to the internet for data and VoIP. Expect a little latency compared to good terrestrial connections, but the lag is worth it. Plans provide Internet connections in addition to voice communication.

Encryption is standard, although anything can be hacked.

When first introduced, sat coms were eye-poppingly expensive to buy and use. Prices have since dropped considerably.

Satellite phones and modems should be part of almost any contingency plan. They can be lifesavers, and most executive protection details will want to bring them along if only for backup communication.

Executive protection teams that travel light will want to check out the Iridium Go!, a compact satellite device that connects wirelessly to your Apple or Android device. Iridium's apps let you use your phone or tablet to do voice calls, send texts or Twitter posts, browse the web, keep up with your emails, check the weather and even compress and send photos. (See https://www.iridium.com/products/details/iridiumgo)

Wireless, network-free smartphone add-ons

A new, hybrid device type is hitting the market, and we're thrilled. Like the Iridium Go!, these devices work with and through your smartphone – which you no doubt always have in your pocket anyway.

But these new devices allow you to communicate completely off the grid – and without satellites – with team members who are similarly equipped. Let's take a closer look at two of them that we find particularly interesting.

1) goTenna

Website: **http://www.gotenna.com/**

goTenna is the first entrant in this new category. For us, it was love at first text.

What it is:
goTenna is a clever little device that lets you use your smartphone to send and receive text messages even if you've got zero phone or wireless coverage. It also allows you to share locations on offline maps. You can send to a designated user or group of users, or shout out your text to any other goTenna user in range.

Why you need it:

Sure, it's text only and no voice or data. And yes, the range is limited (we'd love to see it get Mesh capability to extend this).

But if you're off the grid and really need to communicate with a team member or any other buddy, goTenna can be a lifesaver.

Why we like it:

- **Simplicity:** We tested goTenna in Davos this winter, and it truly is a breeze to set up and use. Just download the app to your Apple or Android phone, link a goTenna to your phone via Bluetooth, write and send your message on your phone – and it's on its way to a similarly equipped phone within range. It'll work up to four miles (6.4 km) in most outdoor terrains, far less in urban settings.

- **Light/compact:** With a form factor of just 5.8 x 1 x 0.5 inches (147 x 25 x 13 mm) and 1.8 oz. (51 g), there's really no reason NOT to have one of these in your kit bag. Just in case.

- **Price:** At $199 for a pair of these (and yes, you need at least a pair – one goTenna will work only with another goTenna), this is the cheaper of the two new devices in this category.

2) Beartooth

Website: **https://www.beartooth.com/**

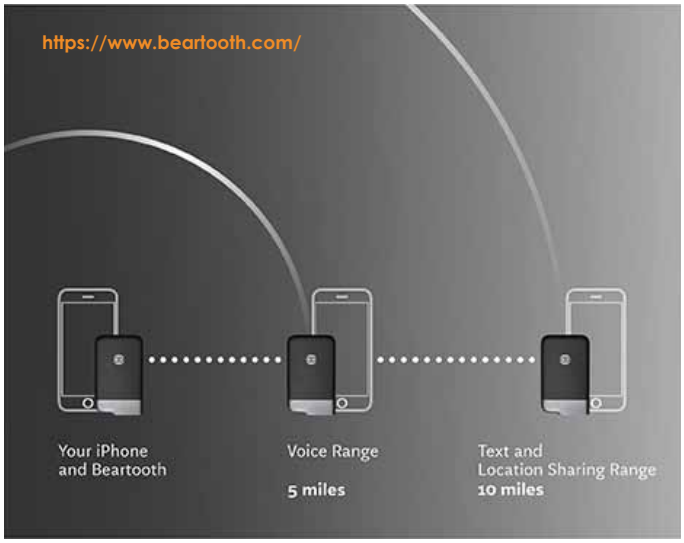
They're not in production yet, so we haven't tested them and can't vouch for performance. But as much as we love our goTennas, we can't wait to get our hands on a couple of Beartooths (or is that Bearteeth?).
Delivery was to begin in December 2016. Early pricing is $149 for a pair; it will rise to $399 after that.

What it is:

Beartooth does everything goTenna does and more: it's got voice (push-to-talk), and it will charge your phone if needed (it holds enough juice to charge an iPhone 6s 1.75 times). And yes, it's also got topographic maps that work offline, but only for the US and Canada.

Why you need it:

Beartooth lets you set up your own voice, text and navigation network without any cellular, wi-fi or satellite coverage.



Why we like it:

- **MacGyver appeal:** Pimp your cell phone with off-grid voice, text and maps and a charger – all in a package the size of a deck of cards? What's NOT to like?

- **Range:** According to their website, Beartooth has better range than goTenna: text and location up to 10 miles (16 km) with clear line-of-site, and voice up to 5 miles (8 km)

- **Mesh networking:** Mesh technology extends your off-grid network with every Beartooth node you add.

GPS tracking devices

Dedicated GPS tracking devices can be an excellent way to determine a person's or an asset's location. They're small, light and have better battery life than smart phones.

Like a lot of other tech, GPS trackers have gotten better and cheaper in recent years. The competition is fierce, and you'll find plenty of options from which to choose.

Here are some things to consider before opting for a tracker for corporate EP use:

- **Battery life:** This is the single most important criteria, and devices vary considerably. All decent trackers will last for at least 24 hours under normal use; a few will take you past 150 hours. Of course, the size of the device affects battery life since

bigger batteries last longer. So does location update frequency. Motion activation boosts battery life dramatically, since as long as the tracker isn't going anywhere it doesn't need to update.

- **App and interface quality:** All trackers come with dedicated apps that let you follow tracker location on your smart phone, tablet or computer. You'll want to be able to set predefined zones, then send a notice if the tracker leaves the zone's boundaries (geofencing); you'll want clear movement history; you'll want simple activation. In short, you'll want good user interface design.

- **Hardware quality:** Materials and build matter when trackers are on the road, so you'll want to opt for the best quality you can. Compare ports, buttons and charging cradles.

- **Panic buttons:** When the tracker is used for keeping an eye on people, panic buttons are a must.

- **Operator coverage**: A lot of people still have the mistaken idea that a GPS tracker is just a smaller version of the navigation device they have in their car – and are surprised to learn that they need GSM coverage, a SIM card and operator plan to transmit location data. And hey, that's the whole idea! So be sure you go with an operator plan that gives you good coverage where you will be tracking. Coverage varies widely between carriers and between cities and rural areas. Satellite phone tracking is also available – at considerably different cost levels than GSM.

- **Voice-to-voice calling:** This is a great back-up feature in case the tracked person's telephone dies.

- **International use:** Not all trackers work outside of their home country. If your tracking is international, make sure you are covered either with multiple trackers and plans, or one that works anywhere.

- **Total costs of operation:** Remember to consider both purchase price and monthly rates for GSM and/or satellite phone plans.

Computers and tablets

We won't go into much detail here, because we're sure you know all you need to know about these tools.

Suffice it to say that our go-to computer is the Microsoft Surface Pro 4. It's powerful, light, versatile and runs everything we need.

We also use our iPads more and more. They're light, easy to pack, and our ADVANCE and ODIN apps work as well on them as they do on a smart phone.

Article by

Christian West
Founder and CEO

Christian has been active in the executive protection industry since the late 1980s, when he worked for Danish musicians who relocated to Hollywood. Upon returning to Denmark, he founded his own EP company, which he quickly grew into Scandinavia's largest, before it was acquired by Securitas.
Christian founded AS Solution in 2003, and in 2009 followed his international clients to the US, where he is now based. An active member of ASIS and a leader in the corporate executive protection industry, Christian has personally planned and led high-profile engagements in over 76 countries for a wide variety of corporate and high net worth individual clients, including the international roadshow for the biggest IPO in history.

Tech Tools for **Event Security**

By Sonny Schürer, Mark Jaques & Antonio Revilla

Before we dig into the tools, let's be clear that while important, technology is only one of the four pillars of security. Without the other three – physical measures, personnel and procedures – tech adds little value. All the tech in the world is ineffective without properly trained personnel following smart procedures to integrate it within the overall protective effort, and then operate and monitor it effectively.

Indeed, tech tools are only as good as their operators and the follow-on procedures that we employ should a tool help identify suspicious items or persons. Ideally, such identification takes place as far as possible from the event or potential targets, and helps create time and space between potential threats and victims.

Good event security starts with a good RTVA

Just like other forms of security, good event security should always be informed by a risk, threat and vulnerability analysis (RTVA). Once the RTVA has been completed, we then select our tech tools based on the specific threats we're attempting to mitigate. If we're providing security for the same type of event year after year, we've found that it's a good idea to periodically review tools and threats to ensure that our tools, procedures and training are all adequate to counter current and pertinent threats.

Tech tools for event security can be categorized into three main types according to their role in protective procedures:

- Threat deterrence
- Threat identification
- Incident management

The one thing that ties everything together, of course, is communication tech, but that's covered elsewhere. So let's now examine the types of tech tools we use in event security.

Tech tools for threat deterrence in event security

Threats can be deterred at events in a variety of ways, and the tech we use for this depends on the situation.

Physical security tech restricts unauthorized access to events themselves, and to restricted areas within an event's perimeter. They are also useful in managing crowds, and in getting event guests to form neat lines rather than surge toward an entrance.

Starting at the periphery of the event venue, we find things like **bollards** (usually short, vertical posts) designed to keep vehicles away from people or buildings. These can be as permanent as concrete planters filled with flowers or trees, or more mobile systems that can be installed temporarily to secure an event.

At the soft end of the scale are low-tech but often-used **simple access control devices** such as plush ropes and stanchion barriers familiar from theaters and hotels. Their

slightly more innovative cousins are the retractable webbing and post devices often used in airports. Although easily breeched, these devices are great ways to manage traffic flows in many situations where people politely wait their turn.

Sometimes, though, velvet ropes and relying on politeness are just not enough. Management of large crowds at rock festivals, for instance requires a whole different level of sturdiness than do cocktail receptions. **Mojo barriers** are great for outdoor events where large numbers of people need to be kept from stages and other restricted areas. The company offers a complete product line of barriers that can be configured in many ways.

Turnstiles, in conjunction with **scanners** that read credential information, are particularly useful at high-volume access points where many people need to be checked before being allowed entry to restricted areas.

Name badges and ID cards that carry credential information are an essential part of security for events such as trade shows or conferences. At the simple end of the range we find **printed badges** that enable security staff to visually identify who should be allowed access to which areas, typically by using color codes, or scanners to check **bar codes**.

RFID cards offer even more possibilities to fine tune the match between credentials and access. Content on the embedded chips can be updated so the card can be deactivated in case of theft or loss. Speakers can be granted backstage access for rehearsal and performance times only.

Another type of physical security tech used to control access is **CCTV surveillance**. Cameras are a simple but helpful way to discover and monitor emerging threats, for example the movements of individuals, groups and crowds at large events. They also enable agents to spot "holes" in crowds, and thus discover that people are lying down and not standing – a sure sign of trampling danger.

Similarly, **thermal cameras** such as those from Flir reveal important information on changes in crowd density that allows event security staff to spot areas that are "heating up" – and put event guests at risk.

Contact pressure sensors on fences or barriers detect and record the pressure exerted by crowds on barriers. This gives event security staff real-time information on barrier hotspots so they can take proactive measures. Analysis of data collected over time also provides insight into where barriers come under most and least pressure, so security planners can adjust barrier layout accordingly in future events. Mojo Barrier's **"Barrier Load Monitor System"** is a good example of such technology.

A recent innovation that goes beyond simple visual monitoring uses Wi-Fi or Bluetooth connections – and the ubiquitous smartphones almost everyone carries – to provide **real-time location analytics** of crowd density and movement, enabling event security managers to deploy staff where it's needed, or initiate other measures to deter or defuse risky situations. These can include instances where too many people are gathered in one place and crowd surges from one place to another. **CrowdConnected** is one company providing these tools. **Bluetrace** is another.

Social media listening and engagement tools provide a different kind of crowd management capability. Security managers can observe what people at an event are communicating about – and where they're doing it – and then deploy staff to deal with emerging security situations if necessary. They can also communicate security-relevant messages directly to event participants.

Finally, let's not forget **event-specific apps** and **digital signage**. These are useful in providing event guests with a constant stream of updates, some of which can deter security threats. For example, security managers can prepare security and information that can be quickly communicated from one to many if needed, or session overflow can be reported to prevent crowd build up and better manage crowd flow. Apps and signs are also practical for things like lost and found information, helping a traveler find a misplaced passport before he or she leaves the event for the airport.

Tech used to identify threats

A number of tech tools are useful in detecting items that pose potential threats:

Security wands or hand-held metal detectors help agents discover weapons or other metal objects – and are easy to travel with.

Walk-through metal detectors, also known as magnetometers, are good for high-volume situations where a lot of people need to get through access control in a short period of time. Both CEIA and Garret provide excellent options, including portable solutions are easier to transport.

X-ray scanners enable agents to inspect bags – as well as freight and mail, if necessary – for weapons, explosives, bottles, etc. We like the technology that Astrophysics and Smiths Detection put into their products.

Sniffer dogs: While some might quibble with us for referring to our four-legged colleagues as "tech tools", we need to include them in this blog anyway. K-9 EDD (a.k.a. Explosive Detection Dogs) have proven their efficacy in detecting explosives (as well as everything from cannabis to cancer), and event security managers rely on them for both pre-event sweeps and access control.

Tech used for incident management

The most important tools for managing event incidents are **emergency medical kits**. Well trained event security staff must be able to provide emergency care if needed.

GPS trackers for geolocating security staff, medics or assets are also helpful in managing incidents. The trackers allow managers to determine where people and things are located, then direct them to other locations as needed. Geofencing can also be set up, so that alarms are delivered should people or assets enter or leave designated areas.

Operations centers pull all relevant information and communications in one place. Tech used here includes monitors, software and communication tools.

Legal issues regarding tech tools for event security

Certifications. Licenses. Permits. Training requirements. Before you deploy any tech tools at an actual event, public or private, you need to understand and comply to all relevant legislation in your jurisdiction.

It's beyond our ability here to dig into all legislation, everywhere. Suffice it to say that legal requirements for event tech vary considerably from country to country, state to state, and even city to city – and that event security managers need to know where they stand.

Article by

Sonny Schürer
Senior Vice President

Sonny Schürer, Senior Vice President, has helped manage AS Solution since its founding in 2003. A leading member of The Danish Trade Organization for Safety and Security and an active member of ASIS, Sonny has extensive experience in executive protection, event security, investigations and maritime security.

As a member of AS Solution's management team, Sonny heads the company's European operations from its Copenhagen-based European headquarters. Sonny serves on the board of Parsifal Services, AS Solution's partner in corporate investigative services, and has also overseen the development and growth of AS Solution's anti-piracy services, Scandinavia's largest maritime security service with operations worldwide.

Mark Jaques
Operations Manager

Event security operations manager with responsibility for managing global teams, working closely with client security managers and vertical business lines, and logistics vendors. He has organized security for client-sponsored events around the globe.

Antonio Revilla
Security Professional

Graduated at the top of his class at the USAF Law Enforcement Academy and the country's top counter-terrorist and protection courses and has provided protection for POTUS and numerous heads of state at Andrews Air Force Base with the U.S. Secret Service.

Completely bi-lingual in English/Spanish, Antonio has extensive experience in all aspects of international security with more than 25 years in the private sector. He has served multinational corporations and high-profile clients in the entertainment and sports industries, and has headed security for global events like the Miss Universe Pageant and the Ted Conference. Antonio was founder of O&R Protective Services, a national leader in complex event security projects and an AS Solution company.

Medical tools for corporate executive protection

By Eric Stewart

Medical training and knowledge matter more than medical tools. That statement might bother some of the more "gear-oriented" people out there, but it can't be emphasized enough: no gizmo, gadget or cool toy can ever replace appropriate training and experience. When I did paramedic schooling, I was lucky enough to ride along with one of the most notable and experienced paramedics in the field of emergency medicine at the time. When we responded to a call, the paramedic stepped out of the ambulance carrying nothing more than a caring attitude and a smile. If and when he needed additional tools, he'd be as likely to ask for a pen as for some advanced piece of gear.

This example isn't meant to dismiss the use or importance of proper equipment—of course not. But I've seen too many executive protection practitioners who have no problem packing and lugging a 40-pound medical kit around without being able to do basic CPR. On the other hand, I've watched a trauma surgeon save a guy's life with a razor blade, a pair of desk scissors, a handful of paper clips and some duct tape. You'll find the best medical kit ever invented right between a good practitioner's ears.

You've got eight minutes to save the guy's life. How are you going to use them?

You should also keep in mind that in most developed countries, the average ambulance response time is around eight minutes. In other areas of the world, you might have to wait much, much longer—if an appropriate ambulance is available at all.

But sometimes even if an ambulance is only a couple of minutes away, you just can't afford to wait. The principal, or one of your team members, needs your help right now.

Of course, different patients, situations, locations, and injuries all call for different equipment, techniques and skill sets. But as an executive protection pro, you have a distinct advantage over other emergency medicine practitioners: you already know your potential patient. Because that's your principal. You can prepare yourself using vital information such as medical history, allergies, current medications, insurance, next of kin/POC, company risk management POCs and much more.

Get good training

Where do you start with training, though? Regardless of your background, you'll generally want to start with EMT-Basic. You can presume companies and organizations will recognize the standards behind an EMT-B certification, but you really shouldn't expect them to understand or appreciate your hard work at the "Combat Lifesaver" course or other niche medical certifications such as "Billy Bob's School of Ninja Medicine".

Further training in areas such as Tactical Medicine or Wilderness Medicine can be helpful, but these more advanced disciplines and should not be your first foray into emergency medicine. If you haven't mastered the basic skills, you sure as hell won't be able to perform them under fire or on in the middle of ice field at night. At the end of the day, medicine is medicine—regardless of where you are.

Forget the idea of a "perfect" medical kit, and welcome to my kit dump

Medical tools are actually very personal, and every practitioner will have his or her own opinion of what constitutes the ideal kit. It's just like asking armed executive protection professionals about what the best firearm for the job is: you'll get plenty of informed but different opinions. So here's my opinion on medical tools: there is no "best" kit that works across the board and applies to all situations. If it existed, everyone would already be using it, right?

Instead, I thought it would be interesting to do a quick "kit dump" with you, so we can have a look at the items in my bag, and I can tell you why I like them. I'll add a few words for a few items in particular, then include a spreadsheet checklist for details and individual agents that I hope you'll also find useful.

General Rule: I hate carrying stuff around, so I always look to lighten the load and ensure that I have all of the items I might need. It's a trade off, and I think the best way to strike the balance is to make sure that everything in your bag serves more than one purpose. The worst items are those that are large and bulky and only have one, esoteric use.

Bags: As a rule, your medical bag should be able to hold everything you need – inside the bag. Nothing should be strapped to the outside. Why? You want something nondescript that doesn't broadcast "medical bag", because that's what your principal would want if he or she bothered to think about it.

Imagine following a principal around with a big red bag with stethoscopes and trauma shears hanging out all over the place. What does imply about your principal? Does he or she have some life-threatening medical condition that requires constant attention? How would that perception affect the price of the company's stock or the image of the principal? Personally, I like the black canvas STOMP bags because they look just like a backpack, but are well-organized inside. You can purchase fully stocked STOMP bags, but I recommend finding an empty bag for a fraction of the cost, and stocking it yourself with only those items that meet your approval.

Some practitioners pack their bags with great care – even to absolute perfection. That's all nice and well. It even works for a while, but when it's crunch time the contents of the bag most often get dumped out onto the floor or the ground. I like to put things in my bag so I generally know where they are, but don't fixate too much over a specific load-plan. Your approach may vary.

A popular philosophy is to preposition several kits throughout the operational area, in other words, one for the car, one inside of the residence, or the boat or plane. To me, this is the "fire extinguisher" approach; trying to have medial bags around where you are likely to need them. As a medic, I strongly believe that it's not how many different medical bags you can bring to bear on a sick client, but how much training and experience you can interject within a very short amount of time.
Finally, I maintain a log using an app called My Stuff Pro so I know what's in my bag and when items expire. If I use an item, I can simply mark it in the app, which then reminds to replace it.

Pulse Oximeters: These are small devices that attach to the tip of a finger and give instantaneous readings of heart rate and blood oxygen saturation. Both of these readings are vital to understanding the patient's condition. Pulse oximeters have their limitations, but a skilled practitioner will understand these and take the limitations into account when caring for the patient. I attach a very colorful lanyard to mine so that when I turn the patient over to higher care, I don't forget to collect the device on my way out.

Stethoscopes: I carry a 3M Littmann, Master Cardiology, 27" (Black Edition) stethoscope. I've had this for many years and it has held up very well. I've taken a piece of medical tape and wrapped it a few times around the right ear-branch, so that in the dark I can ensure that I'm wearing the stethoscope the correct way around. Few things are more embarrassing than putting a stethoscope on backwards; nevertheless, I've seen all levels of clinicians do it. The other modification I make is to tape (the cap of) a black Sharpie Pen to the upper-portion of the central tube. The pen will stay inside of the cap, and I will always have something to write with.

3×5 Cards: While pretty low-tech, a stack of 3×5 cards held together with a small clip is invaluable. You can take notes on the cards, and then simply hand them off to the next level of care as needed. I've seen people scribble on gloves with a Sharpie, which seems silly when your gloves get covered with all sorts of, ahem, stuff. What are you going to do, hand a blood-covered glove to the nurse, and go, "Hey, my notes are on there somewhere"?

Headlamp: This is an invaluable piece of equipment that lets you provide care with two hands instead of trying to hold a penlight in your mouth and carry on a conversation. I used to have the biggest, "baddest", brightest lamp that I could find; then I realized that it's outrageously uncomfortable for a conscious patient to have such a thing shining in their eyes. Instead, go for something that's bright enough for care—but not so bright that you could land a helicopter with it.

Triangular Bandages: These are good for slings, tourniquets, hand-ties (to stop a patient's hands and arms from flopping around during CPR on a gurney). They make pretty good bandages as well. I have about 10 of these in my bag. I've seen guys pre-tie a stack of Popsicle sticks in one or two of the bandages to use as a windlass for a tourniquet. Some guys color-code the ends so that when they pass a handful of them under a leg to secure a splint, they know which ends get tied to which.

Trauma Shears: Go for anything that works and that you're willing to lose, because these are the first things to get left behind on a trauma scene. Don't invest in a $70 pair of "crew-served" shears unless you're happy to repeat such an investment every month.

Apps and Books: There are a ton of emergency medicine apps out there, and they are changing all of the time. Medicine is not a dark art, it's a science, and like all sciences information is readily available in all sorts of forms. As a general rule, I recommend reference material that is

Item	Detail-Level Kit	Notes	Agent-Level Kit
Medical Kit Recommendations			
Lip Treatment	2		1
Burn Spray	1		1
Instant Glucose	2	Can substitute cake frosting	1
Pill Pack	1	Create pill packs with common adult and ped OTC medications: ASA, Tylenol, Naprox, Benedryl, imodium, etc.	1
SAM/universal splints	2		1
Field dressing 7.5"x 8"	2		
Triangular Bandages	5		2
Cervical collar	2	Must be adjustable. Add Pediatric Collar if a child is anticipated	
6" Elastic bdge	2		
2" Elastic bdge	3		1
4"x4" Sterile pads	50		20
2"x2" Gauze sponges	10		5
5'x9" Abdominal pads	2		
Eye pads	2		
Bandage strips assorted sizes	30		10
Butterfly strip	5		2
Instant ice packs	5		1
Roll of 1" tape	10	Should be cotton not nylon or poly	2
Stethoscope	1		1
Blood pressure cuff	1	Manual cuff	1
Trauma shears	2		1
Penlight	3		1
Safety pins	20		6
Exam gloves (pairs)	20	Store in zip-lock bags marked by size	4
Irrigation syringe 50cc	1		
Triple antibiotic packages	20		5
Burn aid packages	3		1
Alcohol wipes	50		10
Iodine PVP wipes	50		10
CPR mask/face shield	2	One Adult and One Pediatric	1 Adult
OPA & NPA	1 Set		4 ccommon sizes
5 -Tongue depressor	5		5
Israeli 4" dressing	2		
Israeli 6" dressing	2		
Hand sanitizer	5		1
Additional Equipment			
Pulse Ox	1		1
AED	1		
BVM with masks	1	Only adult unless pediatric is anticipated	
81 mg ASA	Pill Pack		Pill Pack
IV Start Kits with 2x 1000cc NS	2	Package start kits with NS bags so that it is a single, complete unit	
Hemostatic Intervention	2	Highly arguable	
Nitro tabs	20	Need Rx	5
Complete Suite of ALS Medications and Delivery Options		ALS Only: Need Rx	
Emisis bags	4		1
Consider portable O2 system	1	Not a great cost-benefit argument unless Client has a Hx or repriatory ilness. Then complete suite of COPD/Asthma Tx	
Combi-Tube or King Air	2	Airway management device. Stay away from ET tubes	
Suture material and instruments	Various	Additional training required	
Nail Clippers	1		1
Benidine 20ml bottle	1		
Multi-Tool	1		1
Head Lamp w/ spare batteries	2		1

designed for one or two levels above your current level of practice. I like to understand what the ER Physician is going to be immediately concerned with, so that I can have that information or procedure well at-hand.

The general references that I use are:

- Pharmacopeia: These give the clinician access to a ton of drug information, including trade and generic names, recommended dosages, interactions, etc. Every emergency medicine resident in the Emergency Department has this at their fingertips. I personally use Tarascon's Pharmacopeiaedited by Richard J. Hamilton, MD.
- Pediatric Information: "Broselow-like" apps that take the age or weight of the pediatric patient and calculate device sizes, drug dosages, vital signs, etc.
- Pocket Reference: No matter what your experience level, you'll always be glad to have quick access to some pocket emergency medicine reference. I use Tarascon's Adult Emergency Pocketbook by Dr. Steven G. Rothrock, MD. I'm unsure if it comes in an app version. I carry the actual book, and often add notes to it.
- Anatomy and Physiology: Netter's Atlas of Human Anatomy is hard to beat. It's a classic, it has an app, that lets you review specific anatomy when you have some time to spare.
- Pathophysiology: Pathophysiology by McCance and Huether is a really good place to start. It's a pretty weighty tome, but if you need to know the "pathophys" of a respiratory disease, that's the place to start.
- EKG Interpretation: 12-Lead ECG, The Art of Interpretation by Garcia and Holtz. Admittedly this is an advance skill if you're an EMT-B, but if you're considering delving into the ALS world, this is the best I've seen. (Link). Alternately, your first foray into EKGs should be Dubin's seminal book Rapid Interpretation of EKG's.

Make sure medical issues are part of your RTVA

When most people think of corporate executive protection agents, their understanding is informed by images of bodyguards ready to thwart physical attacks. Understandably, risk, threat and vulnerability assessments (RTVAs) tend to focus on external factors, and there is no doubt that we must be trained and ready to handle physical threats and defuse aggressive confrontations.

But real protection focuses on mitigating risk to the principal in all forms: from the immediate to the probable to the possible. Whether you do the math like an insurance actuarial pro or just use common sense, you'll soon find that a handful of medical emergencies are far more likely to befall most principals than terrorist or active shooter attacks. That's why it's critical that executive protection professionals have solid skills and appropriate tools for first aid and medical assistance.

Article by

Eric Stewart

Retired U.S. Army Special Forces officer

Eric Stewart is a retired U.S. Army Special Forces officer who works in Chicago for A.S. Solution Operations.
Eric has over twenty-years of experience in emergency medicine. He has worked on the frontlines of emergency medicine as an EMS Paramedic in both the inner-cities of Atlanta and Chicago, as well as in several urban trauma centers and emergency departments within the United States as well as post-earthquake Haiti and throughout Latin America.

Eric has provided emergency medical services and consultancy to a leading global medical evacuation company, a top rated reality television show, and has spent two years in the Middle East as a security-medic working for several international media outlets.

Eric currently lives in Chicago with his wife, an Emergency Medicine Physician, and together they frequently travel and speak on current emergency medicine issues.

Tech tools for **halls & walls security**

By Sean Paul Schuriemen and Christian West

In the good old days, there were few tools other than black coffee and an uncomfortable chair that made much of a difference to the job of "sitting outside a hotel room all night trying to stay awake." Halls & walls security was often considered entry-level work for executive protection agents, and not much emphasis was put on either developing technology or methodologies.

But while halls & walls details might at first glance appear less glamourous than other close protection work, it is no less important. Just consider what best-in-class halls & walls security could have done to prevent or mitigate the impact of the 2016 Kim Kardashian robbery in Paris.

And actually, "the good old days" were not always that great. We now know that tech can seriously improve halls & walls performance, so it's an important part of our capabilities moving forward.

Why halls & walls matters in the overall executive protective system – and how tech helps

Of course, without solid training and reliable, tested SOPs, all the tech gear in the world doesn't matter to protective security. The same holds true for tools for halls & walls. Still, when enhanced by the proper tech and procedures, halls & walls security is an important part of EP work for a number of reasons:

- Unlike the simple use of security cameras, tech-enhanced halls & walls is not about recording what happened (although this can also be helpful). It's about using tech to deter or prevent things from happening, and thus mitigate risk.
- It does this by controlling and limiting access to the principal, especially during travel to places where such access control may not otherwise be reliably secured.
- The physical presence of agents will always be part of real halls & walls security. Tech can, however, leverage the effectiveness of one or two agents and increase their productivity manifold.
    - As they say in the military, tech tools can be a "force multiplier" that provides more – and better – halls & walls security without increasing headcount.
    - Instead of struggling to stay wake as they keep an eye on a specific space, agents can use tech to generate alerts – and allow them to spend brain power on other pursuits, such as intel work, while "they're just sitting around anyway".
    - When enhanced by tech, halls & walls teams can choose to turn their visibility up or down. Sometimes it's important to be noticed as part of the deterrence objective. Other times, the principal is not interested in appearing to be in a protective bubble. Tech lets us turn the dial up or down on overt/covert halls & walls operations.

Types of tech tools for halls & walls security – and how they work together before, during and after a detail

The tech tools we use for halls & walls security fall into five main categories: communications, TSCM, sensors, mobile operations coordination and emergency incident response.

With the exception of communication tools, which are useful no matter where or when, these types of tools roughly correspond to the flow of how we secure an area before, during and after a protective detail:

- **Before:** We use **TSCM** gear to make sure the spaces where the principal will be are clear of surveillance. We then set up a variety of **sensors** to maintain the integrity of our TSCM sweeps.
- **During:** We rely on our **sensors** to enhance our situational awareness of relevant spaces and gather information on what's happening, and **mobile operations coordination tools** to collaborate and coordinate protective measures. If necessary, we also make use of **emergency incident response tools**.
- **After:** Sometimes, after a detail has been completed, it can be helpful to use information gathered by **sensors** for after-action reviews, analyses or even investigations.

Sensors increase situational awareness…

A wide variety of sensors make up the bulk of the halls & walls tool kit.

These include:

- Mobile camera systems
- Motion detection sensors
- Smoke detection devices
- Infrared sensors
- Barometric pressure sensors

…but must never compromise the principal's privacy
Protecting the privacy of the principal is paramount to all we do, and use of sensors – sophisticated or simple – must never compromise this.

Even though it might be helpful for security reasons to have eyes and ears on the wall in all the spaces where we know the principal will be, we never just do that. Installing sensors in the principal's hotel room would be completely out of the question – and out of bounds – in almost any case imaginable, for example, and often inappropriate in other spaces, too.

Sensors must never invade client privacy. Period. And while we don't need to involve the principal in all the nitty-gritty, transparency of operations toward clients is essential to ensure this. They should be informed of the types of sensors we're using, and how we're using them.

Mobile operations tools empower team coordination and better intel

Pulling information together in a mobile operations center can provide a huge preventative and reactive advantage. It is now possible to combine a wide variety of information sources all in one place – no matter whether your operations hub is back at HQ or inside a hotel room – to give mobile teams significant protective benefits.

These disparate information sources include:

- Data from halls & walls sensors
- Information from on-the-ground agents
- Feeds from third-party and other intelligence sources
- Asset and traveler tracking systems, including our own ODIN

Halls & walls agents have a lot of time where they are "just on post." Yes, they're keeping eyes and ears where they should, but they often have surplus brain power that can add value to your intel team. Smart EP managers know this, and they equip their halls & walls team with training, instruction and tech that expand their capabilities and increase team efficiency and value to the client.

Tools for emergency incident response are always part of the kit

The final type of tech we want to take a look at is the stuff you hope you'll never need, but would be foolish to travel without.

Halls & walls teams should of course be ready to handle medical emergencies.

All halls & walls teams should also be ready to deal with fire. Literally.

While the likelihood of hotel fires decreases with the number of stars they earn, the halls & walls team should travel with smoke detectors as well **as good, compact evacuation masks** like the one we featured in our gadget roundup last December – both for the principal and for themselves.

Future trends for halls & walls technology

Like all other tech, halls & walls tools continue to get better, smaller and cheaper.

We think these equipment types will see interesting innovations in the next few years, particularly concerning how they integrate, and enable teams to use them to increase the principal's safety and the protective team's efficiency.

The TSCM tools for executive protection

By David Falco & Sean Paul Schuriemen

More casually called "bug sweeping," TSCM refers to electronic and physical inspection of a given area (a principal's room, a vehicle, or even an entire building) to find and neutralize eavesdropping devices—or really, any unwanted surveillance device a nefarious third-party could use to spy on their target.

Think of the implications if someone is eavesdropping on your principal. Let's say they're traveling, and their hotel room is bugged. The bad guys can now record—and exploit—private conversations (either personal or business related). Along with corporate espionage, such bugging might lead to some serious security issues for the principal. What if someone knew your itinerary for the next day? Where you'll eat, how and when you'll get there?

Effective TSCM is crucial in our line of work, both on corporate campuses and on the road.

RF and non-RF: The 2-part bug sweep

The term "bug sweeping" calls to mind scenes from spy movies: Security pros walk around a room with an array complex apparatuses, searching for state-of-the-art devices that emit detectable signals. And, yes, that is one part of a TSCM bug sweep.

The other part entails looking for things that are no more high-tech than a simple recorder—the kind anyone can buy for a few bucks. The bad guys just need to cleverly stash one of these then retrieve it later.

To find such non-RF devices, nothing beats a thorough physical search. This is why complete TCSM inspections must consist of two parts: looking for devices that emit radio frequencies and for devices that don't. Each part requires different gear and methods, so let's look at both types of devices and the tools we use to detect them.

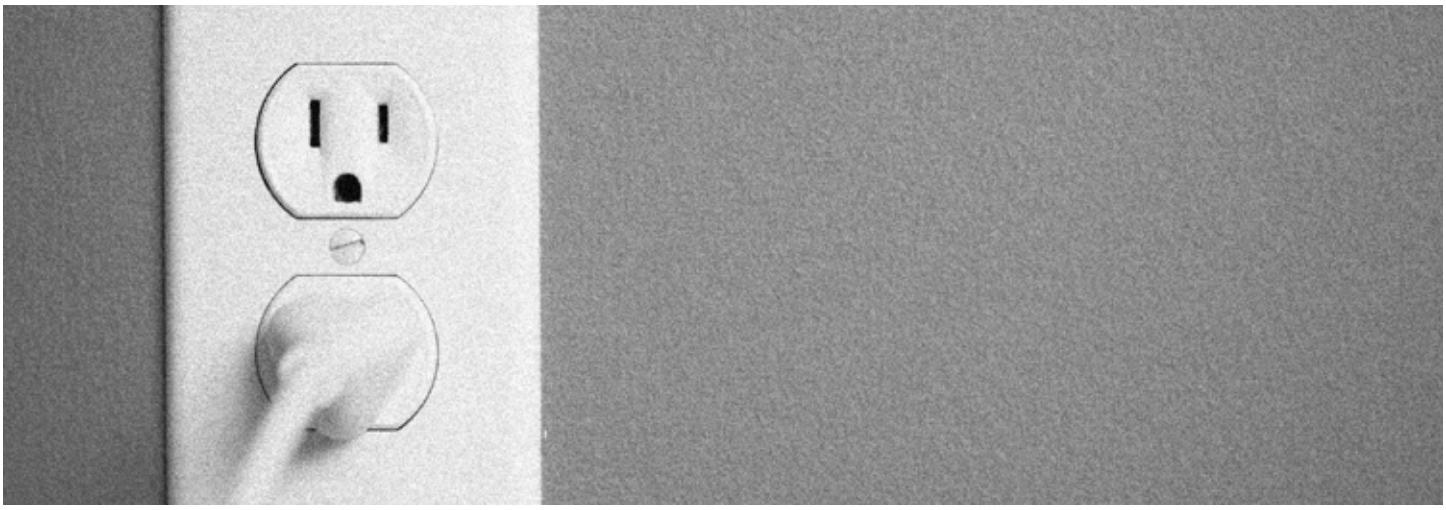
RF devices

Radio frequency devices send data, including voice and video, to a third-party. They're the most "direct" bugs as they transfer info in real time and don't necessarily have to be retrieved. This makes it difficult to discover who planted the bug. RF cams and recorders can tap into the local wi-fi network, or even have access to a cell-phone network. And you can buy them online for less than $30.

Because they transmit data via transmitters within the RF spectrum and not cables, it can sometimes be easier (although by no means easy) for a properly trained and equipped agent to detect them.

RF devices can be particularly tricky to find and neutralize. Some emit radio frequencies only at specific moments so they would not necessarily be spotted by doing a single sweep at any given time. Others simply record to a hard drive, USB, SD card, or some other storage device that can be recovered at a later time.

Technology being what it is, such devices continue to get smaller and cheaper—making them more accessible to more people, and more prevalent than ever.



Non-RF devices

Audio recorders, cameras, microphones and other "hardware interception" devices don't emit RF, but instead rely on other tech such as phone lines, computers and DSL/cable lines to transmit data.

While some gear can help detect non-RF devices, nothing beats a thorough physical inspection. Every single electrical plug, lighting socket, and electronic device should be examined. A deep TSCM bug sweep would include looking for what might be hidden behind or within walls using thermal imaging.

In addition to locating devices that may be powered off, a thorough physical inspection can discover vulnerabilities in three areas/systems within a room:

1. Audio video and video conferencing
2. Phone/data
3. Electrical (carrier current)

TSCM tools used during a sweep

Prior to digging into the TSCM tech itself, let's make clear one important step: assessing the vulnerability of a given area or room by taking some baseline readings.
Before determining if a signal or device is a potential threat or foreign to the target area, three baseline sweeps should be completed in the following areas of vulnerability:

1. Electrical commonalities (carrier current)
2. Video/microphones
   (VC, phone speakers, audio mics, etc.)
3. Phone and data lines

As for phone and data lines, a few provisos are in order: All lines not in use should be sealed off. And if the space is "temporary", such as a hotel room or a rented meeting room, hardline devices should be completely avoided.

The specific steps that follow these baseline sweeps depend on the location's topography and specific layout and size. Similarly, the TSCM tools we use vary depending on our needs.

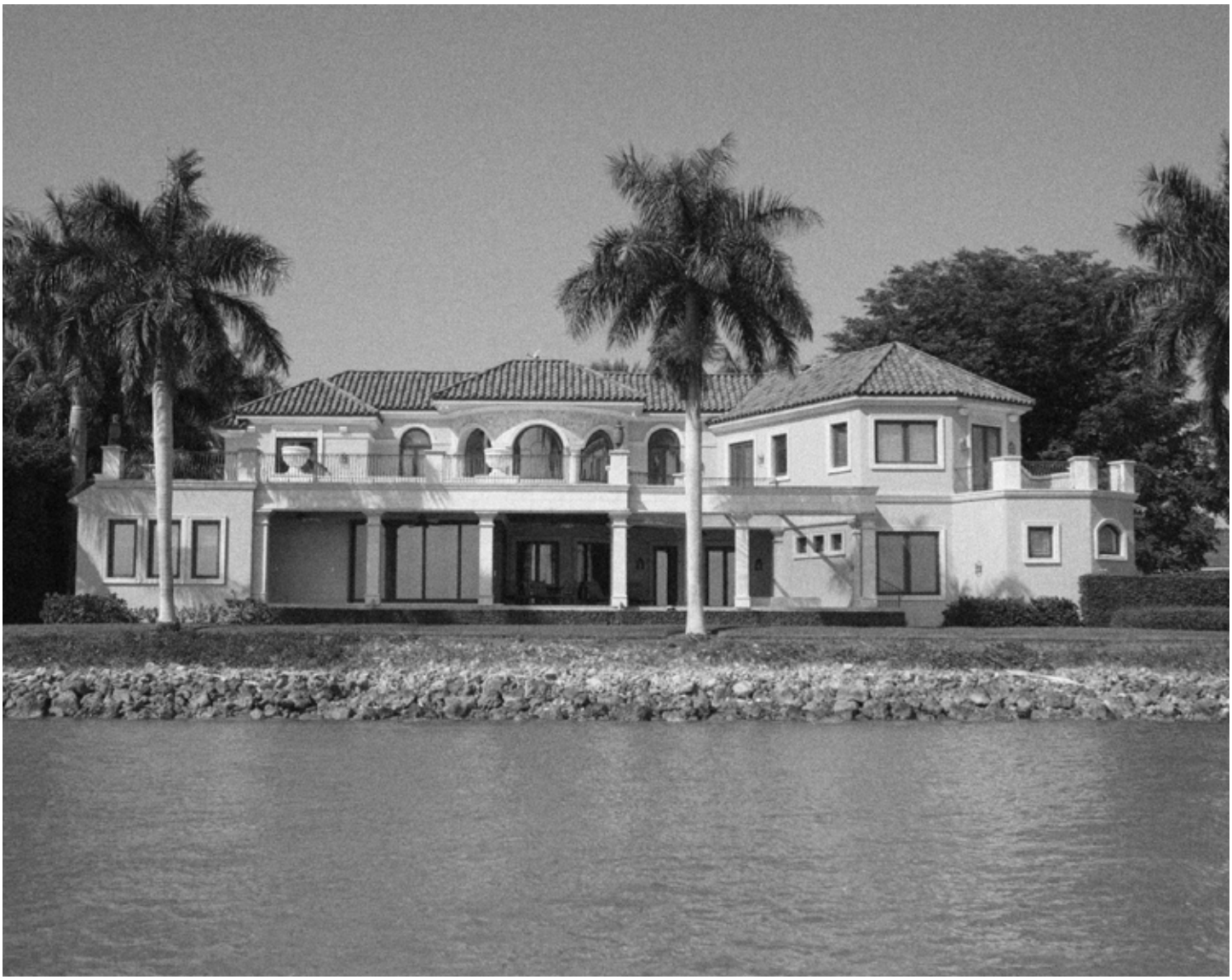
Once the baseline is established, we use the tools described below to complete TSCM bug sweeps.

Spectrum analyzers:

Probably one of the most important pieces of equipment, every reliable TSCM team needs is a decent spectrum analyzer. The spectrum analyzer allows the team conducting the sweep to "map" the area's frequencies and find any suspicious transmissions.

Teams can use multiple spectrum analyzers with different features (e.g., different frequencies and ranges covered, built-in video display, etc.).

REI's Oscor Green is the preferred industry standard and is, in our opinion the best spectrum analyzer available to the public.



Nonlinear junction detectors:

Once spectrograms of the transmitting frequencies are produced, nonlinear junction detectors help check for devices that don't necessarily use RF or that are turned off. These include hardwired devices tethered to computers, Dictaphones, cell phones, circuitry, transmitters, etc.
We like REI's Orion 2.4 HX Non-Linear Junction Detector for this work.

Broadband detector/receiver:

The broadband receiver is designed to detect and locate all major types of electronic surveillance devices including room, phone, body bugs, video transmitters, and tape recorders.

Broadband receivers are an essential tool for professional sweep teams, quickly and effectively detecting and locating transmitted signals.

Once again, we rely on REI for this tool and prefer the CPM-700 Broadband Detector.

Telephone line analyzers:

While phone lines grow less common in households, they're still present in many hotel rooms around the globe. Especially digital ones. Devices such as REI's TALAN allow agents to check phone systems, including Voice over Internet Protocols (VoIPs).

Telephone line analyzers tend to be minimally effective for temporary spaces, since full schematics and physical hardline access are required. This is yet another good reason to avoid using hardline devices while on the road.

Microphone detectors:

Devices such as the SDMS Bloodhound can detect audio signals coming from microphones. We have not used these yet at the client site or in the field, as we rely on broadband or non-linear junction detectors, which also locate any microphone in the room.

Amplifiers:

Amplifiers can identify audio devices attached to wiring (computer cables, wires, AC power, etc.)

This type of device requires wiring diagrams/schematic and physical access as well. REI's CMA-100 Countermeasures Amplifier is a good option here.

UV lights and pens:

Ultraviolet lights and pens assist the physical search of a location. UV pens and lights are a great way to mark objects (e.g., screws and wall fixtures) to check for a breach later. We most often use the REI UV Pen and the REI UV Inspection Light.

Digital cameras, borescopes and video scopes:

Borescopes can be used individually for a specific use, or can be used as a kit to cover a wide variety of situations. The borescope is a fine optical instrument for seeing inside small areas, and is used in many applications including security and manufacturing inspections. It can be utilized in many environments where direct viewing is impossible.

The REI Precision Borescope & Video Monitor and the REI Video Pole Camera – VPC 2.0 have proven track records.

A cheaper alternative is a simple snake inspection camera such as the Ryobi Phone Works, which turns your smart phone into a decent borescope.

Thermal imagers/thermal imaging cams:

Thermal imaging cameras (TICs) find heat signatures of anything left powered on or "hot" from receiving a signal (remotely, electronically, etc.). These can be invaluable when conducting a physical search of an area to discover items behind a wall that are warm from heat (conduit, wires, etc.) and otherwise invisible to the naked eye.

FLIR is the industry leader in thermal imaging for the private sector and the government, and they make some good stuff including the FLIR C2 Camera and the FLIR One (add-on for smart phone). The Seek Compact XR is also a good alternative.

Cable testers:

Wire and cable locators are designed to trace and locate all types of inside and outside wiring and piping.

These devices (similar to the TALAN telephone line analyzer) send out a signal and use precise measurements to time the out and back of the signal to figure out where a device or additional connector (resistance) is placed on the line. The limiting factor is that most lines have many connectors, Ys, etcetera, and schematics are imperative for these types of sweeps.

The RFX 1500 & 2500 are two excellent options.

The RFX-1500 transmitter can be connected to live AC power (up to 220VAC) to allow tracing of live electrical circuits, whether they're in the house or buried outdoors. When connected to working telephone lines, the RFX-1500 Transmitter is totally transparent. It is not audible on phone lines and does not disrupt fax, modem, or voice communications. The RFX-1500 can even transmit into the ground, so you can trace gas and water pipes buried outside.

The RFX-1500/2500 is a sophisticated radio transmitter and receiver operating at 455khz. As it is radio based, the RFX-1500/2500 system has a detection range of more than 10 feet indoors, and can detect buried wiring and cables down to three feet or more outdoors. The system uses a "Null" mode antenna, which, when pointed at the hidden wire, is undetectable on the phone lines you are checking. This allows you to pinpoint the exact location of a hidden wire or cable to within the width of the antenna.

The future of TSCM for corporate executive protection

There are primarily two types of corporate espionage operators: state actors and espionage-as-a-service providers, who are freelancers willing to sell to whomever wants to buy.

State actors are and will be extremely difficult to neutralize as they have the money, resources and authority in their own country to gain access to any location they want.

It is easier (but still not easy) to neutralize attempts by espionage-as-a-service providers: they are usually independent with less funds and fewer resources than state actors.

We expect both state actors and espionage-as-a-service providers to increase activities in the coming years.

Corporate espionage is, unfortunately, a growing business. On its own, it accounted for an estimated $300 million in theft in the US in 2013. Pooled together with cybercrime, which includes far more methods than TSCM sweeps are designed to expose, the costs of espionage and cybercrimes are growing exponentially: a recent report by Juniper estimates that cybercrime, including corporate espionage, will cost businesses worldwide a whopping $2 trillion by 2019.

Not only is the financial impact of corporate espionage growing, but the costs of carrying it out are falling. As mentioned above, surveillance devices continue to get smaller and cheaper, so they will only continue to be more and more accessible to anyone who wants to steal data.

For these reasons alone, we believe corporations will increase their focus on TSCM. But we also believe they will step up anti-surveillance activities for another reason: to mitigate risks to principals as part of executive protection programs.

Five years ago TSCM bug sweeps were seldom seen in corporate EP. Today, they are common practice with our larger clients. In the coming years, we predict that more and more clients will require ongoing and ad hoc TSCM services in conjunction with other corporate executive protection services, and that TSCM will be a very critical piece of the security umbrella that we provide to our clients.

Article by

David Falco
Program Specialist

David Falco works as a Program Specialist at AS Solution North America, Inc.

Sean Paul Schureimen
Special Projects Manager

Sean Paul Schureimen works as a Special Projects Manager at AS Solution North America, Inc.

Drones and corporate security: What's new in 2016

By Sonny Schürer and Sen Paul Schuriemen

Drone technology began migrating from purely military use into other applications, including security, about five years ago. Here at the end of 2016, better technology and lower prices have brought excellent drones within reach of anyone with a few hundred dollars.

We've experienced several firsthand ourselves. In Xian, China, where the photo below is from, a drone suddenly appeared over a large public/private event and no one – least of all the local police – seemed to have the slightest idea what to do about it.

Also called "unmanned aerial vehicles" (UAVs), drones have become a significant part of how we perceive war and security in the 21st century. Their military benefits are obvious. They are unmanned and can be controlled remotely – even from thousands of miles away – so they place no one on your side at risk even when sent to hostile areas. They carry everything from cameras to missiles and can perform a wide variety of combat and surveillance operations. And while military-grade drones are not exactly cheap, they are far less expensive to purchase and operate than the manned versions they replace.

As we'll see, their civilian cousins present real challenges – as well as opportunities – to security professionals worldwide. We'll get to the updates in a bit. First, let's take a quick look at how UAVs have developed into the powerful tools they are today.

A BRIEF HISTORY OF DRONES

Unmanned aerial vehicles have been around in one form or another for a long time. Austrians attacked Venice using unmanned balloons loaded with explosives back in 1849. During the First World War radio-controlled aerial devices were deployed against zeppelins, and the Hewitt-Sperry Automatic Airplane saw service as a form of aerial torpedo against enemy planes.
For decades, UAVs were not much more than rudimentary explosive-delivery devices aimed at hostile targets. World War Two saw the deployment of radio planes for training anti-aircraft gunners, and aerial torpedoes were still being used without much success. From the 1960s to the 1980s, military drones were primarily used for surveillance.

In the 1990s, technological developments and miniaturization ushered in a new era for drones. And when the US military developed its system of global positioning satellites (GPS), drones as we now know them became possible. Since GPS became fully operational in 1995, things have moved quickly. Another type of drone also emerged: Unmanned Ground Vehicles (UGVs). Since then, both aerial and ground drones have been used extensively in military conflicts all around the globe. But as technology progresses, engineering companies have come to realize that drones could be used for much more than warfare.

CIVIL AND DOMESTIC DRONES

With drones proving themselves so effective on the battlefield, using them for non-military purposes became not only a tangible possibility, but an exciting one. Civil and domestic drones have been talked about since the early 2000s and are now rapidly appearing in the skies all around the world. Here 's a brief list of how unmanned vehicles are currently being used, or will soon be used:

- **Farming and agriculture:** Aerial surveys, crop-dusting and daily mapping. Using drones, farmers can selectively spray pesticides on plants that need it rather than spraying an entire field, reducing damage to the environment and cutting costs, too. Infrared cameras can detect both healthy plants as well as those suffering from fungal infections.
- **Sports and other events:** Why use expensive helicopters when you can strap a camera to a $2000 drone and capture live aerial HD shots of any event? The tech has already been used at the Olympics and the World Cup, and there's no doubt it's only the beginning. Coaches are also using them in order to improve their team's strategy–whether on the field or skiing down a hill.
- **Delivery:** Domino's made some waves in 2013 when the company released footage of a small drone delivering a pizza. See a short video here. The company behind Domino's drone play is Flirtey, who just announced plans to deliver pizzas in New Zealand – this time as more than a publicity stunt. Amazon is also working on its own fleet of service drones. The idea is that small quadcopters could bring packages to your doorstep much quicker than any other mode of transportation. And the idea doesn't stop with food or household goods. A startup called Matternet has built drones to distribute medicine in remote areas of the world, and recently announced plans to partner with Mercedes-Benz to provide "A new end-to-end system for last-mile delivery featuring a fully-automated cargo management system and integrated Matternet M2 drones." Zipnet has pioneered medical deliveries in Rwanda, and has recently announced plans to begin parachuting meds and blood from drones into remote areas in the U.S.
- **Photography and reconnaissance:** The sky is (literally) the limit when it comes to using UAVs for non-military recon and data gathering. NASA is already using drones to test the makeup of the ozone. Oil and gas companies want to use them to detect faulty pipelines in need of maintenance. In Italy, drones already spy on illegal waste dumping. Firefighters will use them to put out wildfires more effectively, as recently demonstrated by Lockheed Martin's "optionally-piloted helicopter" experiments. Indonesian scientists have been using them to keep track of endangered orangutans. Artists are also getting in on the fun – check out this fascinating video filmed in Beijing.

DRONES AND CORPORATE SECURITY

With drones now being used in such a wide array of fields, there's no doubt that the security sector will soon also benefit from them.

In 2012, Japanese company Secom announced the world's first autonomous drone for private security. Since then, dozens of other security firms have joined the fray, competing to offer their clients the best high-tech protection possible.

A Silicon Valley startup recently announced plans to couple drones with on the ground sensors to heighten residential security.

Here are a few examples of how drones are being used to change the face of modern security:

- **Airport and port security:** In the last five months of 2015 alone, the FAA reported nearly 600 incidents where drones got too close to airplanes. Abu Dhabi and Gatwick were the first in line to deploy drones to ensure on-site safety. Dubai's Civil Aviation Authority is currently testing a "drone hunter" that uses thermal and infrared imaging to find drones that could get in the way (not to mention in the engines) of planes, then follow them back to their launch points.
- **Event protection:** What used to be thought of as future technology is already part of the past. The Sochi Olympics, the 2014 World Cup in Brazil and the 2016 Rio Olympics all used drones to secure the events. Providing 24-hour air surveillance over high-traffic areas, the unmanned vehicles were used to track crowds and report any sign of disturbance to local law enforcement officers and security companies. The goal of using aerial drones during crowded events is to stifle unrest before it even becomes an issue. While recording events from high above and gathering vast amounts of data, the drones regularly beam back information to ground level, helping secure locations much faster than a regular camera would have.
- **Crowd control:** A South Africa-based firm called Desert Wolf announced its Skunk Riot Control Copter in 2014. The goal? "Control unruly crowds without endangering the lives of the protestors or the security staff." The system carries four high-capacity gun barrels loaded with up to 4,000 paintballs, pepper spray balls and solid plastic balls. Its device has already been sold to mining companies and security firms in South Africa and abroad. See more here.
- **Remote surveillance:** Ground cameras, no matter how high-tech, are still limited by their design. If an intruder steps out of a camera's field of vision, the camera essentially becomes useless. This won't be the case with airborne cameras, at least according to Secom. They've recently unveiled a quadrotor that can be launched in case of a break-in and record crucial footage, covering areas that are usually out of reach. The automaton is fully capable of tracking moving subjects thanks to its laser sensors. Once technology improves, surveillance drones will likely patrol at-risk areas 24 hours a day, acting both as a deterrent and as a set-and-forget mechanism against break-ins.
- **Remote reconnaissance and law enforcement:** Law enforcement officials are using more drones than ever before. Northern California's Alameda County Sherriff's office is a firm believer in their

efficacy, and has deployed them more than 70 times in the last year for everything from incident management to stakeouts.

- **Personal security:** We're not quite there yet – and the legislation surrounding it are barely even drafted – but personal security drones might also be used to disable intruders or criminals once an alarm has been triggered. At the 2014 South By Southwest festival, a company called Chaotic Moon Studios demonstrated one of those drones, equipped with a stun gun. The "pilot" gleefully used his cellphone to control the UAV, tagging one of the company's interns as "hostile" and stunning him with 80,000 volts of electricity. Sunflower Labs, a Swiss startup, will soon sell a home security system that integrates on-ground sensors with drones – and allow you to monitor all the action from your smartphone.

A DANGER TO BOTH EXECUTIVES AND CORPORATIONS

The security industry has begun taking drones into account when it comes to providing protection. The threats are too credible to be ignored: drones are flying over prison walls, nuclear power plants, stadiums, public events, celebrity homes, corporate campuses – anywhere.

Some of the most tangible threats are:

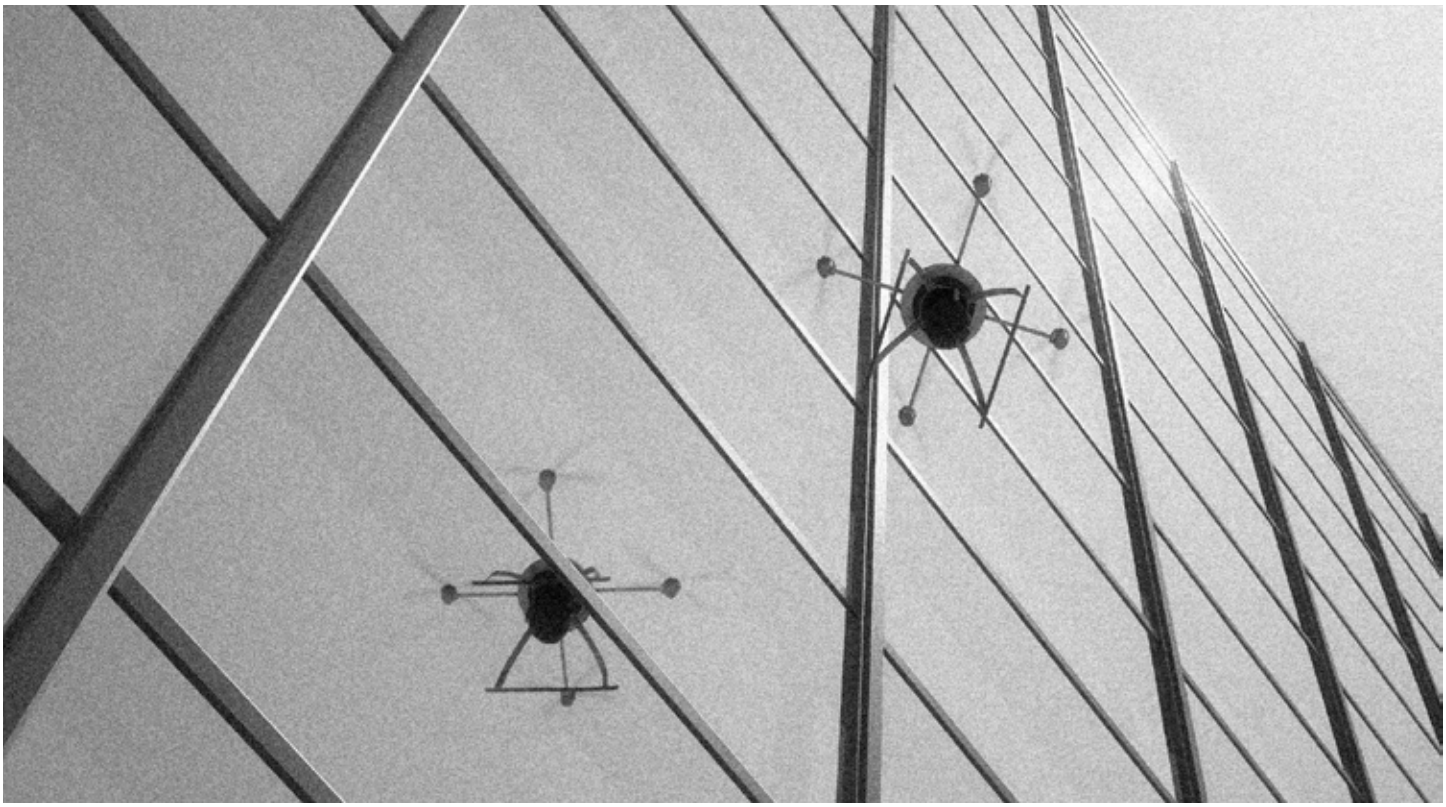
- **Celebrities and executives can be spied on from the air,** which means that their activities and movements (e.g. a target's car) can be tracked in real-time. This is not only a huge security risk, but also a breach of privacy.
- **Sensitive locations (clients' residences, private properties, offices, stadiums, public venues, etc…) can be scouted** by drones and intelligence can be gathered, which could reveal weaknesses in the security arrangement and leave a site vulnerable to attacks.
- **Public locations are also at risk** in a more direct manner: drones could crash into crowds, unload explosives, or deliver weapons that could then be used by a "receiver" on the ground.
- When it comes to **corporate and industrial espionage**, nefarious entities may use to drones to capture footage and recordings, since many UAVs are equipped with HD cameras, infrared cameras, or long-range microphones.
- The latest spy drones are capable of **hacking into Wi-Fi networks** (for example, by landing on a company's roof) and sniffing information. There have been reports of amateur drones being able to crack Wi-Fi-encryption and even intercept phone calls and text messages.
- **Stolen or "repurposed" drones**: As storage solutions expand, more and more data can be stored on the drones themselves: video footage, audio footage, passwords, and more. What happens if a corporation or other organization decides to use UAVs, and then loses one of them? Does the drone carry sensitive data? How secure is that data? If the drone gets snatched by hostiles, what could they extract from it? When it comes to security, drones used by corporations become, at this point, not unlike laptops or mobile devices. Both the physical and cyber- security of the device must be taken into account, and response plans should be put into place in case anything happens to it.
- **Insider threats**: Similarly, how do corporations protect themselves from rogue employees acting as corporate spies who illicitly capture and share data collected by corporate drones?

COUNTERMEASURES AND PROTECTION

Until recently, many of the tactics employed by security pros and governments were passive. For example, detecting and identifying drones with microphones and radars allowed security services to relocate their clients, change their security setup, or alert a company before any damage could be done.

Thankfully, and unsurprisingly, the anti-drone industry is booming, and more and more countermeasures are now available. Let's look at a few:

- **Detection and monitoring**: Those two measures are the foundations upon which anti-drone technology is built. After all, if you can't locate a drone, you can't protect yourself from it.



Detection relies on small radars, cameras, and devices installed on residences or around specific perimeters. Once a drone is detected, the security system can warn the security team via email, SMS, sounding an alarm, or in some cases alerting local law enforcement. One of the most popular detection tools is the Drone Shield, but there are many more out there.

- **Active responses**: Legislation permitting, hunter drones allow companies to "fight fire with fire". These UAV models—such as the Rapere quadcopter or the Interceptor MP200—are equipped with various means to take down an enemy drone. The Rapere navigates via cameras and can entangle an enemy drone's rotors with wires. The Interceptor uses a net to force its target to crash. There is also a third model in development, a "kamikaze" drone developed by Malou Tech, which would simply slam into another UAV to bring it down. Ballistic technology also exists to shoot drones down—but that type of equipment is mostly used by governments so far.
- **Geo-fencing and no-fly zones**: Many geo-fencing tools exist, which send signals to create aerial "barriers" that drones are not allowed to fly over. Unfortunately, fencing may only work with a limited number of drone hardware/software, and can be bypassed by dedicated drone operators. No-fly zones are more effective, as they combine both geo-fencing and more active measures (e.g. nets, ballistics) to both locate and bring down any intruder.
- **Jamming**: Radio frequency jamming remains illegal in some countries (the U.S. in particular) but is still commonly used for lack of better options. While geo-fencing simply sends a message to drones telling them not to fly over a particular location, jamming actively aims to disrupt or interrupt a drone's signals, causing the operator to lose control of the UAV and rendering it useless.

ANTI-DRONE TECHNOLOGY: WHERE DO WE STAND?

Drone neutralization (disabling or destroying the device) is a very delicate topic, and case law in the U.S. and most European countries limits the ability to use drone neutralization capabilities.

Why? Well, for one thing at least in the U.S, the FAA considers drones to be like other aircraft when it comes to blasting them out of the sky: shooting them down could put the public at risk. Liability for the damages a falling drone might cause rests on the neutralizing party, not the drone owner.

Additionally, whether you think the drone is bothersome or not, it is still the property of the remote operator. Lower courts have ruled both for and against the "drone killers" who see drones as trespassers and blow them out of the sky with shotguns. Law enforcement agencies have limited ability to enforce local drone regulation—whether by perception, limited resources, or a lack of clear guidance.

As of now, early warning systems are the best defense for most organizations…

Early warning systems all have pros and cons, primarily relating to the operational environment. The three primary ways of detecting drones are sight (cameras), sound (mics), and radio frequencies.

Detecting drones with RF is more difficult in the urban areas where most people are. There are more birds and radar ghosts due to signal bounce--ultimately leading to false reporting. RF works better in rural areas as it has greater reach, and most systems provide direction finding capabilities and utilize cameras for rapid visual identification. Sound works better in urban areas, but it's highly recommend that sound systems be complemented with a camera sub-system.
In short, there's no "one size fits all" solution when it comes to warning systems. Organizations need to weigh the pros and cons of each solution and consider their location(s) in order to deploy the most effective defense.

…but there is one general fix that will work for many corporations and estates: heliports

As we mentioned above, the FAA recently changed its rulings, simplifying where "recreational" drones may fly. At first glance, it might seem that small drones can fly pretty much anywhere in the country, as long as they stay below 400 feet, stay within visual line of site and keep away from airports. Take a closer look at the rules, however, and you'll notice another important exception that rarely gets mentioned along with airports: heliports.

Drones are not allowed to fly within 2 nautical miles (2.3 miles/3.7 km) of heliports with published instrument flight procedures.

This doesn't mean that you can paint an "H" on your lawn and claim you're a heliport. It does mean that corporations and estates, for a relatively small investment, can ensure both that helicopters can land on the property – and that drones can get nowhere near it.

US DRONE LEGISLATION IN 2016

Governments around the world are hustling to keep up with the proliferation of low-cost drones that can do more and more – and are the cause of increasing concern for everything from personal privacy to civil aviation, event security and prison perimeters.
Here are the key legislative developments in the US:

- **As of January 2016, ALL drones – also the small recreational ones – had to be registered in the U.S. through a simple online registration process**
- **New FAA ruling:** In a long-awaited ruling that was announced in June 2016, the United States' Federal Aviation Authority made clear that recreational drone pilots can pretty much continue flying as previously. Life just got simpler for US companies and for-profit entities, however. Whereas they previously needed FAA permission to operate, they now just have to adhere to a set of new guidelines. Key among these are that drone operators for devices weighing less than 25 kg (55 lbs.) must pass a drone certification exam and complete a UAV ground operator's course; drones must stay within the line of sight and may not fly at night, over 100 miles per hour, or higher than 400 feet from the ground. Should a business wish to bypass some of these guidelines, they must request a waiver/permission from the government. Importantly, this new ruling does not apply to autonomous flight, so companies like Amazon can't automate deliveries just yet, and security companies can't have

drones "patrolling" areas without an operator/ pilot on duty.

- **No-fly zones are becoming more common,** and while drone software may not take regulations into account, the pilots have to. This is taken care of thanks to NOTAMs (Notice to Airmen) and local charts (knowledge gained from courses and test prep.)

RULES AND LEGISLATIONS ARE STILL SOMEWHAT CHAOTIC IN EUROPE

The European Aviation Safety Agency (EASA) has announced that they're working on new rules and amending previous ones in 2016 and 2017, but there's nothing too concrete quite yet.

As in the past, pan-European legislation remains weak, and drone legislation is still very much a country-by-country affair.

WHAT'S NEXT?

We expect the future of drone-related security to be impacted by several factors.
They'll become more quiet as motors improve and rotor blade technology gets better. This is great if you're the one deploying the drone, but not great if you're defending against them.

They'll get smarter, too. Look for even better autonomous operation technology in commercial drone systems as they incorporate video manipulation technologies and algorithms for facial recognition, ground mapping, change detection and predictive insights.

And of course, all of this will of course be combined with what we come to expect in almost every other area where tech meets transistors: better, faster, cheaper. Expect further improvements on everything we mentioned above – better performance, cams, mics and storage capabilities – and all at a lower price.

Article by

Sean Paul Schuriemen
Special Projects Manager

Sean Paul Schuriemen works as a Special Projects Manager at AS Solution North America, Inc.

Sonny Schürer
Senior Vice President

Sonny Schürer, Senior Vice President, has helped manage AS Solution since its founding in 2003. A leading member of The Danish Trade Organization for Safety and Security and an active member of ASIS, Sonny has extensive experience in executive protection, event security, investigations and maritime security.
As a member of AS Solution's management team, Sonny heads the company's European operations from its Copenhagen-based European headquarters. Sonny serves on the board of Parsifal Services, AS Solution's partner in corporate investigative services, and has also overseen the development and growth of AS Solution's anti-piracy services, Scandinavia's largest maritime security service with operations worldwide

www.assolution.com

AS Solution North America, Inc.
14645 NE Bel-Red Road, Suite 103,
Bellevue, WA 98007, USA
+1 (425) 296-3017
info@assolution.com

AS Solution A/S International
Marienlundvej 46 E
2730 Herlev, Denmark
+45 3525 1010
info@assolution.com