News • Reviews • Opinions • Intel • Exclusives

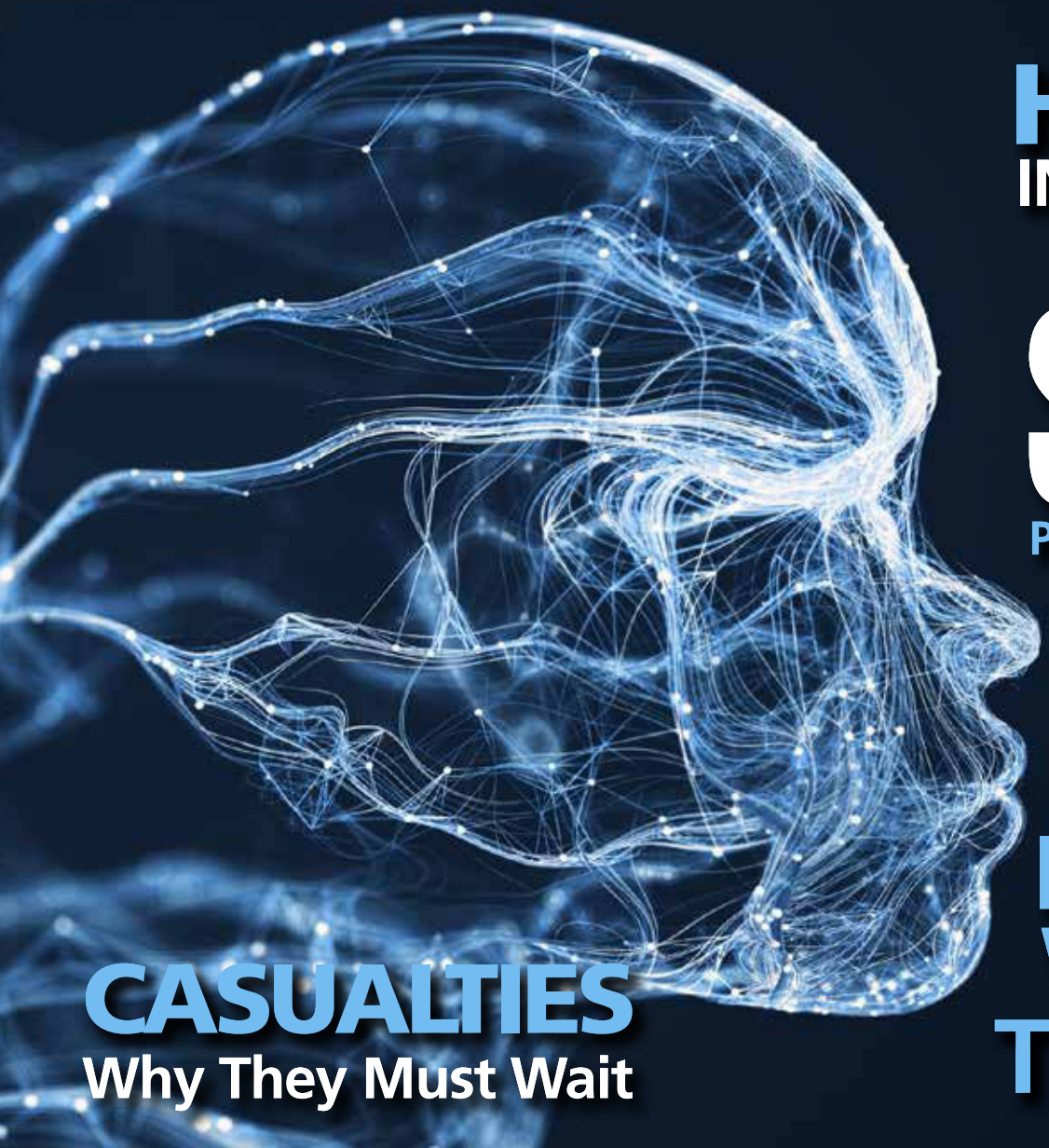
The Circuit

For Security And Protection Specialists

ISSUE 60

DEEPFAKE

Welcome to the Age of Uncertainty



HUMAN INTELLIGENCE

STOP PROCRASTINATING

CASUALTIES
Why They Must Wait

KNOW WHEN TO QUIT

MEDICAL CONSIDERATIONS | CYBER SKILLS SHORTAGE | HOSTILE SURVEILLANCE

By Orlando Wilson

INTELLIGENCE GATHERING: PART 1

HUMAN INTELLIGENCE

Intelligence is the information we obtain on a target or threat in order to locate them, gain information on their operations and to predict their future actions.

Accurate intelligence is not only essential in all security and counter-insurgency operations but also in the corporate world where companies need to know what their competitors are developing and planning.

An easy way to illustrate the importance of intelligence and counterintelligence is this simple example; randomly pick someone online or someone you know and say to yourself "I'm going to kill this person". They are defenseless as they do not even know you are targeting them, if they even know you exist. You can start profiling the target and making your plans for the assassination while they are completely oblivious.

Intelligence and counterintelligence are two sides of the same coin. You cannot expect to be able to source intelligence unless you are alert for others targeting you. Egos and arrogance get people killed. Those who think they know everything and are untouchable are usually ›

the easiest to bring crashing down. Especially if those targeting them are professional, ruthless and unconventional.

There are various means of gathering intelligence but no matter where the information is coming from it needs to be verified and crosschecked to ensure its accuracy and that it is not disinformation provided intentionally. If information and leads are being provided from reliable sources, then every little detail needs to be taken into consideration. One single fact, however apparently insignificant, can open the doors that lead you to your target.

Intelligence gathering can roughly be divided into three areas

- Surveillance: This can include physically following a target, watching the target's home or office, hacking telephones and computers to intercept messages, monitor web traffic and movements, etc.
- Research and Analysis: Useful information can be found from online news reports, photos, social media, newspapers, radio and trade magazines, etc.
- Informants and Espionage: The placing or recruiting of agents and informants with access to the target and their organization can be difficult, time-consuming and dangerous for all involved, but can give you access to the target's plans, documents, networks and the ability to influence or misdirect their activities and goals.

Some of the basic tasks of intelligence operations are to

- Locate criminal and hostile targets.
- Identify criminal and hostile activities.
- Identify the structure, plans and goals of an organization or corporation
- Identify and penetrate an organization or corporation
- Obtain information about an area and its population.

The Intelligence Cycle

The intelligence Cycle is a set of simple bullet points that are used by intelligence agencies to effectively structure their operations.

- Direction: You need to know the objectives and goals for every operation be it short or long term.
- Collection: You need to have a plan for how you will collect the required information; open-source, informants, surveillance, hacking, etc.
- Processing: Once your collection operation starts to deliver information it needs to be checked for accuracy and relevance.
- Analysis: When you have accurate and reliable information or leads you need to assess what it actually identifies and how the information can be used.
- Dissemination: How will you use the information and who will be informed of your findings.
- Feedback: Once your reports have been distributed you will need to wait to see what feedback is given from your clients or the like.
- Be prepared to defend your finding especially if they are controversial or go against what the client expected to be discovered.

If information and leads are being provided from reliable sources, then every little detail needs to be taken into consideration. One single fact, however apparently insignificant, can open the doors that lead you to your target.

The type of information that will be of use to you will depend on the type of operations that you are conducting. You need to clearly define why you are running your operation and what the required end-results are. Only then you can collate the relevant information required to achieve your goals and start to dismiss false leads, disinformation and irrelevant information.

SECRECY

Nothing is as important professionally or personally

as secrecy. All your security, operational or business plans and preparations will be worthless if the bad guys know them. If you cannot protect yourself there is no way you can protect others or work in any potential hostile environments.

Good personal and operational security begins with a clear understanding of what kind of information the criminals or terrorists will be trying to learn about you, your family, business or operations.

Governments must keep secret their diplomatic alliances, secret treaties and military strategies, etc. Although a government may suffer a great loss because of poor security, it is hard to imagine today a situation where a nation's defenses could be completely overwhelmed by a single security leak. However, that is not the case with a small-scale operation.

A company might be ruined as the result of a single security leak. A family might be ambushed and

kidnapped because a single piece of information was found out by the criminals, such as home address, security procedures, routes a child takes to school or their travel itinerary.

Things that should be kept secret and restricted

- Addresses and identity of individual employees, their families or close friends.
- Security plans and methods of operation.
- Transportation capabilities.
- Source's supplies.
- Available backup.
- Location of hideouts, safe houses, etc.
- Codes, signals, passwords, and lines of communications.

Good personal security is a must, good team security begins with good personal security. If a person is living or traveling under their own name, they must keep information about their occupation and activities limited to those who need to know only. There is no one more completely defenseless than the individual whose personal security has been compromised.

Personal security is a 24/7 job, to some, it comes almost instinctively but others can find it very hard to develop. An individual's habits and personality will have a considerable effect on their attitude towards personal security. Some people will just never get it and it can be a liability. Such people should not be allowed access to sensitive information or taken to high-risk locations.

The Basic Principals of Security

- Deception: Deception is essential to the success of all security or investigative operations; always have a cover story and be ready with credible explanations as to who you are, what you're doing and why you are doing it.
- Avoiding attention: One way for any individual or organization to seriously compromise their security is to attract attention. Always keep a low profile and remember that if people don't know what you are doing, they cannot counteract you.
- Self-discipline: Everyone must abide by the rules. If anyone disregards the rules of the security program, they could jeopardize the personal security of all involved.
- The program: A security program must be outlined and made clear to all personnel. Everyone must be briefed, trained and willing to work within the program.
- Continual inspection: The biggest thieves are usually those trusted with the largest responsibilities- they have access to assets or

information worth stealing. The conscientious person with the flawless record can easily deviate by their own accord or with the pressure of a little blackmail. People change and so does the importance they place on their own security; given time people will relax. This is why there is a need for everyone to be constantly inspected.

- Fluid change: This is best illustrated by frequent changes of meeting places, routes and operational procedures to keep the criminals guessing. This principle is necessary because, if given enough time, professional criminals can crack the security of any organization. So, old security measures must be constantly and fluidly replaced and updated.
- Action: If someone is not capable of obeying the security program they will need to be disciplined, they should not be trusted or only trusted with information or tasks that will not jeopardize anyone else.

> If you detect a sympathizer within your operation what are you going to do, fire them or feed them false information?

You will not have a security program by following only one or more of these principles, all must be followed, and you must remain alert 24/7.

Basic Counterintelligence

Basic counterintelligence increases the security of all operations and the chances of surprise in offensive operations. Your security program, even if it is for yourself, should be developed to prevent the leaking of information, or situations where criminals can extract information from you or your business.

You could initially be trying to find criminal sympathizers already within your operation; this could be your locally recruited secretary or attorney. If you detect a sympathizer within your operation what are you going to do, fire them or feed them false information? You should also consider why they sympathize with the criminals: is it for money or are they being threatened. Counterintelligence can be broken down in the two practices, denial and detection operations.

Basic denial operations may include

- Thoroughly brief everyone on how the criminals will try to get information on you, your personnel and your operation.
- Place a high emphasis on the

> To gain information on you. If they cannot get any information on you it makes their job targeting you a lot harder.

security of information. People must understand the need to keep things on a "need to know" basis and not to talk about confidential topics in public.

- Make sure all papers, old computers and communication devices, etc. are properly disposed of.
- Employees should be briefed on the gyms, cafés, bars, clubs and other venues that are safe to frequent socially and those that are not.

Basic detection operations may include

- Background investigations must be done on all employees, especially locals who have access to confidential information.
- Make maximum use of CCTV, covert cameras for detection and overt cameras for deterrence.
- Monitor your staff's communications including e-mail, web activity and telephone calls, , etc.
- Put any staff members acting suspiciously or who seem to be living beyond their means under investigation and surveillance.

These are just some basic considerations, but they can turn your security program into something that would make it extremely difficult for the bad guys to gain information on you. If they cannot get any information on you it makes their job targeting you a lot harder. Hopefully, so hard they'll go and do what we want them to do, find an easier target of which there are plenty.

Orlando Wilson has worked in the security industry internationally for over 25 years. He has become accustomed to the types of complications that can occur, when dealing with international law enforcement agencies, organized criminal and Mafia groups. He is the chief consultant for Risks Inc. and based in Miami but spends much of his time traveling and providing a wide range of kidnapping prevention and tactical training services to private and government clients.