Collection Systems: HUMINT, MASINT and OSINT

Rachael Riggs

National American University

Collection Systems: HUMINT, MASINT and OSINT

HUMINT, MASINT, and OSINT are three intelligence collection disciplines that can be utilized in support of HIDTA to provide much-needed intelligence.

## HUMINT

HUMINT, more widely known as "espionage," refers to human intelligence, which uses human sources and can be done overtly or covertly. HUMINT can effectively support HIDTA's mission. Human sources typically provide the best method to deal with criminal activity and gain knowledge of their plans and intentions. The main idea behind HUMINT is one person interacting with another to gain information. These sources learn and utilize special skills; most have a specialized tradecraft. Human sources covertly interrogate without the other person noticing they are being probed for information. Further information and the tradecrafts accompanying this intelligence discipline are explained as follows.

- **Clandestine Collection (espionage):** Clandestine collection is an intelligence collection that is done covertly so as not to let the target know. This collection is done in an attempt to ensure plausible denial. In most circumstances, there would be catastrophic consequences if the source were revealed.

- **Counterespionage:** Activities intended to detect surveillance or espionage and, in return, administer activities designed to distract an enemy, sabotage his surveillance, and collect or falsify his incoming information.

- **Overt Collection:** The act of obtaining information through legal and open measures. Both sides typically are aware of this type of collection.

- **Surreptitious Entry:** Entry that cannot be detected. No evidence is left behind. Human sources are skilled in entering and exiting establishments while leaving no trace of evidence behind.

- **Interrogation:** Typically begins as an interview. Interrogation is a way to systematically ask questions to obtain valuable information or evidence. Interrogators generally already know the evidence, so interrogation is designed to obtain a confession or a statement.



**MASINT**

Measures and Signals Intelligence (MASINT) is a technical branch of intelligence using advanced technology. It includes radar, nuclear, acoustic, chemical, and biological intelligence. It helps detect, track, and identify the signatures of a fixed or dynamic target source. MASINT is extremely useful in the military as well as law enforcement. This technology would help HIDTA stay organized and focused while providing the information needed to progress through investigations and obtain the knowledge needed to further their efforts. HIDTA could find uses with all of the following examples:
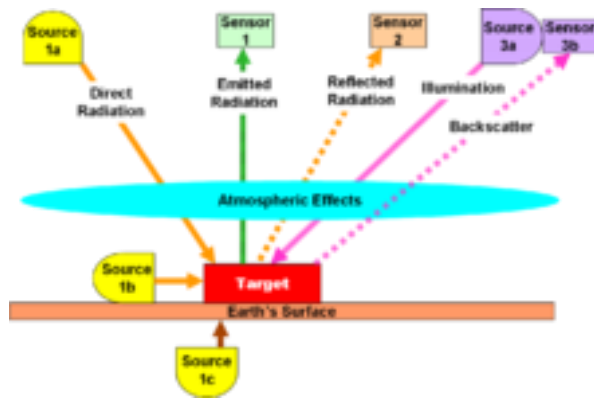
**Nuclear Radiation Detectors:** Nuclear Radiation Detectors are devices that can detect different forms of radiation including alpha, beta, gamma, and x-ray. One such brand is Radiation Alert, which S.E. International Inc. manufactures. They produce survey meters, radiation area monitors, radiation spectrum analyzers, software, and apps to detect radiation. The company offers eight handheld detectors, one of the digital ones being the monitor 200. This device measures alpha, betta, gamma, and Xray. It shows a digital display of the amount on the screen and beeps with each count detected. It can be customized per the needs of the user. It has Bluetooth and comes with the Observer BLE app. Items like this would benefit the military and businesses dealing with radiation. I could not find the price of this item. However, the information I found stated the price ranges of approximately $100-$1000 per handheld detector.



**Biometrics:**

**Facial Recognition:** Facial recognition is a way in which biometrics can scan your face and use the unique data against a database, which can then be used to help identify criminals at traffic

stops with handheld devices. Missing persons could be located by cameras set at stoplights

enabled with this function or any other equipped location, as well as from online posts, as many

websites have already begun incorporating this feature. Businesses could use it to clock their

employees in and out or allow the employee access to restricted areas. It could be used to track a

person under surveillance by using public cameras equipped with the ability and by using the

camera on cell phones to identify who is using it at the time in cases involving investigations. A

system like this costs about $500-$10,000 per door.
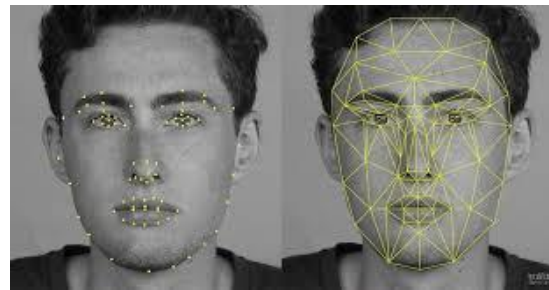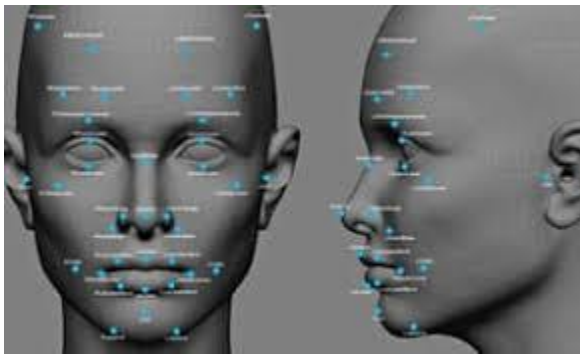


**Body Sensors:**

**Lie Detection:** Body sensors can pick up a person's physical aspects, including their heart rate,

breathing, posture, and gestures, and combined with the biometrics of eye movement and voice

changes, can provide evidence of deception; this could be beneficial in replacing the polygraph

or being used in combination. It could be used in courts in murder trials, which is already being

used at the border, helping Homeland Security to identify people who are untruthful or are a

potential risk and can identify them 60-80% of the time. Human sources can identify deception



54-60% of the time. (Daniels, 2018)

**STORMS (Sense Through Obstruction Remote Monitoring System):** This system is made by

VAWD Engineering out of Arizona and can see through the walls to identify targets on the other

side; a penetrating radar does this. This system uses Doppler and Micro Doppler signatures to

provide this information. It can detect every life form on the other side of the wall and follow

their movements. According to the website "STORMS has proven penetration performance on

the following: solid reinforced concrete, solid high-density adobe, reinforced & filled concrete

block, standard concrete block construction, partially tempest protected facilities, brick

construction, stucco construction, slump block construction, wood with/without drywall plastic,

fiberglass structures, mud-hut primitive construction, aircraft, cars, trucks, trailers, partial metal

buildings, desert, woodland, & jungle foliage." Storms collects its data and sends it back to the

user via a graphical user interface (GUI) and has a detection range of 300m. It can be a handheld

or vehicle mount. A system like this would be helpful to law enforcement for investigations,

SWAT deployment, and military operations. I could not find the pricing of this item.

**VAWD Applied Science & Technology Corporation**

# Sense Through Obstruction Remote Monitoring System (STORMS)

The **STORMS** system is a state of the art, all weather Micro-Doppler Radar system. **STORMS** is able to detect, track, and discriminate human and other life form targets hidden within building structures. The **STORMS** system uses patented technology and is the only device of its kind that can be operated from a long standoff range.

**Features**

- Designed for search/rescue/first response missions, law enforcement, and military operations for locating lost individuals, victims, or hostiles
- Platforms: Vehicle, Portable, and Handheld
- Penetration through single or multiple walls
- Simultaneous detection of stationary and moving life forms
- Custom 1D/2D graphic display
- Longer standoff ranges available

| DEVICE TYPE | HANDHELD | VEHICLE MOUNT |
|---|---|---|
| Penetrable surfaces | Cement block, Brick, Concrete, Adobe, Stucco, Drywall, Multiple Walls, Foliage | |
| Resolution | Less than 0.5 Meters | |
| Custom Display | 1D/2D View | |
| Radiation Safety | Radiation Safe | |
| Range of detection | Up to 100m | Up to 300m |
| Field of View | 32 Degrees | 12 Deg Azimuth-Elevation |
| Dimensions | 10.4"H x 11.8"W x 5.3"D | 18.6"H x 34.3"W (unit closed) |
| Weight | 7lbs. | 80lbs. |
| Power Supply | Rechargeable Battery | Vehicle Power (24V) |
| Run Time | 4 hours | N/A |

*(left vertical label: TECHNICAL SPECIFICATIONS)*

**VAWD Engineering**  1607 S. Pantano Rd. #405  Tucson, AZ 85710
520.760.9888 | corporate@vawdengineering.com

### OSINT

Open Source Intelligence (OSINT) refers to intelligence gathered via open source methods such as the web, journalism, news broadcast, radio, and any source that can be collected openly to the public. Numerous software and apps complement the searches to obtain information about a target's web presence and real-life presence. OSINT can be beneficial in business, law enforcement, and military operations. The benefits it would provide in helping HIDTA's mission include researching individuals of interest, providing information concerning

events or locations of interest, and developing knowledgeable information relating to a target.

These examples are just a few of what OSINT could be used. The list of uses and information

that could be found by using this source is extensive. Options concerning helping collect open-

source intelligence are noted below.

**Maltego**: Paterva is a company out of South Africa that began in 2007. The software
Maltego was introduced in 2008. This software analyzes the relationship of open source
information online with the real world. It can determine the relationship between:

- o   Names.
- o   Email addresses.
- o   Aliases.
- Groups of people (social networks).
- Companies.
- Organizations.
- Web sites.
- Internet infrastructure such as:
  - o   Domains.
  - o   DNS names.
  - o   Netblocks.
  - o   IP addresses.
- Affiliations.
- Documents and files

The software is used to assist in searches and investigations. The desktop is $999-$1999
with a renewal price of $499-$999

https://www.paterva.com/web7/about/company.php
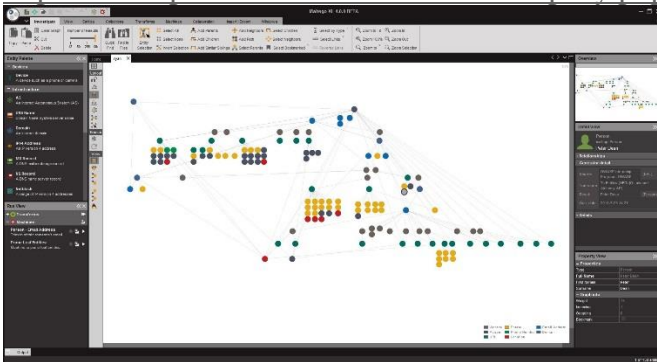


**Shodan:** www.shodan.io is "a search engine for the Internet of things." Find devices on
the internet and see who is using them. Results return physical addresses, IP addresses,
capabilities, HTML, and many other results. Reports can be created, as well as viewing
results on a well-delivered graphical map.

**Check Usernames: www.checkusernames.com** is a website that allows the search of usernames. The website searches over 150 sources to return information on the targeted username, brand, or any other name or search term of interest. Some sites it scans include Myspace, YouTube, Twitter, Houzz, Yelp, My Fitness Pal, Map My Run, Reverb Nation, and numerous others; this is a free search. After entering your search term and selecting the search button, all the websites that do not have that name associated with them will remain on the board and have "Available" next to each one. Those with the name used within their website go grey and say "Not available" or "error" if another problem is found with the username.

**Reverse Image Search:** Tin Eye, found online at www.tineye.com, is a website platform created in Canada that allows you to upload an image and perform a reverse image search. It will track where the image has appeared online by using patterns within the photo. The website offers API and browser extensions.

**Spiderfoot:** www.spiderfoot.net is a software that queries over 100 different sources to return data on a specified target, whether a name, email address, phone number, IP address, etc… The system can run on Windows or Linux and has an interactive GUI and a command Line, an open-source software available for download on their website.

References

Aaron J. Bell, L. U. (02-03). *ANALYSIS OF GPS SATELLITE ALLOCATION FOR THE*

    *UNITED STATES.* Aaron J. Bell.

Daniels, J. (2018). Lie-detecting computer kiosks equipped with artificial intelligence look like

    the future of border security. *CNBC*.


Clark, R. M. (2014). *Intelligence Collection.* SAGE Publishing, CQ PRESS.


    https://www.cnbc.com/2018/05/15/lie-detectors-with-artificial-intelligence-are-future-of-

border-security.html

    https://futurism.com/new-lie-detecting-robot-security-agent-could-help-secure-borders

    https://seintl.com/radiation-detectors/monitor200/

    https://www.tineye.com/technology

    https://www.paterva.com/web7/about/company.php

    https://www.vawdengineering.com/products.html

    https://www.spiderfoot.net/

    https://securitytrails.com/blog/top-20-intel-tools#one5-nmap