Surviving The Cyber Age

Chapter 2 - Sensors

Table of Contents

What can they see and what might they do

In this chapter, we explore the capabilities of threat actors in terms of what they can sense and acts they can undertake. We focus on the maximum capabilities and most malicious intents, but it's important to recognize that any particular threat actor other than a 1st tier nation state alliance is likely to have only a subset of the total capacity described here.

Cybernetic systems

Cybernetic systems, as defined in the 1948 book by Norbert Wiener, “Cybernetics: Or Control and Communication in the Animal and the Machine” consist of sensors, actuators, communications, and control, arranged so that sensed information is communicated to a control mechanism that determines actions to take and invokes those actions through communication with actuators. The results of actions and other events are then sensed by the sensors, and this forms a control loop that can adapt to situations over time.

The issues in this chapter are viewed from this perspective in order to organize presentation. Of course there are other ways to look at things, but hopefully this will inform more than unduly bias your thinking.

One more comment. Cybernetic systems operate with and within other cybernetic systems, from cells to body parts to living things of all sorts to groups to societies as a whole; and of course computers from parts to devices to networks to all of so-called cyberspace; and the combinations of all of these operating together form the world we live in. This holistic approach and recognition of the full spectrum of things in the world and how they interact is fundamental to recognizing and understanding the situation you are in and the things you can do to live within or change it, both on your own and working with others. The saying goes[1]:

No man is an island

Ignoring the issues of gender bias and human bias, it should be understood that we all live in the context of the world around us. The cybernetic system that is the universe of living thinking things and the parts that we are composed of is the context in which we live and must operate. Understanding its richness is foundational to living well and surviving bad situations we may induce or encounter. What we do effects and affects others and what others do effects and affects us.[2]

What are the observables?

You may notice that the term observables has been and will be used a lot. So what are the observables? The observables are the things that can be observed (seems like an obvious answer). That’s different from what is sensed or able to be sensed. The phrase:

> “A man hears what he wants to hear, and disregards the rest".[3]

comes to mind. The concept of confirmation bias and the anticipatory nature of cognition in humans (and likely other creatures) is far older than this expression. Cognition is a process by which, among other things, sensed phenomena is turned into observable phenomena that can be analyzed and understood in the context of the observer. For example, when we sense flashes of light (photons) that hit the back of our eyes, those flashes trigger signals sent from the retina through the optical nerve to the optic chiasm in the brain, which then processes it further (you can read all about it elsewhere).

The point is that what we observe is not what we sense. But it goes further. The way people understand what they sense is by anticipating what is to come and looking for what they

1 John Donne, “No man is an island”
2 Effect vs. Affrects: Causes produce Effects through Mechanisms. Influences produce Affect through Feelings
3 1969, Paul Simon, “The Boxer” (song)

expect. From focus of attention that directs us to look in a particular direction, to changing the configuration of the sensors by squinting, our cognitive systems limit what we are able to observe by limiting what we sense as well as limiting our interpretations of what we sense.

We hear what we want to hear, see what we want to see, feel what we want to feel, smell what we want to smell, and taste what we want to taste, and it changes with conditions – even if we don't like what we see, hear, feel, smell, or taste.

But while the observables may change with time, the sensory capabilities of specific sensory mechanisms are more readily and definitively characterized, even if there are individual variations and they also change over time and with conditions.

In understanding the limitations and capabilities of sensors, the intent is to recognize how they work and what can be gleaned from them. But it is important to recognize that all of the things that can be sensed and gleaned from sensors are not observed and probably can never be fully observed. At the same time, any potential observable might be realized in any specific instance.

What can be sensed?

In essence, there are lots of sensors of different sorts, each with limitations on what they can sense because of the physical nature of their mechanisms. For example, a modern digital camera in a typical cell phone can sense (according to one of their online specifications):

- 48MP Fusion: 24 mm, ƒ/1.78 aperture, optical image stabilization
- Also enables 12MP 2x Telephoto: 48 mm, ƒ/1.78 aperture, optical image stabilization
- 48MP Ultra Wide: 13 mm, ƒ/2.2 aperture and 120° field of view
- 12MP 5x Telephoto: 120 mm, ƒ/2.8 aperture and 20° field of view, optical image stabilization and autofocus
- 5x optical zoom in, 2x optical zoom out; 10x optical zoom range
- and so forth

Those are the capabilities of the sensors – I will translate:

- 48MP = 48 million detectable points (called pixels) usually in a 2-dimensional array, perhaps 8192 pixels by 5520 pixels.
- Each pixel can typically sense 8, 12, or 16 bits of different intensities of each of 3 colors (Red, Green, and Blue). 8 bits means 256 different intensities (2^8=256), 12 bits means 16 times that many (4096), 16 bits means 16 times as many as 12 bits (~64,000).
- The resolution (how small an object can be differentiated) at a distance depends on the distance. If the field of view can see something 8192 inches by 5520 inches in size, that translates into seeing a resolution (the smallest individual area) of a 1 inch square per pixel for the example here. But if the field of view is 8 inches by 5 inches, and assuming the focus is right, the resolution is of a 1/1,000 inch square.

- A wider field of view means that at the same distance, the camera can see a larger width and height, which also means the effective resolution is a larger region of space for each pixel.
- Stabilization means that small movements in the camera will be automatically compensated for to reduce blurriness. For example, if you are driving at 60 miles per hour looking at something a few feet away, and the picture takes 1/100 of a second to capture:
  - A mile is a bit over 60,000 inches, and takes you 1 minute (60 seconds) to pass. So each second, you are going about 1,000 inches, and in 1/100th of a second, you will travel about 10 inches. If the field of view is 100 inches (a bit over 8 feet) and the object of the picture is standing still, a 10,000 pixel wide image will be picking up an area of 1/100th of an inch of area, but because of the motion, it will be smeared over 1,000 inches. You will have a very high resolution smear or blur.
    - With stabilization, in this case, you will have the same smear or blur, and the stabilization won't help you to speak of.

And so forth

Note the in the specifications above, I left an undetailed "and so forth". Of course the devil, as they say, is in the details… Here are some more details:

- Sticking with the camera for now, the range of frequencies of light that the camera can sense are limited, but in many cases, comprise a far larger part of the optical (and non-optical) spectrum than human eyes can see. For example, infrared cameras can sense frequencies too low for humans, and because of different lenses they might be fitted with, they may be able to see microscopic things we cannot see with the naked eye. They might be able to focus at far higher resolution at longer distances by using telescopic lens arrangements, they may be able to capture more 'frames' per second than human eyes can differentiate to detect things happening so fast we could not see them, and in the dark, might be able to observe a single frame over a far longer time period to pick up very dim things we could not see.
- Cameras also often have built-in digital analytical mechanisms that, rather than recording the actual intensity values, adapt what they record and how they observe to conditions. It turns out this is quite similar to how human senses work, in that eyes, for example, change their apertures by changing the pupils. In dim light, the pupils dilate to let more light in; and in bright light, they constrict to reduce the light entering, thus maintaining the dynamic range of values produced by the sensors. Thus the underlying mechanisms change the characteristics of the observables based on conditions.
- Cameras often have built-in mechanisms like line detection to detect and segment areas on the sensor array and color gradient compensation so as to produce higher granularity than the actual sensor can sense. Stabilization is another compensation mechanism that artificially makes a shaking camera or image look like it was taken without movement. In some cases, pixels fail and cameras compensate for failed pixels by producing averages of surrounding values in place of that pixel. So-called logical (as opposed to optical) zoom provides a zoomed in version of the image by effectively

enlarging and possibly averaging pixels to make things look larger. Optical lenses have various defects that may result in distortions changing the light arriving at the lens at different places into different values at the outputs. Human eyes change shape as a result of pressure within the eye and the muscles that control where it looks, while cameras may produce changes in shape related to temperature and may change their view by reorientation using external motors to point the cameras or their sensors in different directions. The list goes on and on and on.

Now let's see the difference between what is sensed and what is observable.

What can be observed?

Sensing is translated into observation by analysis of some sort. Our eyes sense light by optical incoming signals triggering signals from sensors called rods and cones. In simple terms, rods sense black and white while cones sense colors. These sensors transmit signals to other parts of the brain which process those signals through the neural networks (networks of interconnected biological cells called neurons) which produce things we can observe, like lines and areas of different colors which are then fused into objects, like tables, chairs, cows, and so forth. These are generally observable (we can think about them), while the actual signals coming in the eyes are not things we can normally actually see or understand as the photons arrive.

The same is true of computer sensors, like cameras. They capture an image at the level of pixels (which are lower resolution than the underlying reality) and only to a specific color depth (typically a number of bits representing each of 3 ranges of frequencies we call colors). They completely miss many signals as do our eyes, and in order to make use of the sensed bits they produce, systems use analytical hardware and software to interpret them automatically. While the digital system could look at each bit and try to use it as an observable because the actual data is available to do so, in order to make sense of it, algorithms do things like detecting lines and surfaces to produce meaningful (useful in context) observables that can then be used to, for example, recognize you as opposed to other people.

The result of sensing PLUS analysis produces observables, and a hierarchy of observables are built up over time to produce higher level observables, like the notion that you are about to fire a gun, or have just fired one, or the higher level notion that a violent incident is underway, and so forth. This process is often called sensor fusion to produce indicators, and if analysis results in communication of a higher level concept (like an attack underway or pending), it may become a warning. Thus the term "indications and warnings".

And so forth…

Just like sensing has a so-forth, so does analysis. Because computers can be programmed with all sorts of additional analysis as we learn new and different ways to produce new and different observables of different sorts, they can observe things we cannot observe, and draw conclusions we could not draw without them.

The limitations of analysis given the data apply to the available methods of analysis, which change over time. Methods of analysis are limited by available computing time, space, speed,

and techniques, each of which change over time as pricing and availability change and as we make progress on techniques for different contexts.

Also note that multiple pictures can increase effective resolution, and other similar effects may apply. Here are a few key points:

- **Sampling rate and maximum detectable frequency**
  - One of the interesting effects of being able to take samples one after another is that changes in the thing being observed can be tracked. If the sampling rate is far faster than the changes, then samples will show the shape of the changes to a fidelity associated with the sampling rate. But if the rate of change is higher in frequency than the sampling rate, things will be a bit stranger. For example, imagine that change is happening at twice the frequency of the sampling rate. Then 30 samples a second looking at a waveform that going up and down 60 times a second would look like one picture every 2 cycles, or no change at all. If the sampling rate was off just a bit, then it might look like very slow motion when in fact the motion was much faster. So the sampling rate creates aliases of the actual rate of change for frequencies higher than the sampling rate.
- **Small motions and how much more information you can get**
  - Imaging we can look at samples with pixels that resolve to 1 inch per pixel. Suppose we move one inch and take another picture. Then, all other things being equal, we see all but one row (or column) of pixels we saw before and add one new row (or column) of pixels. That's all the new information we get. But suppose we moved half an inch instead. Then we would get values half way between the previous samples, and presumably, they could be different for every row (or column). This would effectively double the resolution of the previous picture.
- **Precision and accuracy issues**
  - Care must also be taken, particularly with digital output of sensors, because they often report a level of accuracy above their actual precision. For example, a sensor that can differentiate 12 bits may have results stored as a 16 bit value, in which case the last 4 bits represent precision beyond the actual accuracy. Also, the non-linearity in sensors produce changes in output that are not necessarily linear in the changes in the intensity of the input. At some point, a 0 flips to a 1 or a 1 to a 0 in the lowest order bit of the output. That difference in input is less than the typical difference before the next data value is reached and it flips back while the higher order bit next to it changes. Similarly, the difference in light intensity that triggers the next bit change in output might be very different in low light intensity than in higher light intensity, or in one color vs. another.
- **Missed frequencies of light**
  - The sensors on most digital cameras are designed for three color visibility (red, gree, and blue typically), while the cones in humans do not necessarily see the same frequencies. In addition, in their color ranges, different frequencies appear brighter than others. For example, so-called Xerox blue is a color that copiers often cannot perceive and thus cannot accurately copy. Similarly, some paper is embedded with particles that make security features printed on them show up when

copied or photographed that are not normally visible to the human eye. In some cases, colors simply do not appear, even though they block the light from behind them from appearing. Consider what happens when you paint your face so as to have your features appear differently to a camera than to another person.

Of course this doesn't just apply to cameras. It applies to all sorts of samples from all sorts of sensors. So the sensors out there, if properly analyzed, can produce a lot more information than you might initially think, and might be more or less accurate or precise than is apparent. They can be fooled by understanding how they work and their limitations and exploiting those limitations against them, just as people can be fooled by understanding our low-level cognitive limitations and exploiting them against us.

Magicians make a living by fooling people at different cognitive levels. They take advantage of cognitive limits like misdirection to change your focus of attention away from something they are doing, and selective concealment to hide something they do from your sight even as you look directly at the place the change is happening. And fraudsters do the same sorts of things to steal from you, while the media does the same sort of thing to get you to see what they want you to see – the zoomed in shot of a crowd that looks huge when it is actually small.

How do we know what they can observe?

These examples with cameras are only about one sort of modern sensing and observation type. Let's look at a bigger list of what they might be able to use to observe you.

What sensors do they have and how can they be used?

A good starting point is the sensors they have:

Cameras and optics:

Cameras and other optical mechanisms can span different ranges of frequencies with different sensitivities in different frequency ranges. The most commonly known types are infrared systems which can produce images when there is no humanly visible light, but systems with wider spectrum sensors can also produce images across a very wide spectrum of frequencies (colors) of light.

- Cameras operating as video devices (taking many images per second) can also observe things like vibrations in a room by watching change in light on reflective surfaces and other similar changes in the appearance of the sensory data. A particularly interesting example is the observation of a glass of fluid that vibrates with sound in the air. By detecting the changes in the surface, subtracting the stable light values at each color from the moment to moment values, the resulting frequencies of change will often reflect the sounds in the room. At 60 frames a second, you can hear sounds of less than 30 cycles per second, but by using cameras in higher frequency ranges and looking across different surfaces in the room, you can often pick up sounds at far higher frequencies. Consider for example that sound travels at about 343 meters/second in air, so in 1 60^{th} of a second, it travels about 5.5 meters, or 18 feet. In a room with objects spread over that distance, changes in objects at different locations will show different parts of the same sonic wave forms at essentially the same moment in time (the speed of light is about $3*10^8$ meters per second, so the light will be delayed

about 1/ 10millionth (10^{-7}) of a second over a distance of 30 meters). By piecing these wave forms together, you should be able to listen quite easily to the full range of frequencies the human ear can hear.

- Research in this area has ranged from using videos to sense vibrations in buildings to detect structural properties[4] to "The Visual Microphone"[5] which uses a high speed digital camera (~2200 frames per second) to reconstruct audio from video. A subsequent study[6] examined how lower speed cameras are limited in achieving this goal. Other methods have been explored to a more limited extent. This is typical of cybersecurity research where demonstrations prove a concept but engineering challenges remain and are often unpublished for a time.

Microphones and vibrations in media:

In addition to cameras and other devices that can sense changes related to motion of the media of a space (air, water, etc.) there are also actual microphones, intended to listen to vibrations in a (typically the air but also any other) medium.

- Typical modern computer microphones are very small and part of almost any device you can name. In fact, many cameras come with built in microphones, as to cell phones, computers, and of course speakers (which as it turns out can usually be used as microphones as well). They typically listen over a far wider frequency than humans can hear (or speak). Most range from 20 cycles per second (Hz) or less up to 20,000 Hz or more and can listen to sounds from about -26 decibels (dB) to 130dB in volume. 10dB is about the level of sound from normal breathing and 20dB the sound of a mosquito buzzing, while 120dB is typical of a siren from an ambulance (standing right next to it), and a shotgun blast is about 150dB. 10DB is about a factor of 2 in perceived volume, so normal breathing is about ½ the perceived volume as a mosquito buzzing. This sensitivity also varies over frequency ranges with more sensitivity typically in the 1,000 Hz to 10,000Hz (10kHz) range. Middle C is about 261 Hz, while each time you double the frequency, you go up one octet in the musical scale. So high C is is about 520Hz, an octave above that is 1040 Hz, and 3 octaves above that is about 8,320 Hz. Dogs typically hear from about 40Hz to 60kHz in frequency and between 10 and 20 dB quieter sounds than people (2 to 4 times quieter).
- You can also add a parabolic sound reflector to a microphone and point it at a target to segregate and amplify the sound coming from the target into a microphone to listen at a longer distance. A parabolic antenna is in the shape of a parabola and, the way a parabola works, reflecting sound (or light or whatever) coming straight toward the parabola is reflected toward the focal point of the parabola, while from other directions, it goes elsewhere. The amplification is proportional to the square of the diameter of the aperture, which is to say, by doubling the width of the antenna dish, you increase

4 Qiankun Zhu, Depeng Cui, Qiong Zhang, and Yongfeng Du, "A robust structural vibration recognition system based on computer vision." https://www.sciencedirect.com/science/article/abs/pii/S0022460X22005041

5 Abe Davis, Michael Rubinstein, Neal Wadhwa, Gautham J. Mysore, Fredo Durand, and William T. Freeman, SIGGRAPH 2014-07-27, "The Visual Microphone: Passive Recovery of Sound from Video", https://dl.acm.org/doi/10.1145/2601097.2601119

6 Edward James Brambley, 2021-05 "Measuring Vibrations from Video Feeds" states "...any existing video footage (such as from CCTV) is unlikely to be of sufficient quality…" with regard to the Davis paper https://www.researchgate.net/publication/351832773

the amplification by a factor of 4. A shotgun microphone uses a phased array of microphones for higher directional fidelity[7] and by combining this with a parabolic sound reflector, you can do even better.

- But what's even more amazing is what you can get from analysis of these sounds. For example, people can be identified by their heartbeat by listening with a special purpose device up to 200 meters away. Similarly, by listening to keystrokes on a keyboard, the characters typed can be differentiated, so we can hear what you type into your computer if your microphone is on. You can hear people in another room if a microphone is on, in many cases, even if the intervening door is closed. You can also hear vibrations of components like power supplies and sounds of printing devices, and background noises from other rooms, and with more than one microphone, you might even be able to physically map a room and its contents by the differences in how sounds bounce around. Add the ability to send sounds with a speaker and listen to the results, and you have a form of sonar. Like video sensors can produce sonic observables, sonic sensors can produce visual observables.
- Footfall, clothing sounds, background sounds, and more can be derived from sound inputs. Footfall, like voice recognition, can be heard in sounds from most microphones. Walking sounds are different based on height, weight, injuries, shoes and shoe styles, floor squeaks and shoe squeaks on floors, echo sounds, specific individuals, and so forth. This is commonly used to differentiate between known individuals. Different sorts of dresses, pants, blouses, shirts, and hats produce different sounds under movement and in the wind. The ocean sounds different from the city, and mechanical equipment, birds, tires on roads, as well as other sorts of background sounds are all differentiable based on sound, as are many other things.
- Medical,[8] industrial, automotive, consumer, agricultural, environmental, aerospace, telecommunications, and military applications of sound and other vibrational sensors are also growing rapidly. Wearable vibrational sensors are being embedded in clothing,[9] nano-sensors embedded in other devices, sensors for vibrations in products as shipped to detect excessive impulse that may damage a product in transit, and you can extend this almost without limit and encounter examples in use today.

Motion and Location:

Sound and picture backgrounds and old detective movies come to mind in terms of detecting location. As an example, if you hear the ocean in the background and the sounds of rides and a boardwalk, there are only a small number of locations where this can actually be found. If you know it is within 100 miles of my house (for example if they left here 2 hours ago by car), it is the Santa Cruz beach boardwalk. If we hear a radio station in the background, we can usually locate within a radius of a few hundred miles, but also identify the time of the sound pretty precisely, because radio stations are required to track and record what is on the air when.

7 https://en.wikipedia.org/wiki/Parabolic_microphone

8 2022-10-07, "Sensing Devices for Detecting and Processing Acoustic Signals in Healthcare", https://pmc.ncbi.nlm.nih.gov/articles/PMC9599683/

9 2023-10-01, "Progress in wearable acoustical sensors for diagnostic applications", Biosensors and Bioelectronics, Volume 237 https://www.sciencedirect.com/science/article/abs/pii/S0956566323004517

- Similarly, portions of images can be used to identify a location using modern AI technology. Simply put in the picture and it will find a match with a fairly precise location. Motion detection can be identified by blurriness in a single image or distance between different images. Using sound, it can be detected by Dopler analysis, the frequency shift associated with sounds approaching and retreating.[10]
- But these are only examples of indirect location and motion detection. Digital devices tend to provide and reveal location and motion as well. Device global positioning system mechanisms, multiple cell tower amplitudes, WiFi availability and signal strength, and other such things can also be used to detect location as a function of time. These can sometimes get a location at a time within a few feet.
- Video from fixed locations, such as closed circuit video, are often used in investigations to figure out who did what and when. This includes both private and public video systems, and when augmented with technologies like facial identification and tracking clothing and individual people in pictures over time, people of interest, even when they seek to conceal themselves, are often found in minutes to hours. Many famous hunts in recent years that historically took a long time and often failed have recently resulted in arrests in only a day or two.
- Satellites can take images in multiple frequency ranges, and depending on the antenna size and distance from Earth, resolution of less than an inch can often be produced. Of course satellites are expensive, but drones, including unmanned aerial, water, ground, underwater, and underground vehicles are far less expensive and can be tasked to follow or find individuals or other things they can observe based on available sensors. And in between these extremes are other aerial assets, like planes and Unmanned Aerial Vehicles (UAVs) used for coordinating and gathering real-time intelligence in battlefield situations.

Electromagnetic and optical wave forms

Emanations from any mechanism using electrical components, including people whose cells interact using electrical signals, can be sensed and analyzed using a wide range of sensory mechanisms.

- At a basic level, waveforms are transmitted by the changes in electromagnetic fields which spread out in all directions at the speed of light in the media, and are attenuated by different materials in the environment, such as walls, air, windows, people, cars, and anything else present. Because the volume of the space in 3 dimensions grows exponentially with distance from a source, the energy available in the waveform decreases exponentially with distance from the source. So as the distance doubles, the energy available for reception goes down by a factor of 8. Signals are received by antennae, which are typically one or more lengths of metal or other conductive material connected to electronic components that amplify and turn the emitted signals into local signals that can be presented and/or stored.
- Light amplification by stimulated emission of radiation (laser) light is coherent, in that the emitted waves are aligned and of the same frequency, which causes them to not spread out as the light moves from place to place. For that reason, a laser can transmit

10 NASA, “Doppler Effect”, https://www.grc.nasa.gov/www/k-12/airplane/doppler.html

over long distances without substantial loss of energy. Lasers are then sent toward a target and reflections returned at great distances to detect, among other things, changes in the reflected surface which result from things like sound hitting the surface. Depending on the frequency, they may be invisible to people.

- Signal processing is used to process incoming waveforms into usable content based on the coding used to create those signals, to produce coherent end-to-end communication. When I say 'coding', that includes the nature of how different signals are produced, so that for example, in a person's brain the communication between cells tends to be a series of electrical pulses in the frequency range of 50 Hz. By listening for these signals, brain activity can be detected, and by using more than one sensor, the location in the brain of those signals can be identified. For example, by paying attention to speech centers, things people say to themselves can be detected, and according to recent research, turned into audible speech that can be understood.[11] So be careful what you think.
- Similarly, signals emitted by computers can be detected and analyzed to find things like what's on the screen, what is being typed, computations underway, keys used in cryptographic systems, and so forth. The distance from the source and medium of transmission are important factors in how these things work. For example, a device like an earphone plugged into your ear has a good chance today of detecting brain signals as well as other physiological states, such as blood pressure, heart rate, and so forth, assuming it is designed to do so. One recent example is a US Patent embedding sensors in earbuds.[12]
- An intentionally planted device, for example in clothing or in a hat, can provide very close physical sensory mechanisms and transmit the results of sensory data over a substantial distance before it gets retransmitted elsewhere. And of course cars, cell phones, computer equipment, and anything 'cyber' today likely contains various sensors that either intentionally gather data or can be exploited to do so. An exploitation example is the microphone on a typical home assistant device. Even if the device does not listen in on conversations, the microphone itself moves with the air, producing electromagnetic waves that can be detected at a distance.
- By the way, most speaker systems have electromagnetic mechanisms that cause a surface to move to produce sound, and sounds in the air move these same surfaces producing electromagnetic changes in the mechanisms that can be detected at a distance, turning them into listening devices as well.
- Noise is also an issue. The signal to noise ratio is the intensity of the signal divided by the intensity of other signals (the noise). In a given frequency range under observation, if the noise is high enough you cannot pick out the signal from the noise. However, if the signal is coherent, by listening for the coherence, you can often pick out the signal even in the presence of a lot of noise. In fact, there are special coding methods for signals designed to make them easier to pick out in the presence of different sorts of noise present in various environments. More on this later I suspect.

11 Search for "Brain Computer Interface" for lots of examples. See as one example, 2025-04-29 "Brain-computer interface restores natural speech after paralysis" at the National Institutes of Health

12 https://patents.google.com/patent/US20170078780A1/en US Patent 2017/0078780 A1

Pressure, temperature, and other environmental factors

Things like pressure sensors can be used, for example, to detect entry and exit from spaces, because of air pressure differentials between closed areas that change when opening doors equalize the pressure.

- Temperature sensors can detect changes indicating the presence of more or fewer people in a space. Pressure sensors on the ground are used for things ranging from foot fall detection to weighing, and of course different people weigh different amounts and have different footfall patterns. Humidity changes in similar ways, and carbon dioxide (CO_2) levels reflect things like people breathing in a space. Depending on the specific sensors and what they are connected to, they might be able to detect levels and differences to the extent of their sensitivity. And of course multiple sensors allow further analysis.
- Wind speed, pollution levels, and other similar sensors are widely available, but less useful for detecting individuals or sensing their presence than they are at detecting general environmental conditions. However, in places where people burn wood for heat, sensors might pick up the presence of a fire in a cabin or similar location indicative of a person being present.
- Ocean-based sensors in arrays are used for things like tsunami detection, but also for detecting schools of fish, thermal regions as they change, undersea vents releasing gasses from below the sea floor, the presence of plumes of different sorts of biological phenomena, tides and wave conditions, oncoming storms, changes in weather patterns and movement indicative of changes in large currents effecting global weather, survival of microscopic species that are at the bottom of the food chain for many of the life forms on Earth, and any number of other things.

Chemical and biological sensors

All manner of chemical sensors are on the market today, and they demonstrate the capacity to smell out, among other things, specific compounds associated with perfumes, after shave lotions, and sprayed products. Of course many of them are used to alarm at the presence of specific compounds in specific areas, but others are more general purpose or have multiple compound detections embedded.

- Most such sensors are composed of receptors that interact with the thing being sensed (called an analyte) and transform the chemical information (usually level of concentration) into a measurable signal, like an electrical current or voltage, a change in resistance, etc.; an optical signal like the amount of light absorbed of a specific frequency producing florescence or changing absorption of light; a fluorescent signal caused by changes in pH; chemiluminescent molecules that measure changes inside a cell; a temperature change resulting from a chemical reaction; or whatever other clever thing the science and engineering folks come up with.
- Biological sensors are often used for medical diagnostic purposes. There are lots of different ways this works, but in many cases, it involves some pre-processing of samples such as taking blood, spinning it in a centrifuge to separate cells from the fluid they reside in, coloring them with a dye, and examining them under a microscope. This process, or parts of it, have been largely automated today. A specific example that is

particularly important today is DNA sequencing. The process essentially breaks down a single cell, extracting the DNA strand from it, and identifying the sequences of "bases" adenine (A), guanine (G), cytosine (C), and thymine (T). Base pairs (A with T and C with G) are in sequences that can be identified, usually by using polymerase chain reaction (PCR) and a detector that recognizes fluorescent tags of different wavelength (one for each base). DNA is generally considered to be unique to individual humans (and other animals) except for identical twins. As such, when they find a flake of dust on a keyboard, if it is from cells of the user, they can identify an individual (or their twin) typing at that keyboard. DNA databases are available, and can also be used to find family members and associated people with potential diseases or similar conditions. DNA tests typically take at least hours to complete, and from a mouth swab, this can be done in 90 minutes or less and completely automatically.

- Biological sensors are placed in sewage systems today to detect levels of specific diseases in populations, can be placed in a specific toilet or urinal to detect whatever they are looking for, and these can report presence and specifics within seconds to minutes of sample arrival. Sensors can also be used to detect the presence of inorganic ions and organic pollutants in wastewater and likely other fluids.
- People emit different biological and chemical signatures as they pass through spaces, and this is also effected by what they eat, their health status, time of day, time within other biological cycles, exercise patterns, and so forth. Some of these are readily sensed with olfactory senses and sensors, while others can be tasted as the compounds float through the air. Gaseous emissions, sweat, recent foods and drinks on the breath, and so forth can be used to categorize people and their recent behaviors, where they have been, and in context, who they have interacted with, what they ordered from which restaurant, and so forth. Dogs have an acute sense of smell to the point where they have been able to detect cancers and other conditions[13] from olfactory examination of serum and urine.
- Today, time frames for such sensors and analysis ranges from seconds to hours, and getting these sensors in place can be expensive, but as the field progresses, costs go down, analyses are simplified, and time frames get shorter. For security detection of biological attacks, costs are balanced with consequences, and populations are the things usually being protected. However, individual application is increasing rapidly, and a revolution in medical diagnosis, detection, and condition tracking is underway.

Nano-technology sensors of various sorts

The development of nano-technology has made leaps and bounds. In this case, a typical sensor is built by making shapes of material that attach to the shapes of compounds (typically fluids or gasses) pumped past the shaped material, resulting in a change in conductivity that is electrically detected to sense a single particle. Generally, the size of these sensors is in the range of less than 100 nano meters (nm), 1 nm being 1 billionth of a meter. To get a sense of this, a human hair is typically 100,000 nm wide, and the distance of an electron orbit from a proton in an hydrogen atom is about 0.05 nm.

13 MacKenzie A. Pellin, Laurie A. Malone, and Patricia Ungar, "The use of sniffer dogs for early detection of cancer: a One Health approach", https://avmajournals.avma.org/view/journals/ajvr/85/1/ajvr.23.10.0222.xml 2023-10-05

- Because of the small size and high sensitivity (a single molecule is detectable), a very large number of nano-sensors can be placed on a very small device to detect an enormous number of different molecules. If they want to spend the money on it, they could presumably make a sensor to detect almost anything they want in terms of particles in the air or water. In many ways, this is how a nose and tongue work. Olfactory (smell) and taste senses are composed of a large number of different sensors that are shaped to detect different chemical compounds. The smell and taste signals are transmitted as electrical signals to regions of the brain and associated with things we perceive through learning. In the automated arena, the same general approach uses learning or programming to associate senses to detectable compounds. The same methods automate an increasing range of other functions for cyber-systems.

People as sensors

We aren't just talking about spies, but they are included of course. By observing people online and in person, anything they express, either directly by things like what they say, and indirectly by what they do, is something that can act as a sensor relating to other people or things.

Other sensor types

There are plenty of other types of things that can be sensed today. Proximity, acceleration, touch, gyroscopic, color, water and other fluid level, tilt, flow, particle, radiation, vibration, flex, impulse, and many other sorts of sensors are out there. To get a decent list of these, you might want to look online...[14]

Active sensors

The sensors listed above are predominantly passive in nature. They simply await signals and process them as they arrive. But in the case of active sensors, sensors are combined with sources of (typically) waveforms to provide sensing of things that would otherwise not be available. Here are some examples:

- **RADAR and SONAR** are obvious examples of active sensor technologies. They transmit signals and look for reflections of those signals off of objects of interest. Similarly, instead of looking at reflections, systems can look at what is transmitted through the targets. Signal processing in these systems combines patterns sent from the emitter(s) with signals received at the sensors to identify properties of the signal changes. As such, these components are themselves cybernetic systems (composites of sensors, actuators, communications, and control) that act as components in other cybernetic systems, such as avoiding collisions or mapping an area. LIDAR (Light Detection and Ranging) is a remote sensing technology that transmits pulsed laser light and detects reflections. RADAR uses radio waves, SONAR uses sound waves, and you get the idea.
- **The Thing** was a device provided as a 'gift' to the US embassy in Moscow. It consisted of a "The Great Seal" (an American Eagle carving), and contained an area with air and a single piece of metal. It had no power, was connected to nothing, and was completely passive… unless transmissions in specific radio frequencies were received.

14 https://en.wikipedia.org/wiki/List_of_sensors is a pretty good list with pointers to specifics.

When such frequencies were received, it acted as an antenna and when active, sound from the room would cause the metal to vibrate, forming a capacitative link resulting in effectively retransmitting the sounds in a classified meeting to the Russians listening outside the embassy.

- **Lasers on windows** reflect, and by observing the reflections, the phase change of the return signal based on the window vibration allows the remote listener to hear the sounds behind the window pane. Recent research appears to show doing the same sort of listening from reflections using signals from optical computer mice.[15]
- **Lots of other things** allow observing (listening or seeing in most cases) what is otherwise hidden. In general, any signal sent into an area that is altered by conditions in the area and can be observed outside the area can be used for active surveillance. This depends on the ability to get signals into the environment and observe signals emitted from the environment, and thus the physical protections of the environment may have to be taken into account to successfully apply these methods to specific environment.

Informational sensors and records

Information of all sorts form the basis for almost every facet of modern society. Here are just some of the examples of the informational 'sensors' and their uses:

- **Archives and governmental records** include records of property ownership, taxes, fines, crimes, facility drawings and approvals, registrations of all sorts, complaints, background checks, birth and death records, health-related records, and anything they are able to access from private datasets by purchase, order, or intelligence operations.
- **Financial records** include transactions, accounts, balances, dates, times, and places of presence and activities; details of what you buy or sell from or to and whom; credit ratings, balances, income, expenses, and payment histories; groups and societies you are a member of, active in, fund, or get funded by; and when fused together, associations of all sorts reflected in financial activities of the society writ large. These records also tend to reveal a great deal of other information, such as buying habits, medical conditions, relationships, your location over time, etc.
- **Usage logs and audit trails** of cybernetic systems provide an almost unlimited variety and amount of information on the users. Old-style logs include things like login, logout, what programs were run and when, from where, by whom, and so forth. Databases tend to keep track of every transaction, including time and user, so each item entered is readily tracked to the individual as logged in. Web logs may include all the content sent to or retrieved from a Web site or anything interconnected with it. AI logs will tend to record everything ever sent to the AI engine and possibly all of the responses. And this extends not only to the interface you are using, but also to interactions with printers, mouse movement, keystrokes, voice and video input, and so forth. They also record entries and exits into rooms, if access cards or similar mechanisms are used, and in stores they increasingly track your movements and what you put in your cart.

15 https://sites.google.com/view/mic-e-mouse has an anonymously published paper on this.

- **Specially planted surveillance devices** in information infrastructure or other mechanisms provides whatever added information the supply chain in place can provide. For example, Chinese solar panels have been shown to include surveillance devices that broadcast whatever they collect to unknown remote recipients, cell phones have long been remotely activated to covertly use their sensors and log location, activity, and so forth. Power systems in homes increasingly log usage of each device and identify when they are working properly and when they are going bad for maintenance purposes because motors and other equipment tend to use more power for the same operations as they age or as lubrication fails. And of course these sorts of mechanisms act as Trojan horses when the user is not aware of them.
- **Communications** lead to all manner of analysis, increasingly including sentiment analysis, cognitive analysis results, details of all information exchanged, associations, timing at locations, and have covert channels, such as timing channels that have been used to detect keystrokes even in encrypted traffic.
- **Stored content** includes what you send, receive, collect, and how you use it and work with it. This can reflect anything from recordings of conversations to all texts sent between parties, to notes taken on devices, to drafts of writings prior to their finalization or publication, and on and on.
- **Time and place information** regarding where and what you do and when and travel time information, holes in records, etc. This has been used many times to associate people with places in criminal investigations, but is also usable for intelligence gathering, identifying associations, noting preferences against religious convictions of others, and on and on.
- **Attribution and attestation infrastructure** is being developed to provide reliable distributed association of acts to actors that enforces event sequence tracking and often includes location, identification information, authentication factors, and related information, including arbitrary content. These systems are designed to allow any content to be attested to by individuals or other entities.[16]

Review of sensor types

The full set of surveillance capabilities in a location comes from combining all of the available mechanisms identified here, plus those I forgot to mention or didn't know about, in every possible way they can be combined over time, and analyzing them with all known and then available methods of analysis, then combining that with other knowledge from other sources to figure out what's going on. In other words, information collected today may be analyzed tomorrow with new techniques, faster computers or analysis mechanisms, and in context of more information gathered and analyzed from other places. Doing this sort of analysis is often referred to as "the puzzle problem".[17]

One more thing. The way I know about the available sensor types is by spending my time and mind on keeping track of things. I add that to my education as an electrical engineer and my experience in computing to understand the situation. But if you want to get a good understanding, it's not all that hard to do. All you have to do is go to trade shows where they

16 F. Cohen, "2025-09-B - Attestation for Attribution", https://all.net/Analyst/2025-09-B.pdf
17 R. Lyon, "The intelligence jigsaw", The Strategist, https://www.aspistrategist.org.au/the-intelligence-jigsaw

sell these things. You can generally get a free ticket, or perhaps pay a few tens of dollars, and spend a day here and there seeing a wide range of products and services offered on the market. While you may imagine that governments have significantly more or better sensors and interpretation mechanisms than commercial companies, it's rarely true to a substantial extent, and most of the actual sensors likely to be used are commercially produced anyway.

Analysis of available observables

Analysis also produces unexpected results to the unsuspecting person. As examples:

- **Usage patterns** can be detected by 'traffic analysis' and other similar 'covert channels', in some cases allowing your user ID and passwords to be read when sent through encrypted communication.
- **Reflections off of walls** can allow the content of a video display to be read without direct line of sight, even around a few corners.[18]
- **Traffic analysis** is another example that is commonly available and often overlooked.[19] By watching network, radio, or other signals between communicating parties, the content of the messages can often be revealed, even if at a low level of granularity. Noticing the there is a party at a location can often be done by observing delivery of party favors, creating association graphs between people to identify groups by online communications is increasingly being used.[20]
- The list goes on and on.

If I missed anything artificial in nature, name it and today it likely has embedded sensors.

Where are they?

Sensors are manufactured from materials and processes and in volumes ranging from 1 to hundreds of millions. They are made all over the world, and placed in all manner of places. Here are just some examples:

- **Dust:** Some have suggested microscopic sensors ('smart dust') be spread over fields where food is grown to detect conditions and communicate them in real time, although to my knowledge, so far, this has not been done in substantial volume.
- **Tags:** Sensors are placed in all sorts of devices we buy, including things like Radio Frequency Identification (RFID) devices which are placed in anything from items of clothing to boxes and tracked over the life-cycle of whatever item they are connected to or embedded within.
- **Household:** Sensor arrays are commonplace in toasters, refrigerators, stoves, and other household appliances, power switching panels in homes now often have sensors to detect what appliances are in use and how they are functioning, including prediction of when they will go bad.

18 M Backes, M. Durmuth, and D. Unruh, "Compromising Reflections-or-How to Read LCD Monitors around the Corner", Security and Privacy, 2008. SP 2008, 10.1109/SP.2008.25

19 https://en.wikipedia.org/wiki/Traffic_analysis

20 T. Wen, Y. Chen, T. Syed, and D. Ghataoura, "Examining communication network behaviors, structure and dynamics in an organizational hierarchy: A social network analysis approach", Information Processing & Management, Volume 62, Issue 1, January 2025

- **Fire and water** sensors that automatically detect and alarm are widely available and becoming more popular, and one company I am invested in automatically mitigates fires and water damage at the point of origin in real-time, forming local cybernetic composites (sensors, actuators, communications, and control) that are then fused as components in a larger composite for multi-unit housing, hotels, and storage facilities to locally mitigate damage without the need to evacuate writ large and with far less damage.
- **Doorbells and home automation** systems, including microphones and other sensors are commonplace in many rooms of homes. These often include automatic detection and categorization of what is happening with selective alarm and response functions, so that, for example, a person with a package generates a different response than a small animal. Again, these are composites of sensors, actuators, communications and controls that form a cybernetic system that integrates as a component into a larger cybernetic system for whole-house control.
- **Temperature** sensors have been common in homes for at least 75 years. They automatically trigger water from sprinkler systems to put out fires, but they tend to not have communications and controls, but rather, have a simple mechanism to dump water when something is broken by the heat of the fire. They may also ring a bell.
- **Cars** and other mobility mechanisms commonly have sensors, at the level of each seat, many parts within the cars, parts of engines, control systems, steering and brakes, windows, tires, drive trains, electric motors, batteries, electronic components, mapping , driver assistance, entertainment, and all manner of other similar systems, and more. Modern vehicles are really cybernetic systems with multiple cybernetic components operating as a composite.
- **Infrastructure:** Roads, sidewalks, subways, underpasses, overpasses, parks, recreational areas, and commercial spaces have sensors of all sorts, including private and public closed circuit televisions, microphones, motion, and the rest of the list of sensors. Cities like London are filled with sensors to the point where they can likely trace any individual in every activity they do outdoors and many indoors, at most times. Small municipalities have sensors to read license plates and picture the drivers and passengers to track down criminals and arrest them without massive car chases or other similar risks. Gunshot detectors are widespread, weapons detectors at venue entries, and other search technologies at malls and public events are widely deployed.
- **More:** Sensors are in almost all transportation systems, water and power systems, networks, communications systems, and commercial items, including commercially sold systems like kits, accessories, keyboards, mice, other computer equipment, lighting systems, printers, test equipment, makers equipment, and on and on.
- **Where:** Sensors are placed in underground, on-ground, under-water, on-water, aerial, and space systems, including fixed and mobile systems. **Anywhere!**

Surveillance vs observation vs. sense, and focus of attention

Surveillance can be thought of as what they chose to observe vs. what they can observe or sense. It has to do with their focus of attention.

Anything anytime is not the same as everything always.

Even with modern AI and all the computing power out there, nobody and no entity can actually observe everything that is sensed all at once all the time, and produce every possible analytical result. And this will always be true. And for that reason, there will always be gaps and limitations. They see what they want to see and hear what they want to hear, because they can only focus so much attention on so many things, and they (and you) have to choose.

As a fundamental, it is a reasonable assumption that if a major government wants to focus attention on you to the maximum extent, they may be able to gain access to and analyze all of the sensor data from every sensor you are meaningfully sensed by and perform all of the analytical functions available to them or anyone else they may want to hire or exploit. Of course this is an exaggeration, or as I like to call it, a conservative assumption.

This is another way of saying that the best way to minimize what they observe and understand about you is to not gain their focus of attention:

Stay below their radar.

Since they cannot watch and analyze everything always, try to get them to ignore you in favor of others. Obviously, you can do this passively by not doing things that trigger their observations or, less obviously, actively by making it look like someone else is doing the things you don't want them to know about and making it look like you are only doing things they do not care about. There are of course variations on these themes.

Of course to do this well when you are doing things they want to observe, you likely have to know what triggers their focus of attention, and this usually requires an intelligence operation (yours, theirs, others'), which you then have to hide or disassociate yourself with.

In practice, actual surveillance usually starts with general things that can be observed about anyone or almost everyone, and which are observed, either uniformly or statistically. If these trigger attention, or on a random basis, increased surveillance is focused on individuals, groups, or entities, typically for periods of time adequate to tell if there is anything to look at in more detail. From this level of attention, the same thing happens to take surveillance to the next level and so forth until maximum surveillance is placed on a relatively small number of people, groups, and entities. If you are unlucky and as good as you can be at avoiding this scrutiny, there is still a chance of getting found out, but the more and more obvious the indicators, the more likely you are to be surveilled more closely.

In some cases in some countries, court orders are required to get to higher levels of detailed surveillance and related searches, and these typically require some level of probable cause that a crime is being committed in order to boost the surveillance beyond an accepted baseline. However, the private entities that collect and analyze observables are generally not bound by the same rules, and often go far beyond what most governments will undertake, for commercial purposes. In essence, private interests can fuse together any information they can get from any source they can get it from and do anything with it except perform actions that are illegal.

In the US, the government has systematically moved a lot of the intelligence process to private companies to avoid government regulatory limitations. And these companies have gotten better and better at gathering, storing, and analyzing this data to the point where

almost anything they likely want to know about the past can be generated from the available data. Predicting the future we will discuss later.

A simple puzzle problem example

It may be helpful to think through a few examples of what information could be gained about you and in what way. Suppose, for example, I want to know if you have a dog. That should be easy to do by looking at you as you walk your dog, assuming I have visual surveillance. But it might not be your dog. Depending on how certain I want to be, I might go further. And of course you might be hiding the dog, etc. So let's look at potential indicators rather than just guess at one or two things we might try.

- **Cameras and Optics:** I can use whatever optical surveillance mechanisms I have access to in order to see whether you and a dog are often together, and where. Adding some rules of thumb, if you are often alone with the dog in your home, we would have a higher level of certainty of it being your dog than if you occasionally walked it or let it stay overnight.
- **Microphones and vibrations in media:** I can listen to hear dog sounds and you sounds. As discussed above, unique or at least differentiating signatures indicate human or animal and what sort of animal, often to the specific animal or human. If the same sensor senses them they are in proximity to the extent that sensor localizes sources, and multiple sensors with volume levels in known locations can give multi-angulation and other redundant results to the resolution associated with those sensors in combination in the space they operate within.
- **Motion and location:** If we have motion or location sensors attached to various things, like vehicles, dog collars, or other accouterments, or of course the dog and person themselves, we can tell if they are together, where, and how often, where they go together, etc. This includes things like RFID tags sensed by RFID scanners in stores and other places around the world.
- **Electromagnetic and optical waveforms:** To the extent things like electronic collars are used, these are detectable, but the far less obvious indicators would be things like differentiable waveforms produced by individuals by their bodies. Again, tracking them for coincidental locations and times produces the observables used to make a determination.
- **Pressure, temperature, and other environmental factors:** Nothing immediately comes to mind for existing sensors I likely have access to, but perhaps you can think of a few for this one.
- **Chemical and biological sensors:** Obviously, dogs and people leave biological indicators as they emit various smells, urinate, defecate, sweat (not dogs), shed, and so forth. If I have sensors for these things in relevant places, or if I can place them there, I can use them to detect indicators.
- **Nano-technology sensors:** To the extent that I have such nano-sensors deployed, I could do that of course. Perhaps you might like to list some of the ones you think would work for this.

- **Other passive sensor types:** As a homework assignment, go find other sensors fo other types that might be useful for indications of “have a dog”.
- **Active sensors:** Many active sensors can be used to watch people and animal;s as they move around together, even within a building from outside. These could be used to track person and dog and associate them with each other over time, giving indications of whether the person has the dog.
- **People:** An obvious source of human-dog relationships is people who know the person and/or the dog. Go to the places they go to walk or train or veterinary clinics near them, and so forth and look for them coming in together.
- I**nformational sensors and records:** Now we hit the mother lode of sensor data that could reveal information. I’ll start the list, but you can probably keep on adding to it for a long time. Dog ownership records, medical records, licensing records, tags used to identify lost or stolen dogs, insurance records, dog club and training records, financial records showing purchase of dog food and accessories, digital photographs of the person with the dog, hotel records showing a tendency toward hotels that allow pets, online dog-related forums, advertiser databases for dog food and accessories, online purchases related to dogs, communications about dogs, phone records showing calls to dog-related entities, Web site visits to dog-related sites or content, and online queries. That’s a good starting point.

A systematic approach would be to go through an inventory of your capabilities for observation and identify all of the observables that might allow information on the dog / human relationship. In the above listing, I have only selected a few of the possibilities for examples. While you are at it, get pricing for the various options so you can optimize your efforts at scale.

The next step is to determine, for the level of certainty desired, what combinations of indicators are adequate for the decision to be made. In this case, the decision is whether you believe the target to “have a dog”. Note the imprecision of the definition. If you want a general sense, this is probably adequate, but as you get more and more precise in terms of what you want to know, the definitions have to be clearer and crisper, eventually to the point where you can put metrics on them. How certain are you that the dog and person are living together? How certain are you that the person has which property rights of ownership with respect to the dog? And so forth.

Once we can determine what information we need to declare the puzzle solved to the desired level of certainty, we start to assemble the puzzle of dog ‘havingness’ by placing or using sensors to find piece after piece until we have enough pieces in place to make the determination determined. We can also trade off time and cost and other factors if we have the data to support the different puzzle solutions and how they can be obtained, and can even sequence it for optimizations of various sorts.

Also note that things change with time. Dogs and people come and go. If it takes too long to put the pieces together you might find that they are not overlapping enough in time to produce a meaningful answer to the desired level of certainty.

To save you a lot of time and effort, my wife and I have a dog as of this writing.

But our dog is old and we don't currently have another one, so there may be a period of time when we do not have a dog, and then we might get another one.

If we find we want to do this again and again, or in a manner to detect the "have a dog" property continuously for some set of people and dogs, we can create a repeatable process at a desired pace that uses indicators to produce warnings. We can automate parts of the process and buy in bulk to reduce costs, or outsource parts of it to 3rd parties who already have the puzzle pieces we want.

Again, we are only looking at sensors at this point. What we can sense to put together the puzzle of "have a dog".

Environmental conditions

Sensors, like all physical things, operate subject to environmental conditions. Their precision, accuracy, timing, range of observables, and other properties change with temperature, pressure, humidity, and so forth. A classic example of this that might help in understanding is the movie Sneakers.[21] In one part of the movie, the part played by Robert Redford is trying to break into a room in a facility covertly. The room has temperature differential sensors, motion sensors, and other such stuff. In order to get past the sensors, they decide to slowly increase the room temperature to body temperature at a pace that won't trigger the change threshold, and they do other similar tricks, but in order to get past the motion sensor, the solution is "Go real slow", not more than an inch per second.

While this may seem like fantasy and is certainly fiction in this specific example, these techniques actually work in these situations. You can change the environment to change the way sensors produce observables, and you can behave in such a way that the sensed information does not produce observables above thresholds for detections.

Sensors summary

I have touched on observables and the difference between observables and what sensors can sense (sensible is not the same thing as sense-able and there Is no word I have found for things we can sense), and focused on the sensor capabilities and some limited ways they can be used to produce observables. But we are a long way from discussing the higher level aspects of communications and control and how they enable larger and more complex composite cognitive mechanisms. We will get to that later.

Hopefully you have an initial sense of what is out there and how it might be able to be used if targeted at you, those you love, or others you care about, to figure out lots of things about you and them. This is usually where folks warn you about the evils of surveillance and why we should try to stop the information from being collected or used. But I think that ship has sailed. The horse is out of the barn, Pandora's box is wide open, and trying to stop it is like spitting into the wind.

Having exhausted my immediate supply of relevant sayings, it's time to move on.

21 https://www.imdb.com/title/tt0105435/

