INTELLIGENCE · OPEN-SOURCE INTELLIGENCE

# Emerging Technologies (Satellites, Drones, IoT) as New Intelligence Knowledge Sources

Commercial satellites, drones and networks of connected sensors now record physical activity on a scale once available only to governments. This article explains what each technology can observe, how observations become intelligence, what research shows about their accuracy and the security, privacy and interpretation problems they raise.

ModQu research article · 2,611 words · 24 references (APA 7th edition)

For most of the twentieth century, watching physical activity from above or measuring it continuously at a distance was the business of governments. The first American photographic reconnaissance satellites of the 1960s, whose film was returned to Earth in capsules, were among the most closely guarded secrets of the Cold War (Day et al., 1998). Today, a business can buy recent satellite images of almost any place on Earth, fly a small drone over its own fields or construction sites, and receive continuous readings from thousands of connected sensors in its factories, vehicles and products.

These technologies have created new sources of knowledge about the physical world: how much is being built, grown, shipped, produced and consumed, and where. This article explains what satellites, drones and connected sensors can observe, how their observations become intelligence, what research shows about their value, and the problems of security, privacy and interpretation they raise.

## Satellites

### From secret to open

Belward and Skøien (2015) document how the number of civilian Earth observation satellites, and the number of countries operating them, grew rapidly in recent decades. Two changes transformed access. First, governments opened their archives: Wulder et al. (2019) describe how the decision to make the long record of Landsat imagery, which began in 1972, freely available in 2008 led to a large increase in its use for research and practical applications. Second, new missions were designed for regular, open coverage. Drusch et al. (2012) describe the European Sentinel-2 mission, whose satellites image the world's land surfaces every few days at a resolution of ten metres in several spectral bands, with data free to all users. Commercial operators now add imagery at much finer resolutions, sometimes daily.

Processing has become accessible too. Gorelick et al. (2017) describe a cloud platform that allows users to analyse decades of satellite imagery at planetary scale without downloading it, putting analyses that once required specialist facilities within reach of small teams.

### What satellites can see

Optical satellites record reflected sunlight in visible and infrared wavelengths, revealing land cover, vegetation health, water, buildings, vehicles and ships. Thermal sensors measure heat. **Synthetic aperture radar** sends microwave pulses and records their echoes; Moreira et al. (2013) explain how it can produce images day or night and through cloud, and can measure small changes in the height of the ground or structures. Satellites that image the Earth at night record artificial light.

### Measuring economic activity

Economists have used these observations to measure activity where other data are poor. Henderson et al. (2012) showed that changes in night-time lights can improve estimates of economic growth, especially in countries with weak statistical systems. Donaldson and Storeygard (2016) review a wide range of economic applications, from measuring urban expansion and crop yields to tracking pollution and deforestation. Jean et al. (2016) combined daytime satellite imagery with machine learning to estimate household consumption and wealth in several African countries, achieving useful accuracy where survey data were sparse. Burke et al. (2021) review evidence that satellite-based estimates of agricultural yields, poverty and other development outcomes can approach the accuracy of ground surveys in some settings, at far lower cost.

In business, satellite observations are used to estimate crop production before harvest, monitor construction and industrial sites, count vehicles in retail car parks, track the storage levels of oil tanks and observe activity at ports. Zhu (2019) found that the availability of such alternative data, including satellite images of retailers' car parks, made share prices more informative about firms' future performance.

### Analysis by machine

The volume of imagery is too great for people to inspect. Zhu et al. (2017) review how deep learning methods have been applied to remote sensing, enabling automated classification of land cover, detection of objects such as buildings, ships and vehicles, and identification of change between images. These methods are powerful but depend on training data, and they can fail when applied to regions, seasons or sensors different from those on which they were trained.

## Drones

Small unmanned aircraft have brought aerial observation within reach of almost any organisation. Colomina and Molina (2014) review the use of drones for mapping and measurement, showing how they can produce detailed images, elevation models and three-dimensional reconstructions of sites at resolutions of a few centimetres. Anderson and Gaston (2013) argued that lightweight drones would transform ecological research by allowing scientists to collect fine-detail data exactly when and where they need it, rather than depending on satellite schedules. Floreano and Wood (2015) describe the rapid development of small autonomous drones and their expanding range of applications.

For businesses, drones are mainly a tool for observing their own operations: inspecting infrastructure such as power lines, pipelines, roofs and wind turbines; monitoring crops; measuring stockpiles in quarries and mines; and recording progress on construction sites. These are forms of intelligence about one's own activities, often replacing slower and more dangerous manual inspection.

Using drones to observe other organisations' property raises legal and ethical issues. Aviation regulations restrict where and how drones may be flown, and privacy and trespass laws apply. In Canada, for example, pilots of drones weighing between 250 grams and 25 kilograms must register their aircraft and hold a pilot certificate from Transport Canada, and flights near people, airports and in controlled airspace are subject to further conditions. In practice, drones are rarely an appropriate tool for competitive intelligence; their main intelligence value lies in an organisation's own sites and assets, where it has permission and a clear purpose.

## Connected sensors: the Internet of Things

The **Internet of Things** refers to physical objects equipped with sensors and network connections, so that they can report their state and sometimes be controlled remotely. Atzori et al. (2010) describe the concept as a pervasive presence of connected things that interact and cooperate, and Gubbi et al. (2013) set out a vision of networks of sensors whose data are processed in the cloud to support decisions.

Connected sensors are now common in industry, logistics, buildings, vehicles and consumer products. They measure temperature, vibration, location, energy use, movement and many other conditions, often continuously. Kitchin (2014) describes how such sensors, combined with other digital data, allow cities to be monitored and managed in real time, while warning that this "real-time city" brings risks of technocratic governance and surveillance.

For businesses, connected sensors provide intelligence about:

- **Operations**: machine performance and early warning of failure, energy use and production rates.
- **Logistics**: the location and condition of shipments, vehicles and containers.
- **Products in use**: how customers actually use products, which features matter and when products fail.
- **Environment**: conditions at sites, in warehouses and along supply routes.

Mobile phones are, in effect, the most widespread connected sensors. Blumenstock et al. (2015) showed that patterns in mobile phone metadata, such as the timing and frequency of calls, could predict the wealth of individual subscribers in Rwanda and be used to map poverty across the country.

## From observation to intelligence

Raw observations are not intelligence. An image shows pixels; a sensor reports numbers. Turning them into knowledge requires several steps.

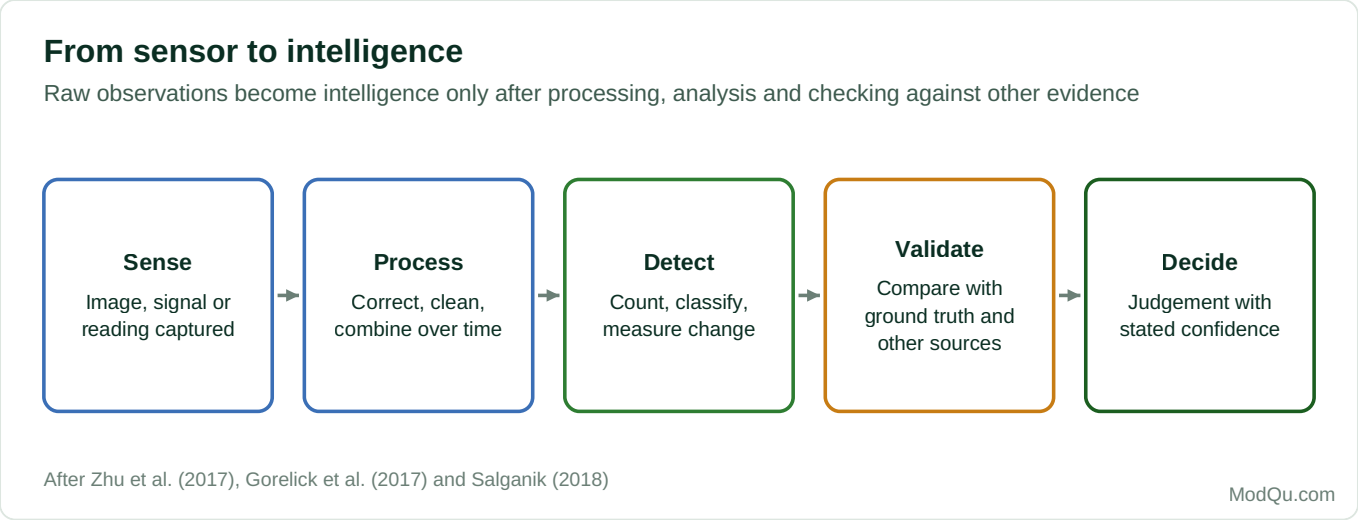



Figure 1. From sensor to intelligence. Raw observations become intelligence only after processing, analysis and checking against other evidence. After Zhu et al. (2017), Gorelick et al. (2017) and Salganik (2018); diagram by ModQu.

1. **Sense.** The satellite, drone or sensor captures an image, signal or reading.
2. **Process.** Data are corrected for distortions, atmospheric effects and sensor errors, cleaned and combined over time.
3. **Detect.** Objects are counted, land is classified, change is measured, anomalies are flagged.
4. **Validate.** Results are compared with ground observations and other sources to check accuracy.
5. **Decide.** Analysts interpret the results in context and state their confidence.

The validation step is often neglected. A model that counts cars in car parks may perform well in summer and poorly when snow covers the markings. A crop-yield estimate may be accurate for one region and biased for another. Salganik (2018) notes that digital data sources are often incomplete and change over time; sensor networks and satellite constellations are no exception. Instruments are replaced, orbits change, and the meaning of a measurement can drift.

### Three new sources of observation compared

Typical characteristics; individual systems vary widely

| | Satellites | Drones | Connected sensors (IoT) |
|---|---|---|---|
| **Observes** | Land, sea, buildings, light, heat, moisture | Sites, crops, structures, at very fine detail | Location, movement, temperature, use, energy |
| **Coverage** | Whole regions, repeatedly | Small areas, on demand | Wherever devices are installed |
| **Frequency** | Daily to weekly for many systems | When flown | Continuous |
| **Access** | Free public archives and commercial imagery | Own operation; flight rules apply | Usually private; some open data |
| **Main limits** | Clouds (for optical), resolution, interpretation | Range, regulation, weather | Security, privacy, uneven coverage |

Compiled from Drusch et al. (2012), Colomina and Molina (2014) and Gubbi et al. (2013)

ModQu.com

Figure 2. Three new sources of observation compared. Typical characteristics; individual systems vary widely. Compiled from Drusch et al. (2012), Colomina and Molina (2014) and Gubbi et al. (2013); table by ModQu.

## Combining with other sources

The new sources are most powerful in combination with each other and with traditional data. Goodchild (2007) described how members of the public act as "sensors", contributing observations, photographs and local knowledge that complement official and satellite data. Satellite images may show that a factory's car park is empty; a local news report, a job posting or a supplier's comment may explain why. Survey data remain essential for understanding motives and attitudes that no sensor can measure.

Jean et al. (2016) and Burke et al. (2021) both emphasise that satellite-based estimates depend on ground data for training and validation. The new sources extend the reach of traditional data; they do not replace it.

## Choosing the right source

The three technologies answer different kinds of questions, and the choice should follow the question rather than the novelty of the tool.

- **Wide area, repeated over time.** Questions about regions, such as crop conditions across a province, expansion of industrial areas or changes in shipping traffic, suit satellites, especially free archives that allow comparison over many years.

- **Fine detail at a specific site, on demand.** Questions about one's own facilities, such as the condition of a roof, the volume of a stockpile or progress on a building, suit drones.
- **Continuous measurement of known objects.** Questions about how machines, vehicles or products are performing from moment to moment suit connected sensors.
- **Activity at others' premises.** Questions about competitors' or suppliers' sites are usually best addressed with satellite imagery, public records and other open sources, rather than drones.

Cost also matters. Free medium-resolution satellite data are sufficient for many regional questions; very fine commercial imagery is expensive and worth buying only when the question requires that detail. A small pilot project that tests whether a source actually improves a forecast or decision is a sensible step before a large investment.

## Governance in practice

Organisations that adopt these sources benefit from a few simple rules agreed in advance:

1. **State the purpose.** Record what question each data source is meant to answer and who will use the results.
2. **Check the law.** Confirm aviation, privacy and contractual requirements before collecting.
3. **Minimise personal data.** Prefer aggregated counts and measurements to data about identifiable people.
4. **Secure the devices.** Change default credentials, keep software updated and separate sensor networks from core business systems.
5. **Validate regularly.** Compare outputs with ground observations or other data at set intervals, not only when results look surprising.
6. **Record uncertainty.** Report estimates with ranges and confidence, and note known weaknesses, such as cloud cover or missing sensors.
7. **Review value.** Check periodically whether the source is still improving decisions enough to justify its cost.

## Security and privacy

Connected devices create vulnerabilities. Weber (2010) identified security and privacy as central challenges for the Internet of Things, noting the need for resilience against attack, authentication of devices, access control and protection of personal data. Kolias et al. (2017) describe how the Mirai botnet took control of large numbers of poorly secured connected devices, such as cameras and routers, many still using default passwords, and used them to launch some of the largest denial-of-service attacks then recorded. A sensor network that supplies intelligence can also be a route into an organisation's systems.

Privacy risks are significant. Mayer et al. (2016) showed that telephone metadata, records of who called whom and when without any content, can reveal sensitive information such as medical conditions and religious affiliation. Location data from phones, vehicles and wearable devices can reveal where people live, work and travel. Satellite and drone imagery at high resolution can show private property and activities. Organisations using these sources must comply with privacy law, minimise the collection of personal information, aggregate data where possible and secure what they hold.

## Skills and organisation

Using these sources well requires a mix of skills that few people hold alone. Remote sensing specialists understand sensors, resolution, atmospheric correction and the limits of what an image can show. Data scientists build and test the models that detect objects and estimate quantities. Engineers install, maintain and secure sensor networks. Analysts with knowledge of the industry or region interpret what the numbers mean and connect them with other evidence. And legal and privacy advisers ensure that collection is lawful and proportionate.

Many organisations start by buying processed products from specialist providers, such as crop estimates, port activity indexes or shipment tracking, rather than building their own capability. This is often sensible, but the same questions apply to purchased data: how was it produced, how has it been validated, how does it handle gaps such as cloud cover, and how has its method changed over time? Providers that cannot answer these questions clearly are a risk. A small in-house team that understands the methods, even if it does not run them, is valuable for asking the right questions and for spotting results that do not make sense.

## Limits and pitfalls

- **Correlation without explanation.** A count of vehicles or a level of night-time light is a proxy. It may move for reasons unrelated to the activity of interest.
- **Coverage gaps.** Clouds block optical satellites; sensors are installed only where someone chose to place them; drones cover small areas.
- **Model transfer.** Algorithms trained in one place or season may fail in another.
- **Cost and expertise.** Fine-resolution imagery, processing and interpretation can be expensive and require specialist skills.
- **Commoditisation.** When many investors or competitors buy the same data, its advantage diminishes.
- **Overconfidence.** Precise-looking numbers from sophisticated systems can conceal large uncertainties.
- **Deception.** Those being observed can adapt. Activity can be moved indoors, scheduled for times when satellites are not overhead, or disguised, so an absence of visible activity is not proof that nothing is happening.

## An illustration

A Canadian grain trading company wants earlier estimates of the harvest in a major exporting region abroad, where official estimates arrive late. Its analysts use freely available satellite imagery to monitor vegetation health across the growing season, combined with weather data and historical yields. To train and test their model, they compare its estimates for previous years with the official final figures, finding that it predicts yields within a modest margin of error by mid-season, but performs poorly in years with late frost, which the imagery detects only after the damage. They add frost warnings from weather data as a separate indicator.

At home, the company installs connected temperature and moisture sensors in its own grain storage facilities, which provide early warning of spoilage. A security review leads it to place the sensors on a separate network from its business systems and to change all default passwords. The satellite estimates inform trading decisions alongside reports from local agents and official forecasts, with the analysts stating their confidence for each estimate.

## Conclusion

Satellites, drones and connected sensors have given organisations direct, often continuous observation of physical activity that once required government resources. Free satellite archives, cloud processing and machine learning have made remote sensing widely accessible; drones provide detailed views of an organisation's own operations; and connected sensors report the state of machines, shipments and products in real time. These sources become intelligence only through careful processing, validation against ground truth and combination with other evidence. They also bring security risks and privacy obligations. Used with that care, they add a powerful new layer of evidence about the physical world to the intelligence that organisations rely on.

## References

Anderson, K., & Gaston, K. J. (2013). Lightweight unmanned aerial vehicles will revolutionize spatial ecology. *Frontiers in Ecology and the Environment*, *11*(3), 138–146. https://doi.org/10.1890/120150

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Belward, A. S., & Skøien, J. O. (2015). Who launched what, when and why: Trends in global land-cover observation capacity from civilian earth observation satellites. *ISPRS Journal of Photogrammetry and Remote Sensing*, *103*, 115–128. https://doi.org/10.1016/j.isprsjprs.2014.03.009

Blumenstock, J., Cadamuro, G., & On, R. (2015). Predicting poverty and wealth from mobile phone metadata. *Science*, *350*(6264), 1073–1076. https://doi.org/10.1126/science.aac4420

Burke, M., Driscoll, A., Lobell, D. B., & Ermon, S. (2021). Using satellite imagery to understand and promote sustainable development. *Science*, *371*(6535), Article eabe8628. https://doi.org/10.1126/science.abe8628

Colomina, I., & Molina, P. (2014). Unmanned aerial systems for photogrammetry and remote sensing: A review. *ISPRS Journal of Photogrammetry and Remote Sensing*, *92*, 79–97. https://doi.org/10.1016/j.isprsjprs.2014.02.013

Day, D. A., Logsdon, J. M., & Latell, B. (Eds.). (1998). *Eye in the sky: The story of the Corona spy satellites*. Smithsonian Institution Press.

Donaldson, D., & Storeygard, A. (2016). The view from above: Applications of satellite data in economics. *Journal of Economic Perspectives*, *30*(4), 171–198. https://doi.org/10.1257/jep.30.4.171

Drusch, M., Del Bello, U., Carlier, S., Colin, O., Fernandez, V., Gascon, F., Hoersch, B., Isola, C., Laberinti, P., Martimort, P., Meygret, A., Spoto, F., Sy, O., Marchese, F., & Bargellini, P. (2012). Sentinel-2: ESA's optical high-resolution mission for GMES operational services. *Remote Sensing of Environment*, *120*, 25–36. https://doi.org/10.1016/j.rse.2011.11.026

Floreano, D., & Wood, R. J. (2015). Science, technology and the future of small autonomous drones. *Nature, 521*(7553), 460–466. https://doi.org/10.1038/nature14542

Goodchild, M. F. (2007). Citizens as sensors: The world of volunteered geography. *GeoJournal, 69*(4), 211–221. https://doi.org/10.1007/s10708-007-9111-y

Gorelick, N., Hancher, M., Dixon, M., Ilyushchenko, S., Thau, D., & Moore, R. (2017). Google Earth Engine: Planetary-scale geospatial analysis for everyone. *Remote Sensing of Environment, 202*, 18–27. https://doi.org/10.1016/j.rse.2017.06.031

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

Henderson, J. V., Storeygard, A., & Weil, D. N. (2012). Measuring economic growth from outer space. *American Economic Review, 102*(2), 994–1028. https://doi.org/10.1257/aer.102.2.994

Jean, N., Burke, M., Xie, M., Davis, W. M., Lobell, D. B., & Ermon, S. (2016). Combining satellite imagery and machine learning to predict poverty. *Science, 353*(6301), 790–794. https://doi.org/10.1126/science.aaf7894

Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal, 79*(1), 1–14. https://doi.org/10.1007/s10708-013-9516-8

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer, 50*(7), 80–84. https://doi.org/10.1109/MC.2017.201

Mayer, J., Mutchler, P., & Mitchell, J. C. (2016). Evaluating the privacy properties of telephone metadata. *Proceedings of the National Academy of Sciences, 113*(20), 5536–5541. https://doi.org/10.1073/pnas.1508081113

Moreira, A., Prats-Iraola, P., Younis, M., Krieger, G., Hajnsek, I., & Papathanassiou, K. P. (2013). A tutorial on synthetic aperture radar. *IEEE Geoscience and Remote Sensing Magazine, 1*(1), 6–43. https://doi.org/10.1109/MGRS.2013.2248301

Salganik, M. J. (2018). *Bit by bit: Social research in the digital age*. Princeton University Press.

Weber, R. H. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review, 26*(1), 23–30. https://doi.org/10.1016/j.clsr.2009.11.008

Wulder, M. A., Loveland, T. R., Roy, D. P., Crawford, C. J., Masek, J. G., Woodcock, C. E., Allen, R. G., Anderson, M. C., Belward, A. S., Cohen, W. B., Dwyer, J., Erb, A., Gao, F., Griffiths, P., Helder, D., Hermosilla, T., Hipple, J. D., Hostert, P., Hughes, M. J., ... Zhu, Z. (2019). Current status of Landsat program, science, and applications. *Remote Sensing of Environment, 225*, 127–147. https://doi.org/10.1016/j.rse.2019.02.015

Zhu, C. (2019). Big data as a governance mechanism. *Review of Financial Studies*, *32*(5), 2021–2061. https://doi.org/10.1093/rfs/hhy081

Zhu, X. X., Tuia, D., Mou, L., Xia, G.-S., Zhang, L., Xu, F., & Fraundorfer, F. (2017). Deep learning in remote sensing: A comprehensive review and list of resources. *IEEE Geoscience and Remote Sensing Magazine*, *5*(4), 8–36. https://doi.org/10.1109/MGRS.2017.2762307