INTELLIGENCE · ORGANISATIONAL INTELLIGENCE

The Future of Intelligence in a Data-Saturated World

Intelligence work was built for a world where information was scarce. Today the problem is abundance. This article looks at how data saturation, open sources and artificial intelligence are changing intelligence work, what will stay the same, and how organisations can prepare.

ModQu research article · 1,842 words · 19 references (APA 7th edition)

For most of its history, intelligence work was organised around scarcity. Useful information was hard to obtain, and much of the effort of an intelligence service, or a company's market research team, went into collecting it. That world has gone. Satellite images can be bought by the square kilometre, social media produces billions of posts a day, companies publish detailed data about themselves, and sensors in phones, vehicles and factories record activity continuously. Zegart (2022) argues that this shift, together with advances in computing, is the biggest change in the intelligence environment since the start of the Cold War.

This article looks at what data saturation means for intelligence work: what changes, what stays the same, and how organisations can prepare. It draws on government intelligence, where these questions have been studied most closely, but the lessons apply equally to businesses.

From scarcity to abundance

When information is scarce, the main question is how to get it. When it is abundant, the main questions become which information matters, whether it can be trusted and what it means. Omand (2010) describes a move from intelligence based mainly on secret sources to intelligence that combines secret and open material, much of it held by private companies rather than governments. Williams and Blum (2018) describe a "second generation" of open source intelligence, in which commercial imagery, online data and automated tools give analysts access to information that once required secret collection.

Abundance has three main consequences. First, collection is no longer the bottleneck; analysis and attention are. Second, the intelligence service or team no longer has privileged access to much of what matters; journalists, researchers, companies and citizens can see the same data. Third, the volume of material makes it easier to find support for almost any conclusion, which raises the risk of confirmation bias and of false confidence.

Information overload

People cannot absorb unlimited information. Edmunds and Morris (2000), reviewing research on business organisations, found that information overload is widespread and is associated with stress, poor decisions and wasted time. More information does not always lead to better judgements; beyond a point, it leads to worse ones, as people struggle to separate signal from noise and fall back on simple rules.

For intelligence teams, overload affects both analysts and users. Analysts can spend their time processing material rather than thinking about it. Users can receive more reports than they can read. Lowenthal (2022) notes that policymakers often feel overwhelmed by intelligence products, and that the most valued products are short and focused. In a data-saturated world, the value of intelligence lies increasingly in selection and synthesis: telling the reader what matters and what can be ignored.

From scarcity to abundance

How the conditions of intelligence work are changing

	Scarce information	Abundant information
Main constraint	Collection: getting the data	Attention: choosing what matters
Main skill	Gaining access	Selecting, verifying, synthesising
Key sources	Secret and specialist	Open, commercial and automated
Main risk	Missing information	Noise, deception, false confidence
Role of machines	Storage and search	Sorting, translating, flagging
Value to users	Exclusive access	Judgement and explanation

Compiled from Omand (2010), Zegart (2022) and Williams and Blum (2018); table by ModQu

ModQu.com

Figure 1. From scarcity to abundance. The constraint moves from collection to attention, and the main value moves from access to judgement. Compiled from Omand (2010), Zegart (2022) and Williams and Blum (2018); table by ModQu.

Artificial intelligence and automation

Artificial intelligence (AI) is the obvious response to data saturation. Machine learning can sort, translate, transcribe and classify material far faster than people, flag anomalies in large datasets and recognise objects in images. The National Security Commission on Artificial Intelligence (2021) in the United States concluded that AI would transform

intelligence work and urged agencies to adopt it quickly. In the United Kingdom, Babuta et al. (2020) identified similar opportunities, particularly in processing large volumes of data, while stressing the need for human oversight, legal safeguards and attention to bias.

It is important to be clear about what current AI does well and what it does not. Russell and Norvig (2021) describe most practical AI as pattern recognition learned from data. Brynjolfsson and Mitchell (2017) suggest that tasks suited to machine learning are those with clear inputs and outputs, large amounts of training data and tolerance for occasional error. Many intelligence tasks fit this description: translating documents, identifying vehicles in imagery, grouping similar news stories. Others do not: judging the intentions of a competitor's leadership, assessing whether a source is lying, or deciding what a decision-maker needs to know. These depend on context, judgement and understanding of people.

The likely future, therefore, is not replacement of analysts but a changed division of labour. Malone (2018) describes "superminds", groups of people and computers working together, which can be more capable than either alone. Machines handle volume, speed and consistency; people handle meaning, judgement and communication with users. The skill of the analyst shifts towards framing questions, checking machine output and explaining conclusions.

New risks

Abundance and automation bring new risks as well as new capabilities.

Deception and manipulation. When anyone can publish, false information spreads easily, and generative AI makes convincing fakes cheap to produce. Images, documents and recordings can no longer be trusted on sight. Zegart (2022) warns that intelligence organisations will increasingly need to verify the authenticity of material, not just interpret it.

Automation bias. People tend to trust machine outputs too much, especially when they cannot see how the result was produced. An analyst who accepts an algorithm's classification without checking may pass on errors with unwarranted confidence. Babuta et al. (2020) stress that human judgement must remain meaningful, not a rubber stamp.

Loss of expertise. If machines do the routine work, analysts may have fewer opportunities to build the deep knowledge that comes from reading primary material. Organisations need to protect time for analysts to develop expertise.

Privacy and legitimacy. The same data that helps intelligence teams describes real people. Collecting and combining it raises legal and ethical questions. Omand (2010) argues that intelligence agencies keep public trust only if their methods are seen as necessary and proportionate; businesses face the same test with customers and regulators.

What stays the same

Despite these changes, much of intelligence work endures. Its purpose is still to reduce uncertainty for decision-makers, as Fingar (2011) puts it, by providing timely, relevant and objective assessments. It still depends on understanding what users need. Kerbel and Olcott (2010) argue that analysts should work with their users to make sense of situations, rather than delivering finished products from a distance; this becomes more important, not less, when users can access raw data themselves.

The traditional intelligence cycle of direction, collection, processing, analysis and dissemination has long been criticised as too linear (Hulnick, 2006; Phythian, 2013). In a data-saturated world it fits even less well, since collection is continuous and users often access information directly. Yet the questions the cycle poses remain: what do we need to know, where can we find it, what does it mean, and who needs to hear it? Gill and Phythian (2018) suggest viewing intelligence as a web of activities rather than a cycle, which better fits a world in which data flows constantly.

Above all, judgement remains central. Tetlock and Gardner (2015) found that the best forecasters are not those with the most information but those who think carefully, update their views in response to evidence and express uncertainty precisely. Mellers et al. (2014) showed that training, teamwork and tracking of accuracy improved forecasting performance substantially. These are human skills, and they matter more when data is abundant.

Lessons from past failures

History suggests that new technology does not by itself prevent intelligence failures. Zegart (2007) showed that the American intelligence community had relevant information before the attacks of 11 September 2001, but organisational problems, such as poor sharing between agencies and outdated structures, prevented it from being used. Data saturation could make this problem worse: the relevant signal may be present but buried among millions of irrelevant items, or held by an organisation that does not know it matters. Agrell and Treverton (2015) argue that intelligence must learn from science in testing ideas against evidence and in being open about uncertainty, habits that become more important as data grows.

Preparing for the future

Organisations that want their intelligence functions to thrive in a data-saturated world can take several practical steps.

1. **Focus on questions, not data.** Start with the decisions users face and the questions that matter most, and collect and analyse data to answer them, rather than gathering data in the hope it will prove useful.
2. **Invest in synthesis.** Value products that select and explain. Short, clear assessments that tell users what matters are worth more than comprehensive reports that nobody reads.
3. **Use automation for volume.** Apply machine tools to translation, sorting, monitoring and anomaly detection, freeing analysts for judgement.
4. **Keep people in the loop.** Require analysts to check and explain machine outputs, and record when they disagree with them.
5. **Build verification skills.** Train analysts to check the authenticity and provenance of images, documents and online material.
6. **Track accuracy.** Record forecasts and judgements and compare them with outcomes, so that the organisation learns which methods and sources work.
7. **Govern data use.** Establish clear rules for what data may be collected and combined, with attention to privacy, law and public trust.
8. **Protect expertise.** Give analysts time to develop deep knowledge of their subjects, not just to process the daily flow.

A business illustration

A consumer goods company once relied on quarterly market research reports and a small team that read trade press. Today it has access to real-time sales data, social media monitoring, online reviews, search trends and web-scraped competitor prices. At first, the intelligence team simply passes more data to managers, in the form of dashboards and daily alerts. Managers complain that they are overwhelmed and still do not know what matters.

The team changes approach. It agrees with senior managers on a short list of key questions, such as whether a new competitor brand is gaining share and whether a price rise will hold. It uses automated tools to monitor relevant data and flag significant changes, and analysts spend their time interpreting those changes and writing short weekly assessments. Each assessment states what has changed, what it means for the key questions and how confident the team is. The team records its forecasts and reviews them each quarter. Managers now receive less material but find it far more useful.

Common mistakes

- **Confusing more data with better intelligence.** Volume without focus increases noise and confusion.
- **Treating AI as an oracle.** Machine outputs need checking, context and explanation.
- **Neglecting verification.** Material found online may be false, manipulated or out of date.
- **Ignoring the user.** When users can see raw data themselves, intelligence must add interpretation they cannot easily produce.
- **Forgetting governance.** Using data in ways customers or the public see as intrusive can damage trust and invite regulation.

Conclusion

The future of intelligence in a data-saturated world is not a future without analysts. It is one in which collection matters less and judgement matters more. Machines will handle much of the volume, but people will still need to decide what questions matter, check whether information is true, understand what it means and explain it clearly to those who must act. Organisations that focus on these skills, use automation wisely and govern their data use carefully will turn abundance into advantage. Those that simply collect more will drown in it.

References

Agrell, W., & Treverton, G. F. (2015). *National intelligence and science: Beyond the great divide in analysis and policy*. Oxford University Press.

Babuta, A., Oswald, M., & Janjeva, A. (2020). *Artificial intelligence and UK national security: Policy considerations* (Occasional Paper). Royal United Services Institute.

Brynjolfsson, E., & Mitchell, T. (2017). What can machine learning do? Workforce implications. *Science*, *358*(6370), 1530–1534. https://doi.org/10.1126/science.aap8062

Edmunds, A., & Morris, A. (2000). The problem of information overload in business organisations: A review of the literature. *International Journal of Information Management, 20*(1), 17–28. https://doi.org/10.1016/S0268-4012(99)00051-1

Fingar, T. (2011). *Reducing uncertainty: Intelligence analysis and national security*. Stanford University Press.

Gill, P., & Phythian, M. (2018). *Intelligence in an insecure world* (3rd ed.). Polity Press.

Hulnick, A. S. (2006). What's wrong with the intelligence cycle. *Intelligence and National Security, 21*(6), 959–979. https://doi.org/10.1080/02684520601046291

Kerbel, J., & Olcott, A. (2010). Synthesizing with clients, not analyzing for customers. *Studies in Intelligence, 54*(4), 11–27.

Lowenthal, M. M. (2022). *Intelligence: From secrets to policy* (9th ed.). CQ Press.

Malone, T. W. (2018). *Superminds: The surprising power of people and computers thinking together*. Little, Brown.

Mellers, B., Ungar, L., Baron, J., Ramos, J., Gurcay, B., Fincher, K., Scott, S. E., Moore, D., Atanasov, P., Swift, S. A., Murray, T., Stone, E., & Tetlock, P. E. (2014). Psychological strategies for winning a geopolitical forecasting tournament. *Psychological Science, 25*(5), 1106–1115. https://doi.org/10.1177/0956797614524255

National Security Commission on Artificial Intelligence. (2021). *Final report*.

Omand, D. (2010). *Securing the state*. Hurst.

Phythian, M. (Ed.). (2013). *Understanding the intelligence cycle*. Routledge. https://doi.org/10.4324/9780203558478

Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.

Tetlock, P. E., & Gardner, D. (2015). *Superforecasting: The art and science of prediction*. Crown.

Williams, H. J., & Blum, I. (2018). *Defining second generation open source intelligence (OSINT) for the defense enterprise* (Report RR-1964-OSD). RAND Corporation.

Zegart, A. B. (2007). *Spying blind: The CIA, the FBI, and the origins of 9/11*. Princeton University Press.

Zegart, A. B. (2022). *Spies, lies, and algorithms: The history and future of American intelligence*. Princeton University Press.