REGULATORY INTELLIGENCE TRAINING – A NEW FRONTIER FOR EDUCATORS

Neil QUARMBY*

Abstract

Education in intelligence and analysis has traditionally been oriented towards national security and more recently law enforcement. Reforms in personal and business behaviours are driving the need for improved regulatory systems in the Western world, which is also creating an imperative to build professional intelligence capability and networks across new areas of government and industry.

Keywords: *intelligence, regulation, supervision, compliance, prevention, risk.*

Introduction

Regulation, licensing, supervision, monitoring, inspection, compliance, safety investigation, accreditation … all representative of the broad church of government and organisational controls reflected in this paper as "Regulation". They all have a core determinant: assessing and monitoring the performance of participants in a government defined area of risk that has socially or legally sanctioned rules for appropriate behaviours. The aim: to prevent harms to people and business. (Sparrow, 2008)

* Neil Quarmby is the chief executive of Intelligence Rising, a consultancy and online training company in intelligence. His career spans over twenty years in Defence intelligence, law enforcement intelligence, and he has led three regulators in three different government sectors. He has published two books on intelligence and is affiliated with Macquarie University, Australia. He can be contacted through contact@intelligencerising.com.

The scale and complexity of regulation on peoples' lives is daunting. The effectiveness of regulatory controls has even become a key measure of a nation's status as a modern economy. Hence there can be an apparently limitless number of regulators, ranging from several staff to major government departments. The scale of preventable harm is also daunting – and touches everyone daily in the costs of living, doing business and in injury and death.

Contemporary intelligence thinking is being propelled into the world of regulation by: negative performance reviews of regulators; new leadership intent on achieving a sense of public value; the idea of connected government; and demands for more efficient targeting of resources at risks. Yet there remain sizeable barriers in regulation to intelligence capacity-building. Some of these barriers are legislated while others relate to the nature and scale of the data held by regulators. However, the most significant barrier relates to cultures within regulators themselves and the government they provide assurance services to.

One key issue is that regulators are not supported academically – like national security and law enforcement – as there is no active debate on targeting intelligence practices, detection thresholds, surveillance, and counterintelligence. There is a general absence of intelligence as a discipline across the broad expanse of regulatory entities. Globally, academic, judicial and government reviews of regulatory failure rarely mention the word intelligence. Recent reviews of failures of financial and banking system oversight (supervision) observe failures in monitoring, targeting, indications and warnings, and threat assessment of the culture of financial organisations. Regulators have been publically flogged for their focus on financial performance data. Yet the term intelligence is rarely used in the findings of failure.[1]

Hence, this paper foresees a growing demand on the intelligence profession over the next twenty years for core skills and expertise to be transitioned into the varied arms of state regulation and commercial compliance; similar to the journey started by law enforcement internationally twenty years ago. The paper explores the number of

[1] An example capturing a range of reviews of the performance of European and Australian regulators is in Hane (2019, pp. 337-385).

inherent cultural and structural barriers to the easy adoption of intelligence-led decision-making in this broad sector and presents some observations on the types of focus areas to address this new and exciting challenge for education and training systems.

Definition

For the purposes of this paper, the term 'regulatory intelligence' can be viewed as: involving the systematic collection, identification and analysis of behaviour, important hazards, risks, or patterns of non-compliance for regulatory decisions. (Sparrow, 2000, p. 100. Quarmby & Young, 2010, pp. 3-4)

The world of regulation

Taking a helicopter view of regulation, the scope can be viewed as too large for a simple education framework. The scale of law enforcement tends to outweigh national security and the scale of regulation outweighs law enforcement in fully modernised countries. All markets and sectors have rules regulating interaction between private actors or the interaction between private actors and government. Regulations also cover how government departments and agencies interact between themselves – and hence there may even be government watchdogs oversighting government officials. In the traditional national security view of intelligence, the less trusted states are those with few internal, public, regulatory controls in place.

Modern economies have a plethora of ombudsman, audit, complaints management, protection, security, and review bodies. The scope can also be expanded to include self-regulating market bodies such as professional associations (peak bodies and representative bodies) that accredit members and investigate performance; such as medical practitioner associations and legal professional bodies. In some cases, these representative bodies may themselves be subject to government regulation.

In the work-place, there are code-of-conduct measures imposed by employers subject to varying levels of investigation. In turn, there are appeals mechanisms for complaints against such systems, subject to

review by external intermediary and/or investigative bodies. Just when you think you can escape such codified behaviour, your home may also have rules and standards – some of which are self-imposed but others may be highly codified by society; for example, how you get rid of your waste.

Regulators obtain and generate staggering amounts of information and data needed to support the decisions they make to reduce harm. 'Harm' is used in this paper in the broadest of senses and relates to the primary prevention purpose of all regulators. Harm may refer to the impact of poor behaviours on systems integrity, travel controls, identity security, market equity and integrity, public health and safety, environmental stewardship, corruption control, personal integrity, and transaction integrity. (Sparrow, 2008, pp. 1-2) Reputational harm leading to loss of public confidence in a market sector is also often a crucial factor; for example in banking and business behaviours.

The complexity multiplies on a scale of national harm. From a social perspective, more people die in preventable circumstances in the domain of regulation than in the domain of crime (Quarmby 2018, p. 5). On a financial scale, more tax-dollars are lost to noncompliance and incorrect or inappropriate practices than criminality. The global financial crisis of 2007-09 was attributed in part to the many regulators' reduction in regulatory oversight and subsequent failures "to monitor individual financial institutions and individuals" (Black, 2011, p. 1). A recent Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry in Australia, reflected on previous work done in improving the supervision of banks in Europe; especially in the Netherlands and under the auspices of the G20. The Royal Commission found significant weaknesses in the regulatory system leading to financial and social harms. The result: loss of confidence in the banking sector and billions of dollars required to be paid in reparations. (Hane 2019, p. 37)

While the Commission identified regulatory failures in monitoring and detection, the word 'intelligence' is never used in the Royal Commission's findings – as it would be if the problem was deemed a national security issue. In reflecting on this failure, the

Commission notes the absence of learning from international experience. For example, the financial crisis in Dutch banks led to the regulatory arm of the De Nederlandsche Bank (DNB) introducing a regime of assessments of behaviour and culture in the institutions within its regulatory coverage. The DNB's program has been developed on the idea that '[c]ulture and behaviour are essential elements for financial and prudential supervision, since the behaviour and culture of a financial organisation influence its financial and organisational performance'. By 2015, the DNB conducted 52 assessments of 'banks, insurance companies, pension funds and trust offices'. Most assessments focused on senior management. According to the DNB, more than half of the boards assessed 'showed serious problems with regard to their board culture'. (Hane 2019, pp. 377-9)

Drivers for investment in intelligence tradecraft

Given this sense of harm and the clear relevance of intelligence tradecraft, it remains surprising that few areas of regulation appear to attract serious intelligence investment. Certainly, revenue regulation and assuring welfare payments tends to attract investment by government in control and targeting measures due to the considerable impacts on the public purse. In Australia, the government revenue regulator (the Australian Tax Office [ATO]) identifies a key task is to work "with other Australian Government agencies to deliver services; share data, intelligence and expertise; and participate in multi-agency taskforces." The ATO reports it has 115 Memorandums of Understanding (MOUs) in place with other Australian government agencies and bodies (federal, state, territory and local) to manage this function. (Commissioner of Taxation, Annual report, p. 17)

Finance and Tax regimes have tended to attract a greater proportion of intelligence expertise due to undercurrents of crime and the national security agenda. Other major regulatory arms with significant harm issues such as Health regulation are lagging internationally. 'Health intelligence' more often means statistics on a morbidity factor. While there are more financial costs and human costs arising from failure in Health regulation than there will ever be in national security and revenue regulation, this regulatory sector tends to

remain impervious to contemporary intelligence practices, and hence investment is data-centric and meaning-limited.

The value of centralised intelligence centres, able to acquire and fuse multi-source information for the benefit of connected intelligence capability in supported business lines, is ingrained in national security and has come late to law enforcement. In the US – with some 17,000 law enforcement bodies (including very many regulatory bodies) – there are approximately 75 fusion centres attempting to share information and intelligence across the security, crime and public safety divides (Ratcliffe 2016, p. 21). Such centres do not occur naturally in regulation without a push from national security entities or crime fighting bodies. There remain significant barriers to implementing such innovative ideas within regulatory circles.

As a sample, the 'public face' of 58 international regulators was reviewed by the author as to whether they advertised their regulatory approach as incorporating intelligence practices. 16 out of 58 had a publically stated approach to operations that intelligence practitioners could vaguely associate with (Quarmby 2018, p. 51). Only three of the 58 regulators – at the time of review – had a publically stated approach to targeting behaviour that appears to be in tune with contemporary intelligence-led theory and practice (Quarmby 2018, p. 53).

The public would assume that, where regulators operated in similar jurisdictions (for example with common participants and like harms), regulators would adopt consistent approaches to targeting harm. In national security circles this is often referred to as interoperability. However, the study showed that consistency should not be assumed. Dissimilar regulatory philosophy and approaches between agencies tends to create barriers to sharing information and intelligence. Meaning that - even in like sectors where they have to deal with a common problem – regulators struggle to share crucial intelligence without the same language to assess and define problems (Quarmby 2018, p. 52).

So … what is different about regulatory intelligence for educators of intelligence?

The educational institutions are absent: Much of the world's contemporary education of intelligence has its foundations in international relations. Early academic texts placed intelligence firmly in the domain of supporting decisions about foreign threats. Much of debate therefore tends to be about how independent the intelligence system should be from the policy-makers (Davis, The Kent-Kendall Debate of 1949). Hence the rationale for intelligence education is usually perceived in the Machiavellian tradition of understanding inter and intra state threats, and protections for people in a national security construct. The academic pursuit becomes one of understanding whether intelligence is best understood as a manifestation of realpolitik, neo liberal perspectives, neo Marxist/culturalism views, or even through the recent constructivists who have a more practical, inter-state problem-solving approach to education. The shape of such academic pursuit is strategic in nature. Given, the vast majority of intelligence officer jobs are tactical, such an academic prism is only viable where the core of intelligence officer tradecraft exists in the training regimes of those agencies affiliated with national security.[2] Academia then provides a more foundational, strategic capacity outcome. This education structure allows education in academia to focus on strategic intelligence roles and analytical tools relevant for the study of wicked international relations problems.

That is the theory … however; the nature of academic tradition can confuse the theory. In the US, intelligence education arose to assist the growth of large numbers of strategic analysts from within the international politics domain and later gained traction in criminology studies. In Australasia, intelligence education was initially driven by Universities' Criminal and Justice Departments from the 1990s, with then a later take-up in International Politics Departments. Here the

[2] Numerous works by Bob de Graaff on intelligence highlight this tradition through Europe. One work notes a driver from the military to enhance academic intelligence training in the Netherlands and not to duplicate the training work of the services (de Graaff 2013, p. 88-9).

tradition is more social and humanist than political.[3] More recently Information Technology Departments are growing their intelligence and counterintelligence expertise to ultimately challenge the intellectual ownership of intelligence – but based on a scientific and mathematical tradition.

The nature of internal to agency training capacity also confuses the education continuum. For example, there has been a general absence of a training capability within justice/policing agencies to grow intelligence officers. Where internal-to-agency intelligence training exists, it may focus on the type of IT analytical support tools used by that enforcement arm. Many Western policing departments/agencies may not allow intelligence officers to be involved in what are the traditional collection practices of intelligence. Rather, their intelligence staff are contained to only analytical roles.

Hence, there has been a natural problem in university justice courses attempting to adopt the structured analytical approaches used in national security without pre-existing tactical intelligence and decision-making DNA in place within the police forces serviced. The outcome is cognitive dissonance. For example, police workplaces not liking to employ intelligence students who have been focussed on the analysis of strategic problems far removed from their daily tactical work in criminal intelligence. Also the students themselves may not be able to relate academic study to the volume of tactical work faced by them in their justice or enforcement roles. For both employer and employee, the intelligence cycle may not be considered relevant – only the analytical segment.

While there are educational issues for law enforcement in linking their own internal training to the broader education offering of universities, the problem compounds for regulators who have little internal training and no university departmental alignment. The growing number of regulators seeking to professionally develop their analytics staff has few places to turn. What is worse, is the converging influence of data analytics and a pervasive view that regulators may only make decisions on data or evidence, and means regulators seek to

[3] For a history of the rise of intelligence practices in law enforcement see Ratcliffe (2016).

fill this void through education in the data sciences. Hence, many information systems or legal/justice studies departments in universities are seizing the education ground on intelligence; however, the view of intelligence is one of managing the system to share data, to store data, to match and collate data, and to report data.

Poor design in regulation does not help! Regulatory systems are characterised by the law that authorises action, the participants being regulated, the capabilities of the regulated, others impacted by regulation, the policy and political stewards of the system, the legal sector and representative groups of various parties. The interplay between these various elements is often referred to as the 'regulatory scheme'. (Quarmby 2018, pp. 66-68)

The design of regulatory schemes drives a lot of regulatory culture that flows through operations and intelligence. It is interesting that medical practitioners defrauding or conducting noncompliant billing in the USA are targeted by the FBI within an enforcement context. In Australia, the same targeting is conducted by a non-statutory regulator (and one that bounces between polar views of itself as a regulator or an internal public service assurance body). Hence the design itself sends a clear message as to public acceptability of what is tolerated. Where corruption and black-markets operate in normal business transactions, less meaningful regulatory systems will be in-place and certainly no regulatory intelligence system will be in-place.

A well designed regulatory scheme would include the right level of information access to enable the regulator to monitor performance and behaviour. Unfortunately, very few regulatory schemes are designed with intelligence functions in mind. Most have an overriding focus on how specific enforcement tools or powers can be used. This is important work, but tends to leave regulators with authorising environments representative of 20th century law enforcement approaches and not 21st century contemporary regulatory practices. Worse case, design inhibits the regulator's ability from the outset to monitor those areas of behaviours and risks likely to generate the most harm.

Sparrow in his seminal work on the Character of Harms (Sparrow 2008), outlines a number of approaches regulators take from being: Type 1 prescriptive and rules-based; to Type 4 no real oversight;

through various iterations between these polar opposites. These models can be characterized as shown in the figure below.

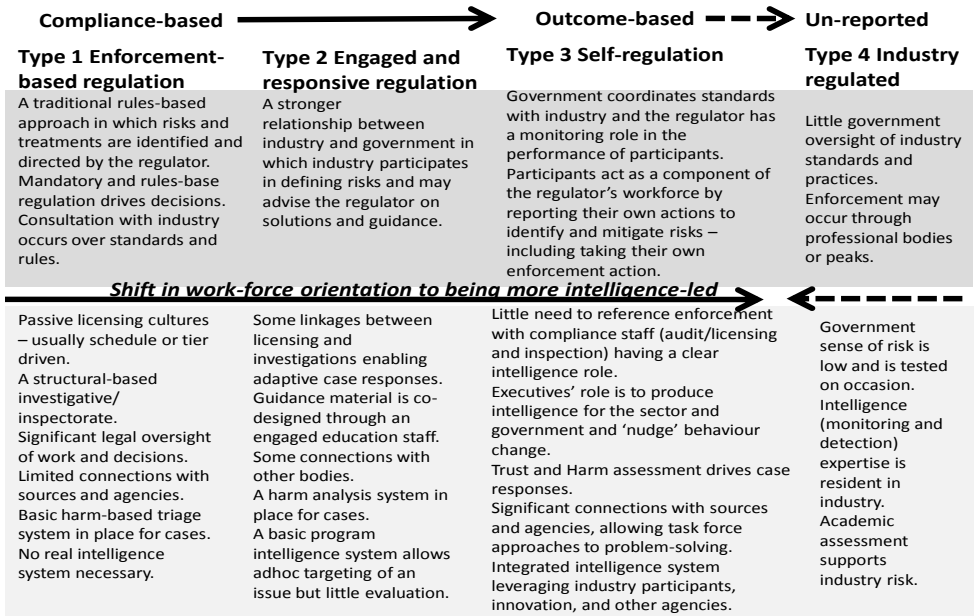

Figure 1: Stewardship models of regulation taken from Quarmby (2018, p. 109).

These models are especially useful in starting the discussion about the nature, type and scope of capacity building needed in the regulator. Most regulators and scheme stewards will aspire to the third model. They are wary of the fourth due to systemic failures and lack of transparency and protections. They are wary of the first due to the connotations of being anti-business and pro-red tape. Often the models are proposed simplistically; that is, a regulator can only be one or the other. In the author's experience most regulators will have market segments necessitating a variance in approach across this scale. At the same time, it is the author's experience that most regulators cannot clearly articulate (as a unified voice) what approach they have to these different market segments.

The most important and fundamental aspect to these four models that is lost in most contemporary literature is that the workforce as well as the culture changes markedly as regulators shifts from Type 1 to 4. These implications are covered in detail in *Intelligence in Regulation* (Quarmby 2018, pp. 109-122). Suffice for educators to know they need to discuss the shape of intelligence arising from the culture of the regulator and the key shifts in intelligence work depending on this culture. For example, a critical shift for regulators seeking to be more of a Type 3 regulator is the necessity to understand what good behaviour looks like and how best to adjust it and reinforce it. National security and police intelligence officers have extensive professional expertise in analysing bad behaviours; but good behaviour? Not so much. National security success can be measured in identifying and dealing with threats. Regulatory success can be measured in expanding the growth of the compliant and better practice participants to achieve a social end-state in which the regulator is no longer required and behaviour is self-policed and self-reinforcing.

Transparency and the relationship with policy making: There are two other major departures from traditional intelligence perspectives worth noting. The first is the element of transparency. National security and police intelligence operates in a carefully controlled environment due to very real counterintelligence risks and due to the sensitive nature of many sources. In regulation, often the most important tool to sustain good behaviour is through public engagement and public reporting on performance. Indeed there is a public expectation for regulators to report on the performance of their jurisdiction and the types of harm manifesting. Hence in Type 3 regulator there should be a clear shift to visibility and openness that is often uncomfortable for traditional compliance and intelligence staff.

The second is the relationship to policy. As noted earlier, traditional academic study into intelligence fusses over the independence of the intelligence officer from the policy officer. This means there is little doctrinal support for intelligence reports providing recommendations. In regulation the issue is compounded as often it is weaknesses in regulatory response or policy controls that allow noncompliant behaviours to manifest. Deeming government policy to

be the most important threat factor can be career limiting; however, very necessary in regulatory intelligence work!

Barriers to be understood by educators

Organisational culture and the absence of decision-making DNA: To explore approaches to educate intelligence officers working in the regulatory and compliance world, academic institutions and trainers need to understand the barriers to employing such expertise. These are covered at length in Intelligence in Regulation (Quarmby 2018, pp. 7-64). In short, these barriers include the conservative culture of many regulators. Passive rules-based obsession is not normally conducive to encouraging the creativity and networking necessary for a contemporary intelligence culture. Also the data-centric nature of regulators tends to confuse contemporary intelligence thinking with that of data analytics and business intelligence.

For many regulators, understanding the intelligence function is problematic because of the absence of 'direction'. Regulatory decision-making is often case specific. Hence the term 'strategic' may be used in regulators for those big cases that have reputational risks. In many regulators, key case decisions related to licensing, audit programs, the use of powers, campaigning and enforcement responses are made at the highest levels. Such decision-making is often (and quite necessarily) guarded by legally formatted and contestable process requiring hard evidence. Speculation may be spurned.

Where there is little organisational space for strategic and operational level decisions, the intelligence function is most often subsumed by business intelligence or data analytics functions. Here, analysis is reduced to reporting known statistics and may even be overshadowed by internal performance reporting. Hence, creative innovators seeking to source new data and information get frustrated in regulators; especially where the perception internally is that additional information from other sources cannot be used in legally defined decision processes (Quarmby, 2018 pp. 44-5).

Where regulators do recognise the value of other sources, intelligence may be considered an IT problem; about the sourcing and integration of data. This may lead to structural and functional

uncertainty as to whether analysis of data is best placed as a corporate rather than a business function, and also may lead to expensive solutions for otherwise simple problems.

For educators, an intelligence capability needs to be present in regulators for the type of behavioural analysis that will drive successful domestic policy and targeting decisions.

- It needs to be present to support strategic thinking on the future connections between law reform, public value shifts, and operational capability development.
- It needs to be present to assist decision-makers seeking an appropriate response to a behavioural problem (operational decision-making) within their jurisdiction.
- It needs to be present to allow compliance case management to select and use the appropriate tool in responding to a case (tactical intelligence).

Absence of scholarly support: The academic view of regulation is yet to mature and explore the concept of improving decision-making through enhanced intelligence systems. Rather the focus to date has been on responding at the case/incident level (Quarmby 2018, p. 46). The intellectual discourse for intelligence in regulation is non-existent in comparison to both law enforcement and national security. In the few volumes of good academic writing on regulation, there is very little mention of intelligence and decision support. Even Sparrow's seminal works are light on the subject (Sparrow 2000 and 2008). Baldwin and Black (2007) also comment on this general literary absence.

Recruitment of people into regulatory positions often follows the literal interpretation of the authorising environment and not the subtleties of creative problem-solving imposed by contemporary thinking. Hence, regulators tend to recruit from industry or recruit operational people specific to their statutory functions of audit, inspection, complaints handling, investigation, information management etc. Complicating matters, there is very little in the way of educational pathways for regulators through universities or public service training regimes. Such pathways could assist people from various backgrounds to professionalise as a regulatory leader.

Within such a context, it is easy to see why many regulators have internal cultures not conducive to contemporary intelligence design and indeed how they get caught 'not knowing' what is clear and obvious.

The most public failures internationally include the 2007-09 Global Financial Crisis and the Deepwater Horizon drilling disaster in the US in 2010 and both have been extensively examined. As Julia Black notes: *"The nature and reasons for the failures are extensive, but were largely common to regulators and market participants alike. Many of these were cognitive: fundamental failures of regulators as to how the markets were operating…"* (Black, 2011)

Every country has these regulatory failures and lack of knowledge or ability to harness information is often a key symptom. Underneath, there is often more of a dynamic of poor decision-making that has precluded investment in contemporary intelligence.

With such evident and catastrophic failures, why the lack of interest from intelligence and academic professions? Low likelihood + high consequence events are the core analytical grist of the national security intelligence arena. These are often attractive and intellectually stimulating for many analytically minded people. Conversely, the daily grist of analysing our own behaviours that undermine our ability to govern our own transactions is far less intellectually stimulating.

An absence of tradecraft: 'Direction' and artistry in driving an intelligence cycle demands intelligence trade craft in collection management. In national security, education in this art is usually the accountability of service or intelligence agency internal training programs. Hence – as noted earlier – there is foundation education that can rationalise the academic focus on strategic international problem-solving along a broader training to education continuum.

In regulation and law enforcement, the academia focus on training staff as just strategic analysts can be calamitous for their burgeoning intelligence profession.

Intelligence officers will, by their nature, always search for what is not known. However, in law enforcement and regulation internationally, analysts are required to collate information at hand; within a problem set for them. Analysts are rarely let out to collect; let

alone shape collection. Analysts become contained within the organisational bias of their employ. Hence, broadening education and training systems to encourage tradecraft in planning and monitoring – by breadth and depth and driven by intelligent questions – is paramount.

Intelligence practitioners are trained to reduce intelligence requirements into a series of information requirements which are necessary for analysis and to answer the decision-need. What information is at hand is first considered and preliminary significance and meaning – as well as a gap analysis – occurs. Consideration is then given to the need to address gaps and how to most efficiently fill them. Use of other agencies is considered as well as pursuing sources through the operational arms. If such skills permeated regulation, where another agency has the information sought, then – in the spirit of red-tape reduction – participants in the scheme do not need to be levied with additional information checks. However, such approaches in regulation are rare or require extensive legal agreements. Given most information requirements in a regulator can be answered from within accessible data-sets, the default is usually not to bother with chasing other sources. However, often the key issue of behavioural motivation and causality is not easily derived from the information at hand and hence the core tenant of intelligence is lost.

The lack of clear thinking around this concept is usually at the heart of regulators suffering adverse reviews or 'missing something' (Quarmby 2018, Part 2). There will always be information gaps in regulatory knowledge requiring access to information not immediately available. The cost/benefits of resourcing collection against these gaps should be carefully considered and additional layers of collection tasking added.

Education in how intelligence systems can be designed for coverage (by both breadth and depth) is therefore very necessary. Many regulators check or validate behaviours based on a schedule or sample. A contemporary view of the concept of coverage implies a considered balance of resources (both external and internal) applied proportionately across the at-risk behaviours in the jurisdiction. The more at-risk (higher impact) behaviours have more frequent or tailored

monitoring, while there is still capacity held aside to check on less frequent or less interactive participants (Quarmby 2018, pp. 129-131).

The concept of depth is inherently tied to the concept of breadth in regulatory intelligence. Monitoring has to have a sense of 'how deep are we trawling?' connected to 'how wide are we casting the surveillance net?'

An absence of tradecraft in collection planning is exacerbated by an absence in tradecraft in operational collection and exploitation of sources. In the human intelligence domain, regulators rely heavily on people and contacts for information that provide texture to otherwise grey transaction information and data. The tip-off, the whistle-blower, the people the inspector talks to on the work-site, the union official, the lawyer, the family members, the social networking group; all contribute essential intelligence for regulators. A contemporary intelligence system will enable a framework around human intelligence; set rules and collection management accountabilities. However, few regulators have professionalised the management of sources; hence, valuable insights and sources can be lost. Similarly, the transferable communications intelligence tradecraft for regulators lies in social media exploitation. Yet few invest in the skillsets to exploit new age media (Quarmby 2018, p. 131-133).

A critical footnote in this absence of tradecraft is that most regulators (if they have an intelligence function) are often single-source intelligence agencies. As noted previously the extent of data collection, data myopia and organisational culture lend regulators to only analyse what they know, based on their preferred source. For some this involves a leaning towards reliance on their transaction data. For others, action only occurs from public tip-offs. The narrow idea of intelligence as **a process** of converting information into intelligence satisfactorily fits in with such myopic cultures. The concept of being intelligence-led is readily converted into the need for a few extra staff and an extra step in the call centre or in the data extract and analysis process. The main point becomes lost in the single-source preferences of the organisation; the main point being: 'what don't we know, how significant is it, and how can we collect it?'

Differences in analytical techniques: risk, threat and harm

Much of the analytical approaches taught in intelligence are relevant in regulation. There are, however, a number of terms or types of analytical lens worth highlighting.

Risk – is a term related to decisions – and has a consequence and likelihood (event-based) analytical construct. Risk language used across regulators tends to limit analysis and the employment of intelligence professionals. Intelligence investment needs to be focussed on expanding the regulator's understanding of harms and trust/threat levels, as well as trends and patterns in behaviour. This is best stylised as 'at-risk' behaviours. Without this simple construct, the term risk can be confused with the concept of the risk of noncompliance; in other words, the risk of breaking a rule. As the failure of banking regulation internationally has uncovered, often the core at-risk behaviour to be assessed is more the organisational intent or the culture, and this is not an arbitrary rules-based measure (Quarmby 2018, pp. 59-61).

Harm is a term more relevant to behaviours targeted by regulators where the harm manifests as impacts in the domains of the social, economic, political/reputational, equity, personal, real/perceived… (and is therefore public value-based). The term 'triage' is used in regulation as the most basic form of analysis for harm.

Threat / trust – are interchangeable analytical lens in regulation segmenting those participants in the scheme likely to commit the harm. Some regulators may refer to participant "conduct" or "attitude to compliance". As a minimum it includes analysis of history, individuals, governance, associations, leadership, workers, market segments, stakeholders, interest groups etc. (and is therefore entity-based).

Three analytical approaches tend to dominate regulatory intelligence work:

- Statistical analysis – where there are patterns available in transaction data;
- Typology/morphological analysis – where there are no statistical patterns in data but the various component parts of 'problems' cross-connecting behaviours with identifiable actions, can be grouped and considered;

- Profiling – a combination of statistical and typology providing current and background assessment of the performance of an entity. Usually includes comparative indicators aligned by designated attributes. More complex profiling includes association analysis and projections of behaviour.

The following table provides an example of the various components of a profile of a commercial entity subject to a number of performance standards within a jurisdiction. The example fuses the concept of morphological, statistical and trust analysis noted above.

<table>
<tr><th>Attribute</th><th>Assessment and Metrics</th><th>So What?</th><th>Now What?</th></tr>
<tr><td>Governance</td><td>Better practice</td><td rowspan="4">Market sector importance, viability, strengths and weaknesses Associated with the Regulator's current areas of interest?</td><td rowspan="8">Desired behavioural change
• Entity level
• Sector level
Tone, timing and tempo of engagement</td></tr>
<tr><td>Probity</td><td>History</td></tr>
<tr><td>Business performance</td><td>Statistics</td></tr>
<tr><td>Financial performance</td><td>Statistics</td></tr>
<tr><td>Safety or harm to people or markets</td><td>Events and system quality, complaints</td><td rowspan="4">Trust and Harm
Real or projected?
Known or unknown?
Comparative or unique?
Impact on regulatory or scheme reputation?</td></tr>
<tr><td>Reporting and regulatory responsiveness</td><td>Statistics
Other inputs</td></tr>
<tr><td>Associations</td><td>Association analysis</td></tr>
<tr><td>Intent and investment in better practice (including regulation)</td><td>Futures</td></tr>
</table>

Table 1: Systems, attributes and morphological analysis (Quarmby 2018, p. 157)

Conclusion

With the rising demand for the cross-pollination of intelligence skill-sets and tradecraft from new sectors such as commercial competition intelligence, compliance, risk and regulation, there is scope for new innovative service offerings supplementing traditional academic courses. Training needs can be, to some extent, met online. The more enduring education provided by Universities could expand the environmental constructs of the intelligence course beyond the traditional domains of national security.

There is little education on offer internationally for regulators and especially for intelligence functions in regulation. The test for academia is managing the ownership of intelligence professional education across otherwise competing faculties. In the meantime, in-house training will remain central until education systems catch up with the demand.

Some thoughts tying training together with the other workforce planning notes above are contained in the following table.

	STRATEGIC	**OPERATIONAL**	**TACTICAL**
Training Requirements (Level Specific)	**Senior Analysts and Managers only:** • Managing in intelligence • Influencing and Reporting • Performance measurement • The art of regulation • Public value **Analysts and Senior Analysts and Managers only:** • Strategic	**For Senior Analysts and Managers only:** • Managing data analysis, mining and sharing • Business intelligence • Influencing and Reporting • Performance measurement • The art of regulation • Requirements and collection management	**For Senior Analysts:** • Managing entity analysis • Influencing and Target Packaging • Performance measurement • Requirements and collection management **For Analysts and Senior Analysts only:** • Advanced entity analysis and association

	assessment processes **Induction for all**: • Intelligence cycle • Basic collation, analysis and reporting techniques	**Analysts and Senior Analysts only:** • Advanced analysis techniques – statistical, systems and morphological modelling • Harm and trust analysis • Specialist tools – eg geospatial • Collection techniques • Source development **Induction for all:** • Intelligence cycle • Basic collation, analysis and reporting techniques	techniques • Profiling • Harm and trust • Specialist tools • Collection techniques – source exploitation and management **Induction for all:** • Intelligence cycle • Basic collation, analysis and reporting techniques

Table 2: Intelligence training needs in regulation (Quarmby 2018, p. 170)

References:

1. Ayres, I., Braithwaite, J., (1992). *Responsive Regulation: Transcending the Deregulation Debate*, Oxford University Press.

2. Baldwin, R., Black, J., (2007). *Really Responsive Regulation*, LSE Law Society and Economy Working Papers 15/2007, London School of Economics and Political Science Law Department.

3. Black, J., (2011). *Learning from Failures: New Governance techniques and the financial crisis*, Warwick University and Law Commission Symposium, September 2011.

4. Commissioner of Taxation (2015): Annual report 2014–2015, Part 02.

5. Davenport, T.H., Harris J.G., (2007). *Competing on analytics: The new science of winning*. Boston: Harvard Business School Press.

6. Davis, J., *The Kent-Kendall Debate of 1949*, Analysis and Policy, https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/Fvol35no2/2Fpdf/2Fv35i2a06p.pdf, downloaded 29 April 2019.

7. De Graaff, Bob, (2013). "Training Intelligence Producers and Consumers for the Future: The Dutch Approach", in *Journal of Strategic Security*, 6, no. 3 Suppl. 2013.

8. Freiberg, A., (2010). *The Tools of Regulation*. Annandale: The Federation Press.

9. Hane, K. M., (2019). *Royal Commission into Misconduct in the Banking*, Superannuation and Financial Services Industry, Final Report Vol 1. Commonwealth of Australia 1 Feb 2019, https://financialservices.royalcommission.gov.au/Pages/reports.aspx#final.

10. Ivec, M., Braithwaite, V., (2015). *Applications of Responsive Regulatory Theory in Australia and Overseas: Update*, Australian National University, Regulatory Institutions Network, Occasional Paper 23, March 2015.

11. Moore, M.H., (2013). *Recognising Public Value*. Cambridge: Harvard University Press.

12. Quarmby, N and Young, L.J. (2010). *Managing Intelligence, the art of influence*. The Federation Press, 2010.

13. Quarmby, N., (2019). *Intelligence in Regulation*. The Federation Press, Sydney Australia.

14. Ratcliffe, J., (2004). *Strategic Thinking in Criminal Intelligence*. The Federation Press, Annandale Australia.

15. Ratcliffe, J., (2016). *Intelligence-led Policing*, Routledge, New York 2nd Edition.

16. Sparrow, M.K., (2000). *The regulatory craft: Controlling risks, solving problems and managing compliance*. Washington DC: Brookings Institute Press.

17. Sparrow, M.K., (2008). *The character of harms: operational challenges in control*. Cambridge: Cambridge University Press.

18. Thaler, R.H., Sunstein, (2008). *C.R. Nudge: Improving decisions about health, wealth, and happiness*, Penguin.