Risk intelligence:
a Centre for Risk Research discussion document
FOREWORD

This latest addition to the Centre for Risk Research series of discussion and guidance documents is intended to enliven debate about how organisational risk management can be improved to tackle risk associated with both cyber and non-cyber related security threat, and with business competition. It contends that risk managers should focus more on actively gathering "risk intelligence," and likewise that the "risk radar" concept deserves closer scrutiny and development in order to recognise the need for proactive exploration of risk environments. These suggestions reflect the importance of developing shared terminology within risk management as a basis for improving practice. They also speak to the need for risk management to integrate with other organisational functions. The document’s various illustrations of how this can entail learning from military intelligence techniques and engaging the skills of competitive intelligence professionals will hopefully stimulate students of risk management and practitioners alike to view the risk profession in a new light. We are grateful to all contributors and welcome feedback from everyone.

Professor Johnnie Johnson
Director of the Centre for Risk Research

Professional Association Foreword: “The Institute of Risk Management is keen to stimulate debate about new techniques to manage risk in a world of increasing complexity. We welcome new, interdisciplinary thinking that moves us beyond process and linear analysis and supports effective Enterprise Risk Management. We would encourage our members and the wider risk community to engage with this paper and consider how its concepts might play out in a real world context.”

Carolyn Williams CMIRM, ACII
Director of Corporate Relations, Institute of Risk Management

INTRODUCTION

This discussion document asks whether risk management should seek to mature as a more proactive organisational function offering capability for audacious non-routine engagement with non-routine threat involving competitive or other hostile ill will by persons or groups towards organisations. This concern leads it to contemplate how risk management might develop forms of vigilance and investigation which actively explore the social world well beyond the radar scope currently associated with the risk profession. More fully, this central question can be expressed in terms of how risk management might focus more towards providing effective early warning against - and engage with - threats rooted in ill will towards organisations. The first half of this discussion document will explore this idea using the metaphor of an enhanced 'risk radar' for organisations. The second half will continue the discussion on a more practical level by looking at how the risk radar can gather and process 'risk intelligence' to create the 'risk intelligent' organisation.

Thinking along these lines entails asking the risk profession to look more closely at how 'risk identification' is best understood and undertaken within organisations. Perhaps some healthy introspection is called for on the question of whether there is too much desk-based risk identification practice. In other words, perhaps risk identification is all too often ensconced within organisational 'safe spaces' where it is limited by desk-bound imagination and readily available data. Perhaps what really matters, much more than is commonly acknowledged, is risk identification activity which goes out into the world seeking information which is elusive and yet highly valuable for organisations.

Professional Association Commentary: “Many risk professionals agree that a healthy approach to risk identification is to be perpetually dissatisfied with existing ‘legacy’ risk information, and to appreciate the necessity of striving to access more and better information from whatever more predictive sources become available. In a world where 90% of data was created in the last two years, the more proactive and creative such effort, the more likely it is that an organisation will be able to test, broaden and update its view of risk to keep pace with the fast-moving, complex and increasingly connected risk environment.”

Julia Graham,
Depute CEO and Technical Director, Association of Insurance and Risk Managers in Industry and Commerce
Given the above problem of organisational ‘lag time’ in relation to emerging threat, it makes good sense for organisations to seek to improve their defences by taking whatever reasonable investigative measures they can to reduce lag time for constructing defences against emerging threats. Such improvements can be theorised metaphorically in terms of organisations extending the reach of their ‘risk radars’ to get as close as they dare to the primary sources who pose the threats. Such improvements can be further theorised as aspiring to enable organisations, wherever possible, to prepare defences against threats before attackers/intruders have time to develop them toward implementation. In that sense, organisational risk radars are perhaps best conceived of as things that should be developed towards providing as much enhanced ‘early warning’ as possible.

Risk Management Ownership of the Risk Radar

A strong case can be made that these risk radar defences are best championed and owned by the risk management function in particular, despite protestations that might be levied by marketing, cybersecurity, competitive intelligence and others. Numerous issues need to be addressed within any new thinking we might do to sketch out what is required here. Firstly, we need to conceive of a suitable risk management process incorporating and moving forward from risk identification, which is integrated clearly, effectively and efficiently – and to achieve clarity efficiency in particular – with various other management and governance processes. At the very least, the situation of such a process within - and across - the organisation’s various ‘lines of defence’ would need to be clear. However the broader challenge would essentially be one of information management, re-envisioned to accommodate the risk radar metaphor as the basic sensory apparatus through which the organisation becomes aware of and responds to what is happening in the world.

Problems with Looking at Information Gathering through a Risk Lens

It should really be common sense to anyone employing the risk radar concept that it should seek sensitive attunement to all sorts of information, demanding various forms of expression and useful for diverse organisational purposes. It would be ludicrous to build a risk radar which sees only ‘risk’, which is to say one that partially blinds itself by missing upon seeing only what the lens of ‘risk’ renders visible. Alternatively, it can credibly be argued that risk radars need to gather all sorts of information so that, speaking generally and abstractly, the organisation can manage its risks more effectively.

Secondly, we would however need to consider that some conceptual awkwardness inevitably arises with our conceptual prism of risk radar designed to receive and relay risk information while also performing a broader information gathering and processing role. In the real world, what would matter is that investigative effort yields information useful for various organisational purposes, and that all gathered information can circulate throughout organisational lattices effectively and with the sometimes highly confidential treatment it requires. However, why should such information always be couched in the language of risk and flow through what are called ‘risk management’ processes? Surely it would it be foolish to even attempt this? Clarity would be required concerning the scope of each risk radar, with broader scope tending to bring with it more serious fitness for purpose issues for the processes concerned. It would be particularly important to guard against any use of unnecessarily restrictive terminology whose effect might be to funnel information through inappropriate semantic and organizational channels. Would the risk radar focus on providing early warning of all sorts of threats, including those arising with human ill will towards organisations? And what about opportunities? Would it also seek to initiate what is often termed competitor intelligence, business intelligence, marketing intelligence, or even consumer insight?

Perhaps the biggest problem with the risk radar concept, then, is that people may use it with insufficient understanding of why simplifying metaphors are problematic. The ‘risk radar’ metaphor is plainly just one of many interrelated metaphors which are fundamental to risk management practice, whose combined effect might sometimes be to normalise their uncritical use. Fortunately there is a fascinating management literature dedicated to debating the pros and cons of management metaphor, which reminds us how we can be critical. One prominent author within this literature, Gareth Morgan, has famously argued that despite problems such as the ease with which the mind can become trapped in metaphor, we nonetheless need it for our mental dexterity, particularly in order to engage with complexity.

This idea arguably has important implications for risk management. The profession’s terminology should, arguably, align to a fundamental management concern to achieve a rich causal understanding of what is going on in the world so that actions can be taken to improve organisational prospects. We perhaps begin to disengage from this concern when we view a ‘risk radar’ as a device that spots ‘the risks’ – just as a military radar might spot incoming enemy aircraft – so that ‘the risks’ can then be pushed through risk management processes and dumped into risk registers and internal control systems. The solution is perhaps, very simply, to regard the ‘risk radar’ as information gathering which, when used well, advances the organisation’s concern to have a rich understanding of its environment which can be useful for many purposes.
Generating Consumer Insights

Thinking flexibly about purpose, then, the notion that risk radars can be used to generate consumer insights is particularly intriguing because it leads us to consider the potential social benefit which risk professionals might regard as insights of nugget of gold for organisations, discovered only rarely, yet sometimes offering tremendous competitive advantage. An excellent (2008) text by Brian Smith and Paul Raspin called ‘Creating Marketing Insight’ discusses consumer insight along these lines. A very relevant source for further opening up the risk radar concept skims over within the text, but which need for rethinks the risk management skills to include, for example, the skillets of competitive intelligence professionals and other specialists whose bread and butter is to know the dos and don’ts of dealing with primary information sources. This suggests, at the very least, a need for more cooperation between these specialisms.

‘Boosting’ the Risk Radar

Professional Association Commentary: “Today’s businesses, large or small, operate in an increasingly VUCA world; that is, in a world characterised by volatility, uncertainty, complexity and ambiguity. Mary would describe this as the new normal. In the VUCA world, flows of information offer more business value than ever before. Such information can be accessed by its type, its volume, its gravity, its velocity and its veracity. This is best achieved by a dedicated organisational function. Competitive intelligence, the ethical and legal collection and analysis of all source public domain information to create the knowledge and understanding of the market around us, as a prelude to decision-making action, is the ideal antidote to the VUCA world. Analytical frameworks available to the trained and experienced competitive intelligence professional (and/or business professionals) help businesses and other public organisations to control the uncontrollable. They can be pointed to larger businesses’ risk management processes, and can be adapted by smaller businesses to create competitive advantage. The term ‘risk radar’ is well established in the business context. Analytical frameworks include STEEPLE Analysis, Nine Forces’ Model and Scenario Analysis to name just three. The risk management process aligns particularly strongly to ‘early warning’ competitive intelligence applications – which can do much to help businesses navigate through the VUCA world”.

Andrew Beurschgens

Volunteer UK Chapter Chair

Strategic and Competitive Intelligence Professionals (SCIP)

Clearly, the potential advantage to be derived from accessing primary sources of information about human threats to organisations might be enormous. And now - really, why not? Why should risk managers not use the tools which are useful for enhancing organisational awareness of threat and opportunity more generally, and indeed for gathering all sorts of valuable insights for organisations? There’s much to be said for a ‘radar’ to assist in this. However, we can construct a compelling case for - at the very least - some lively discussion concerning whether the risk profession should today be manoeuvring to progress the agenda for a new and better risk management with a ‘boosted’ risk radar, benefiting and requiring organisational functions. To reiterate in quite strong terms, such an improved risk management function would need to relax any vice-like semantic grip it might have to either deliberately or unwarrantedly in any flow of information across organisations, in order to elicit enthusiastic participation from across the organisations. It would certainly need to resist any temptation to process information through the conceptual straitjacket of the risk register. Has it not become clear that a more flexible alternative to the risk register by maintaining an ‘action point register’ geared towards providing trigs for incoming information, in particular, encouraging information flow to where it will offer value, with the urgency and sensitivity appropriate to it.

A Dangerous High Stakes Activity?

Somewhat, however, the risk profession should wash its hands of this opportunity to raise its profile. They might claim that ‘active investigation of primary sources of risk information’ had been left to the area of fuzzy overlap between the competitive intelligence, business intelligence and marketing intelligence domains (to be discussed in more detail later). Nonetheless there seems to be an empire-building opportunity for risk management here. Risk managers might build cases for overseeing the development of their organisation’s risk radar as a means to access more resources and strengthen their case for more participation in top level management decisions. This could be of particular interest wherever there is organisational policies characterised by various organisational functions competing for influence and resources.

ERM CONTEXT FOR BOOSTED RISK RADARS

Speaking further to the above issue of overlapping specialisms, it can also be argued that the risk profession is already strongly committed to conceiving of itself as aspiring to subsume various other – sometimes competing - organisational specialisms to serve its master concept of a singular, overarching, early warning risk radar for organisations. Thinking from this perspective, the risk profession is fundamentally concerned to promote such a system because without it there cannot be organisation-wide enterprise risk management (ERM) practice, through which organisations become resilient within their ever-changing and hard-to-anticipate risk environments.

Resilience Context for Boosted Risk Radars

Indeed, the term ‘risk radar’ itself is one that many already consider a business buzzword. ‘Radar’ is a NATO term meaning ‘rapid response before crises or disasters happen’ (see the report produced by Cranfield Management School on behalf of the ARMC, risk management professional association, recognises five such principles (hence the R) as follows:

- The Risk radar which anticipates problems before they escalate;
- Resources and assets which are diversified;
- Relationships and networks which allow risk information to flow freely;
- Rapid response before crises or disasters happen;
- Review and adapt, to learn from experience and make changes.

Notice that the first, third, fourth and fifth R is in particular describe an ordered sequence of activities. Hence we can conceive of the risk radar as driving the resilience process, or indeed the resilience cycle, depending on the context. Either way, we can construct that organisational resilience can only be as good as the risk radar which makes the risk environment visible.

The present document’s added suggestion that the risk radar for organisational resilience should lay strong emphasis on the need for people with very high rate skills people to do it, and active explore the social world (thereby ‘boosting’ the risk radar) should be of interest not just with respect to problems of ill will towards organisations, but also in view of the risk profession’s growing interest today in what is variously termed third party risk and partnership risk. We live in what is often termed an ‘age of access’ characterised by highly complex supply chains and emergent partnerships. A major concern is how these risks which matter most today relate to ambiguity in the relationship which organisations rely on. Surely this places a high premium on robust people skills, and a willingness to go out into the social world, in order to build the risk radar which risk management needs.

Developing the case for the Boosted Risk Radar using ERM’s Biological Adaptation Metaphor

The argument that organisations need risk radars which actively explore the social world as a part of the human environment of organisations can usefully be linked to the biological adaptation metaphor for enterprise risk management (ERM). This depicts the organisational entity as constantly exploring the organisational environment and feeding the results into their ‘organisational nervous system’ to its ‘organisational brain’ in order to navigate through that environment, just as every human being relies on their individual senses every minute they move through their physical, interpersonal, and more broadly social environments.

An opportunity to release further value from the metaphor arises when it is considered that some brains are better at handling social information than others. Some people, for example, have a ‘social radar’ which Dunbar have famously emphasised, have extra neo-cortical brain development over apes in order to move through, and gain advantage within, much larger and more complex social environments than apes can handle. It could be argued that the equivalent organisational development can occur when ambitious risk management departments aspire to develop and improve ERM towards greater attentiveness to the social interactive aspects of the risk environment in particular. This of course provides a very loose criterion by which ERM systems might be compared and evaluated. Some are likely to be better at handling higher levels of social complexity than others. Arguably, if risk management departments are not risk management ‘risk radars’ which we propose, then in terms of the biological adaptation metaphor they will become ‘simian’ and more fully ‘human’ in their social intelligence. Some further discussion of what might differentiate ‘simian’ from ‘human’ ERM might prove useful – but we leave that to the reader.

This subtly enhanced biological adaptation metaphor can easily accommodate many further individual and social psychology-based metaphors for opening our minds to what it can mean for organisations to navigate the social aspects of their risk environments. Humans are social animals in ways too rich and diverse to begin to list here with any thoroughness. They explore their social environments by getting to know people around them, by talking to them, by finding out who they like, who can cooperate with and trust, who can grant them access to resources and information, and which pursue risk identification largely as a sedentary introverted mathematician who prefers to steer clear of the rough-
and tangle of interpersonal confrontation because they find social engagement psychologically awkward or painful, or indeed perhaps in some cases because they fear falling foul of the law if any resulting conflict escalates. A more humorous alternative would be to consider such organisations as rather like ‘smartphone zombies’ who amble down busy pavements engrossed in the data they call up in front of them, all the while remaining dangerously unaware of their surroundings. These suggestions might each in their own ways stimulate some further fresh thinking about challenges and opportunities for the risk radar organisations need.

Some Key Problems with the Boosted Risk Radar

Nonetheless, there remain some very reasonable additional grounds for resisting this discussion document’s central proposal. Perhaps the most obvious problem is that primary sources and others close to them will be highly resistant to disclosure of any usable information concerning threats which they themselves either pose or have a stake in concealing. They may take strong measures to prevent or dissemble any such disclosures. They may well try to take legal action if their activities are within the law and they believe their privacy has been invaded, or that they have been subjected to some uncompetitive behaviour. If they believe organisations are investigating them using any legally or ethically dubious practices, they may go straight to the media to inflict what reputational damage and/or legal cost they believe organisations are investigating them using any legally or ethically dubious practices, they may go straight to the media to inflict.

The Ethics of using Boosted Risk Radars

Seeking solutions to the above problems, the remainder of this discussion document proposes a new form of non-routine engagement with purposeful and targeted human threat in a way that bringing about ethical, non-cyber, and non-human threat dangers. Boosted risk radars could add value in such contexts, and indeed in other contexts too. For as we have seen, the virtue ethics paradigm, the document argued for a vision of what it means to have ‘ethical’ risk management which emphasised the need for proactive and sometimes very risky truth-seeking and truth-telling behaviours, such as speaking truth-to-power in acts of whistleblowing and admitting failure or weakness in order to improve the flow of risk information. This vision of ethical risk management based on virtue ethics also seems to fit very neatly indeed with the present document’s advocacy of active and investigative forms of risk identification. An important consideration here is that virtue ethics arguably comes to its own as an approach to ethics under circumstances where very difficult individualised decisions need to be taken, where boldness is often a prerequisite for success, and where frameworks of rules and regulation offer less practical guidance value than individual conscience and resolve. Arguably ethical culture and ethical psychology become especially important practical considerations if the profession is to grow its ethical credentials while also sourcing vital information from sometimes hostile parties resistant to disclosure. Much consideration of the best ethical frameworks to allow this to happen is certainly called for.

A Respectable Front for Corporate Espionage?

The challenges facing any effort to build ethical risk management under these circumstances are, however, formidable. Behavioural imperatives can crush ethical conscience. Dishonesty might often seem like a tempting option if it allows high value risk information to be accessed. Another less obvious but nonetheless important challenge arises with the fact that, while our concept of a ‘boosted risk radar’ refers in part to a capacity for counter-espionage, we should also appreciate that any risk management capacity which subsumes capacity for counter-espionage must also provide some capacity for espionage itself.

Hence there arises the possibility that risk management could conceivably be operated as a respectable front for organisational resource geared towards espionage. After all, irrespective of whether espionage or counter- espionage is at issue, the same sensitivity to legal and reputational checks on covert activity, and the same concern about human and technological vulnerability, supply the essential knowledge and skills base. There may exist similar temptations to subvert ethical norms, or even to break the law, when exploiting human or technological vulnerabilities, no matter whether the intention is directed towards exposing the presence of competitors in acts of espionage or to access vital risk information in acts of counter-espionage. Taking stock, some of the key ethical challenges surrounding this document’s advocacy of a more proactive front for the risk profession will be explored later in this discussion paper.
‘RISK INTELLIGENCE’: THREE MEANINGS

TERMINOLOGY MATTERS. An important challenge facing risk managers is how to be efficient and effective as a very thinly spread organisational resource. A key consideration here – perhaps under-recognised in most risk management guidance – is that for risks linked to objectives to be managed effectively, it is unwise for the management of each risk to become remote from the management of its associated objective. Where there is careful coordination, we can conceive of risk management as being integral to managing an objective, such that risk management becomes an obviously necessary part of simply ‘managing’. By contrast, where there is poor coordination we can instead begin to conceive of risk management as a ‘bolt-on’ activity, vulnerable to being perceived as unnecessary added bureaucracy.

Mindful of the need for such coordination, we can further conceive of risk management activity as intrinsically social in character, involving a coming together of different forms of essential professional experience and knowledge from different sources. Hence shared risk management terminology matters greatly. Accordingly, the present discussion document frames the view that important conceptual innovations in risk management should pass basic tests of clarity and simplicity in how they are understood and applied. It further holds that where new developments are driven through injections of new thinking about the nature and scope of the discipline, they should ideally gain acceptance as simple common sense which everyone can agree on. Once incorporated within risk management thought and practice, people should wonder why they were not thought of earlier. It is hoped that this risk intelligence fits this bill well, as indeed does our development of the concept of a ‘boosted’ risk radar to extend the already widely-used risk radar concept. Might it even be argued that such new terminology offers risk management some glamour which will make people across organisations more likely to want to participate in it?

Whereas risk identification is something which can all to easily be desk-bound, risk intelligence offers an alternative form of words where we naturally contemplate active and energetic intelligence gathering activities.

Thus, we look to ‘risk intelligence’ to supply the pivotal terminological innovation for driving best practice forward. A definition is therefore appropriate. Seeking a working definition of risk intelligence which is clear, and yet whose multiple interrelated meanings are sufficiently rich as to enable risk professionals to rethink best practice, we do not choose between but instead synthesise thought-provoking definitions which have arisen within previous writings on risk intelligence.

We argue that risk intelligence deserves a central place in the risk management lexicon when understood as:

1. A professional aptitude; thinking from this perspective, the ‘risk intelligent’ risk manager appreciates the gravity of the challenge in developing a view of risk that is both thorough and detailed, objective and kept up-to-date; crucially, this ‘risk intelligent’ professional aptitude can be expected to manifest, in part at least, as a strong commitment to proactively tempering ethical integrity in both the pursuit and critical interrogation of risk information, fundamentally at issue here is aptitude for intelligent – and in particular, socially astute as well as legally and reputationally sensitive – engagement and interaction with potentially hostile primary or near-primary sources of risk information (i.e. that practice which we referred to earlier as corresponding to hazardous and high stakes ‘organisational edgework’).

2. An organisational role and its output; thinking from this perspective, the risk intelligence role centres upon organisational processes focussed flexibly towards gathering and churning out risk intelligence information for use within various management contexts, the flexibility at issue here can be understood as relating not just to flexibility in the use of various possible methods of gathering information, but also flexibility in how that information is triaged onwards so that best use is made of it while privacy and confidentiality issues are respected.

3. A hallmark of mature organisational risk management; thinking from this perspective, a vision of mature risk management practice arises where highly developed professional aptitudes (1, above) align with flexible organisational process capability (2, above) to create the risk intelligent organisation geared towards responding urgently and effectively to all sorts of non-routine risk issues involving purposeful and targeted human threat, over and above all of those risk issues conventionally handled by risk management. More fully, here we may also converse of the risk intelligent organisation in more metaphorical terms as relying upon its “boosted risk radar” to navigate all the threats and opportunities which loom up before it within its risk environment.

To summarise, then, the remainder of this discussion document argues that a new professional focus on risk intelligence – based on the above definitions which are intended to accommodate and integrate the full range of senses in which the expression may be used within everyday language in organisations – might well prove the best way to grow the risk management role within many organisations today. Its ideas should be of interest to academics, students and practitioners of risk management alike.

The challenge at hand, then, is to explore the above interrelated meanings of ‘risk intelligence’ in order to outline their practical implications for risk management can mean, and for how risk managers might consider going about their workaday lives differently. We will work towards concluding that the risk profession should give much more attention to the challenge of developing risk intelligence in the third and most ambitious sense of the term. To reiterate, it will be argued that such effort might usefully focus on exploiting organisational efficiencies by combining a number of management processes to form a singular integrated ‘risk radar’, which can be ‘boosted’ to engage with purposeful human threat to organisations while also better fulfilling the organisation’s broader information gathering needs.
MEANING ONE: RISK INTELLIGENCE IS MANAGING RISK INTELLIGENTLY

Studies treating risk intelligence as a measurable aptitude use the abbreviation ‘RQ’. They define high RQ individuals by their ability to estimate probabilities accurately. Its constituent items achieve this by asking respondents to rate their certainty rating to support the statement’s claim of Dante’s authorship,Someone not knowing that Goethe is the true author, who gives a 100% question is “The “Sorrows of Young Werther” was written by Dante”. Its constituent items achieve this by asking respondents to rate their professional attitude and knowledge. For example, one question is “The “Sorrows of Young Werther” was written by Dante.” Someone not knowing that Goethe is the true author, who gives a 100% certainty rating to support the statement’s claim of Dante’s authorship, would achieve a credible RQ score as a consequence.

PROFESSIONAL ATTITUDE AND KNOWLEDGE

Dylan Evans’ RQ scale has been reproduced widely on the internet. It seeks to measure a person’s ability to estimate probabilities accurately. Its constituent items achieve this by asking respondents to rate their level of certainty in the truthfulness of some proposition. Hence RQ diminishes with false confidence in wrong answers. For example, one question is “The “Sorrows of Young Werther” was written by Dante.” Someone not knowing that Goethe is the true author, who gives a 100% certainty rating to support the statement’s claim of Dante’s authorship, would achieve a credible RQ score as a consequence.

Ethical Rules of Thumb for Risk Intelligence

One of the likely benefits of such dialogue is a clearer understanding, within the risk profession, of the ethical dos and don’ts of engaging with various primary or near-primary sources in order to elicit risk information. Speaking very generally, no matter what the legal issues involved, organisations may well pay reputational penalties if their information gathering activities are exposed in the media and publicly perceived to breach ethical conventions. Hence the ethical intelligence (our second form of IQ) which risk intelligence requires needs to be flexible in its view of what it means to be ethical. Some good ethical ‘rules of thumb’ are:

- From virtue ethics: Can someone be open, honest and proud of their actions?
- From the golden rule: Are you treating others as you would wish to be treated yourself?
- From Kantian universal law: What if everyone acted as you are acting?
- From Utilitarianism: Will benefits outweigh harms, for the greater number?
- From Rawlsian Justice: What if there were a ‘veil of ignorance’ preventing the decision-maker from knowing whether they would be among the people impacted by an action?
- From Lockean rights: Will the action violate basic rights of those affected?

Let us further consider that the scientific measurement approach to RQ suffers from narrowness in what it measures. Opening out some parallels with the RQ construct, we could first of all argue that effective risk management also requires ‘IQ’. This naturally sets us thinking of cognitive problem-solving skills like pattern recognition and why they might often prove useful. However we could also expand our scope to consider emotional intelligence (EQ), which could lead us to reflect upon why various affective biases often matter for risk management (for example during effective coping with crises or when relying on heuristics to base decisions under uncertainty). We could then bring in cultural intelligence (CQ) and contemplate the risk profession’s rapidly growing interest in cultural context. In context, critical risk intelligence, emphasising cultural and social skills is likely to be more valuable than RQ defined narrowly as aptitude for estimating probabilities, where engagement with primary sources of risk information is at issue. More dialogue between the risk and competitive intelligence professions seems appropriate in order to clarify the spikes needed.

Ethics Codes for Risk Intelligence

Further, more practical guidance on the ethical intelligence that risk intelligence requires, can be derived from codes of conduct developed within the competitive intelligence profession. Here the practical challenges arising with ‘boosted’ risk radar concept start to become very clear.

The approach taken by the ‘Strategic and Competitive Intelligence Professionals’ global professional organisation on their website. www.scip.org is to offer a succinct high level code of conduct. As one might expect, this emphasises the importance of honesty, the need for compliance with all laws, and the need to avoid conflicts of interest. It also incorporates a more specific need to faithfully adhere to and abide by one’s company policies, objectives and guidelines, which should be an important consideration for anyone whose initial view of the profession is that it might sometimes operate in the grey areas between espionage and rectitude. Off further interest for anyone concerned to understand the ethical credentials of the profession is the specific need to accurately disclose all relevant information, including one’s identity and organisation, prior to all interviews. Notably, then, the effect of the code is to accentuate the profession’s specialisation in legitimate intelligence gathering free from all deceit and subterfuge.

The SCIP website also offers some interesting FAQs which illustrate how the code’s ethical requirements can be applied to various circumstances. Here are some examples:

Should Private Investigators (Pis) look at files discarded by a company? The SCIP guidance urges consideration that such activity is likely to be in breach of most organisations’ codes of ethics. They recommend applying a ‘red face test’ (debatable in meaning but perhaps best understood as a ‘shame’ test comparable with our test ‘from virtue ethics’ which might be considered a ‘guilt’ test) by asking the company employing the services of the investigator to consider whether they would be comfortable with a newspaper report revealing how the files had been sourced and used.

Is it ok to source information from another company by calling them and pretending to be a customer or a student? The SCIP guidance highlights an ethical imperative to disclose all relevant identifying information, further noting that misrepresentation may sometimes be illegal. However it further mentions that ‘mystery shopping’ is an ethically acceptable practice provided it does not violate retailer-specific rules.

Is it ok to buy or otherwise obtain a password to access a competitor’s website? The SCIP guidance advises that this is likely to be illegal, and to violate most organisations’ codes of conduct.
Should PIs be hired to investigate the Principals of Companies? Should Companies hire former government operatives to direct their intelligence operations? The SCIP is to find such practices unethical. This may lead us to consider that ethical and legal problems encountered by competitive intelligence practitioners should be referred to management or legal counsel. Here the SCIP guidance advises that all such activity should ‘begin’ with public domain information, however further investigations may sometimes be legally and ethically permissible. Some further commentary in addition to what the SCIP say may be helpful here. This is a complex area because there are many subtle techniques which companies can and do use to source intelligence information from Principals at rival companies. For example, if company A wishes to know what company B, it may send their local employee, X, who was a friend of X’s during their undergraduate days, to attend a corporate event where they know X will be present. The resulting ethical ambiguity experienced by X when meeting X’s may then prove extremely challenging. Also consider the above conditions repeated, only this time X and Y are senior sales managers. Even what may seem a perfectly innocent conversation, where X tells Y who they recently travelled to exotic destinations, may constitute valuable competitive intelligence by unintentionally revealing where commercial opportunities lie. Furthermore if X gives Y a phone number or social media identity to allow them to stay in contact, then such information might later be exploited to monitor X’s changing geographical locations.

MEANINGS TWO AND THREE: RISK INTELLIGENT PROCESSES AND RISK INTELLIGENT ORGANISATIONS

This section assumes the reader’s familiarity with the stage-by-stage logic of the risk management process, as found in the (2002) AIRMIC/ALARM/IRM Risk Management Standard, and more recently with some minor changes in the (2009) ISO 31000. Throughout the discussion which follows, we selectively juxtapose some basics of the risk management process, as illustrated by these guidance documents, with various similar organisational processes and related activities which all deal with gathering and processing information. The chief purpose will be to highlight some learning examples and opportunities for consolidation. This will enable us to outline what a consolidated risk intelligence process, and hence a risk intelligent organisation, might look like.

We cannot undertake exhaustive comparative studies of specific processes. However we can whet the appetite for such studies by illustrating how ideas and practices relating to arming of closely related organisational processes can all be drawn together within a consolidated risk intelligence process geared towards systematic and sustained reaching out much further into the social world to engage with hard-to-access, unobtainable, and often seemingly unobtainable types of information which has hitherto been regarded as unattainable. A simplifying starting point is to appreciate that business intelligence, marketing intelligence and competitive intelligence processes overlap considerably, and are often considered not to amount to much the same thing. This is partly because of their common ancestry in military intelligence processes.

Learning from Competitive and Marketing Intelligence Processes

Competitive intelligence processes can straightforwardly be consolidated with general risk management processes where they are already risk management processes to begin with, such that they observe the risk identification, analysis, evaluation and control staging of the risk management process. Consider that competitive intelligence processes are often conceived through risk lens as centring on risk management of the competitive environment. Such risk-focused competitive intelligence processes may differentiate themselves from general risk management by requiring consideration of a particular category of risk, ‘industry disruption’, as a basis for exploring what a company can do to achieve competitive advantage.

When competitive intelligence is undertaken with a marketing focus, it may employ a whole host of further very specific risk subcategories underpinning what is, collectively, ‘market risk’. For example, risk uncertainty over whether new products will have sufficient market sizes, ‘product risk’ (based on uncertainty over whether the product strategies will suffice sufficient market share), and profit risk (based on uncertainty over whether markets have been sufficiently profitable). For further reading on this, a (2005) text by McDonald, Ward & Smith entitled “Marketing Due Diligence” is particularly helpful. It discusses six risk subcategories under each of these three risk hierarchy headings and urges systematic consideration of the resulting eighteen point probabilistic risk reports within strategic decision-making. All of these risk categories and subcategories can be used to focus creative imagination on risk identification. Hence competitive intelligence cycles, focused on processing such risks, are very strong candidates for being consolidated within risk intelligence processes. Simply making explicit provision for consideration of the above risks within general risk identification might in itself provide a spur for risk management to remould itself upon the proactivity of the competitive intelligence processes. Furthermore, by enhancing the due diligence value of risk information, this would help improve the standing of risk management in its association with strategic decision-making.

Adopting the language of competitive and military intelligence processes

Yet perhaps an even more important consideration when advocating for a risk management process more integrated with - and enhanced through learning from - other information processes, is that the latter commonly uses language of risk identification or ‘collecting’. The equivalent stage within risk management processes is ‘risk identification’. These terms convey markedly different connotations, which we can consider significant because, as Whorfian linguistics and simple common sense tell us, words influence how we perceive and act. ‘Collecting’ and ‘gathering’ are words suggesting ‘motive’ or ‘direction’. ‘Collecting’ connotes the observer who can see clearest when stationary. Consider, therefore, the difference in meaning of the words let’s talk about identifying risk information and let’s talk about gathering risk information might have when spoken at a workshop. Which has more meaning and power as a call to action? This emphasis on ‘gathering’ or ‘collecting’ information, which is key to intelligence practice within organisations, has deep roots in decades of intelligence practice and technique developed by the military. Whereas the ISO 31000 risk management process begins with an ‘establishing the context’ stage prior to its ‘risk identification’ stage, US Military Joint Publication 2-0 moves through parallel planning and direction followed by ‘collection’ stages. The military process captures much of the logic of ISO 31000’s first two stages in its view of ‘planning and direction’ to be brought to bear in the context of ‘risk identification’. This emphasis on establishing the successful achievement of specified military objectives, so that follow through ‘collection’ activities can then take place at the next stage. However, in the military intelligence process the intelligence ‘collection’ stage is distinct from the ‘planning and direction’ equivalent for ‘direction’ in the equivalent risk management process did such elicitation of active information gathering effort may not necessarily take place at all, or take place at all, and may be delayed itself with identifying important areas of uncertainty so that risk identification then becomes compelled to gather information to resolve that uncertainty. However this may not happen. The ‘establishing the context’ stage is widely understood to be concerned with exploring various relations, structures, factors, drivers, trends, etc., which compose the ‘internal’ and ‘external’ context of the organisation, so that risk identification effort can then be focused towards specific areas of concern. More practically speaking, the emphasis may simply be on deciding who to invite to risk identification meetings. Hence the first two stages of the ISO process can actually be considered as being concerned with go-and-find-the-answers logic as are the first two stages of the military intelligence cycle. As a consequence, the two processes invite very different management approaches at their respective second stages. For the SCIP, ‘establishing the context’ stage would have been more effective in spurring active investigative effort at stage two had its wording dealt with establishing contextual uncertainties so that stage two negotiation to go out into the world and find answers might then favour enhanced risk identification.

Notably, however, neither of these processes reflect a resilience philosophy based on a perceived need for ceaseless scarifying activities permitting organisations to respond urgently to unexpected threat. Each has a first stage, but not a second stage. Furthermore, by enhancing the due diligence value of risk information, this would help improve the standing of risk management in its association with strategic decision-making.
Learning from Military Intelligence Practice

Next we turn to a further, this time much simpler and easier-to-implement, example of how risk intelligence can learn from military intelligence. Within the risk management process, risk analysis typically focuses on estimating probabilities and consequencess for risks, so that risk evaluation can then consider each risk's significance with reference to pre-established criteria such as risk appetite or tolerance. The more-or-less parallel military practice evaluates collected items of intelligence by estimating the reliability and credibility of sources for filtering and weighting purposes. The well known "Admiralty" or NATO classification system uses a lettering form for reliability of sources and numbering form for credibility of what the sources say, as follows:

If we are to re-envision risk management as a practice invigorated by the active information gathering skills of the competitive intelligence profession, it follows that simple reliability ratings for sources, and simple credibility ratings for the information these sources provide, may offer valuable and effective enhancements. During the risk identification stage of the risk management process, reliability and credibility ratings might be used to score risk information derived from secondary or primary sources. These scores might then be used to filter matters for consideration. Later on, during the risk analysis stage they might offer further value as touchstones for estimating risk likelihoods and impacts. And of course, anyone given ownership of a risk control lane within the risk management process would naturally want to reflect on the reliability of sources and the credibility of what they say, as indeed would anyone wishing to use the risk information yielded by the risk management process for decision-making purposes.

Reliability

Credibility

Completely reliable

Confirmed by other sources

Probable true

Fairly reliable

Possibly true

Not reliably

Doubtful

Unreliable

Improbable

Reliability cannot be judged

Expert Commentary: “My experience in the US military and its employment of Red Teaming provided valuable insight into military operations planning. By utilizing a Red Team familiar with tactics and techniques of a potential adversary, the Blue Team played out its operational plan within a given scenario. After a series of moves and reactions, the results of each move could be further analysed, and the results utilized in future iterations of the physical military plan.

Business could employ military Red Teaming to provide decision makers with potential outcomes, weaknesses or risks that may have been overlooked by individuals with intimate knowledge or personal ties to a plan. This provides a second view point that can be tested which may reduce risk or be used to identify a new solution or path to take on a project.

From my experience, Red Teaming caused us to consider new ways to deploy a force as compared to what we had experienced in the Cold War or even in our recent history in Counter Insurgency and fluid operations that we face in Syria and Iraq. The results of the Red Team Exercises are leading to employment, tactics and techniques and equipment by forcing institutional change in how planners deploy and project forces within military planning activities”.

Ross IV, Richard R., MSgt (Ret) USAF.
Former Red Teamer with HQ US Air Forces Europe, Directorate of Logistics, Engineering and Forces Protection, Engineer Division. The term ‘red teaming’ itself derives from the colour-coded nomenclature used by the US military for wargaming during the cold war, where ‘red teams’ played the attackers and ‘blue teams’ played the defenders. Various other teams also play important roles. ‘White teams’ set the standards and ensure that teams follow them accordingly. ‘Purple teams’ shape the learning narratives by listening carefully to the perspectives of all participants. ‘Green teams’ extend the simulations and consider conflict impacts upon third parties. In military wargaming these third parties may be neutral military powers, or refugees and other civilians in conflict zones. In business wargaming they may be an organisation’s stakeholders. Hence ‘green teams’ case study to be considered for defensive risk to render risk management more sensitive to stakeholder concerns.

Professional Association Commentary: “One important competitive intelligence framework is called war gaming, or competitive role play. This technique can use ‘red teaming’. A war game is neither a war nor a game but a structured forum to assess a market’s competitors and other stakeholders’ (customers, regulator, lobbyists) likely moves in relation to a specific market event or series of events. From a commercial perspective a wide number of stakeholder groups are often in play, therefore making the more binary focused ‘Red Team’ concept less relevant.

One of the benefits of war gaming is to gain a better and shared understanding of the competitive arena, therefore making it ideal to the risk management process. Other benefits include sensitising the management war game participants and wider business to competitive moves, identifying ‘blindspots’, providing the starting point for developing new products, ideas or advancements. The more serious and well planned a Red Team exercise is, the more the CIO/CEOs should not forget the team building benefits. Given that the average CEO tenure in the United Kingdom is 4.8 years, there is a strong argument for using wargaming for new incoming CIO/CEOs to stress test the robustness of the strategy he/she is inheriting and/or use it to craft a new one. However, operating in a VUCA world implies that this facilitated analytical practice should be taken place more frequently”.

Andrew Beurshagens
Volunteer UK Chapter Chair Strategic and Competitive Intelligence Professionals (SCIP). Sometimes also included in these simulations are ‘tiger teams’. Here the strength and agility of the tiger symbolises the discretionary powers which can be granted to participating teams whenever it is deemed that they are best placed to follow up on the learning outcomes from a simulation. However conflict simulation outputs are often advisory rather than determinative for real world follow up. The case for tiger teams is stronger where the simulations produce technical solutions rather than policy recommendations. Immediately a project or event becomes urgent action is required to address cybersecurity vulnerabilities. 3. RED TEAMING AS VULNERABILITY ANALYSIS

What sets vulnerability analysis apart from the above exercises is that they are less readily described as simulations because they focus on detecting real vulnerabilities. Vulnerability analysis is a form of wargaming where the red teams gain advantage from surprise in choosing how, when and where they attack. There are many famous examples of this. For example the US Department of Homeland Security’s Office of the Inspector General publishes statistics on the success rates of the red teams breaching security measures multiple times at specific airports. Positing as ordinary travellers, these red teams are often successful in smuggling fake ID’s, weapons, drugs and explosives through airport security. This has the effect of leveraging security improvements through public embarrassment. No airport security system can undoubtedly detect a security vulnerability which has been exposed in national media.

It’s also well known that military and business organisations employ hackers to test cybersecurity arrangements. For example, Peter Judge (Financial Times, 2015) he had formerly been associated with the “Loph” hacker collective whose members testified before US Congress in 1998 that they could shut down the internet in thirty minutes. Loph’s commercialisation during the 1990s onward provides a vivid illustration of how the intelligence service would wish to neglect a security vulnerability which may in itself provide a technique and spur for developing the risk management at the latter stage of the risk management process. Risk management is the independent application of a range of structures, creative and critical thinking techniques to assist the end user make a better informed decision to produce a more robust product”. The guidelines notes that NATO prefers to call this alternative analysis, defined as “the deliberate application of independent critical thought and alternative perspectives to improve decision-making”.

Israel’s government and military are reputed to make systematic use of alternative analysis in their major decisions. The red team they use for this is a secret unit within the Israeli Defence Forces called ‘Ipcha Mistabra’ (a term of Hebrew and Aramaic origin meaning ‘on the contrary’). Set up following the cosy from Kippur war, the team operates on the principle that it is the duty of the military officers they send to participate in decision-making, to challenge the assumptions and conclusions others make, no matter what their rank or seniority. This (and especially the legal implications of this Ipcha Mistabra role) are of course fascinating. It may be necessary to rotate contributing officers frequently to ensure nobody gets ‘stuck’ in their adversarial roles and drifts from their mission commitment and loyalty.

Essentially at issue within this view of red teaming, then, is bringing criticism and challenge to bear in order to enhance decision-making. The (2010) MoD guide offers specific guidance on the diagnostic ‘creative and challenge’ phases of red teaming practice. It also suggests specific analytical techniques which might be used. Of particular note is one of their ‘guidelines for good red teaming’ which notes that nothing is more critical in fostering a culture of ‘challenge and criticism’. Two comments can be made about this particular guideline. Firstly, it is valid for all three forms of red teaming introduced above. Secondly, it also matches what most risk management professionals would look for in a healthy risk culture. Hence it is interesting to consider that wider use of redteaming might in itself provide a technique and spur for developing the risk culture within organisations that make it more effective. Moreover, in a risk intelligent organisation, it makes sense that all relevant, reliable and credible intelligence information received by those making strategic decisions is passed to the risk management makers to consider – including information they would rather not have to deal with. Accordingly, we might even advocate for healthy risk cultures manifesting as a mix of critical and control. Finally, it is interesting to consider that hiring individuals with high scepticism and strategic intelligence will be a defensive risk to red teaming, does seem to bring it with increased opportunity for using secretive red teams as ‘fronts’ for corporate espionage, or at least for competitive intelligence activity which pushes legal and ethical boundaries. Concerns are likely to be high if/when the individuals hired have previous histories of engaging in such activities.

3. RED TEAMING AS ALTERNATIVE ANALYSIS

Here red teaming is considered as a decision support activity. A (2010) UK Ministry of Defence (MoD) Red Teaming Guide defines red teaming as “the independent application of a range of structures, creative and critical thinking techniques to assist the end user make a better informed decision to produce a more robust product”. The guidelines notes that NATO prefers to call this alternative analysis, defined as “the deliberate application of independent critical thought and alternative perspectives to improve decision-making”.

Finally, it is interesting to consider that hiring individuals with high scepticism and strategic intelligence will be a defensive risk to red teaming, does seem to bring it with increased opportunity for using secretive red teams as ‘fronts’ for corporate espionage, or at least for competitive intelligence activity which pushes legal and ethical boundaries. Concerns are likely to be high if/when the individuals hired have previous histories of engaging in such activities.

Israel’s government and military are reputed to make systematic use of alternative analysis in their major decisions. The red team they use for this is a secret unit within the Israeli Defence Forces called ‘Ipcha Mistabra’ (a term of Hebrew and Aramaic origin meaning ‘on the contrary’). Set up following the cosy from Kippur war, the team operates on the principle that it is the duty of the military officers they send to participate in decision-making, to challenge the assumptions and conclusions others make, no matter what their rank or seniority. This (and especially the legal implications of this Ipcha Mistabra role) are of course fascinating. It may be necessary to rotate contributing officers frequently to ensure nobody gets ‘stuck’ in their adversarial roles and drifts from their mission commitment and loyalty.

Essentially at issue within this view of red teaming, then, is bringing criticism and challenge to bear in order to enhance decision-making. The (2010) MoD guide offers specific guidance on the diagnostic ‘creative and challenge’ phases of red teaming practice. It also suggests specific analytical techniques which might be used. Of particular note is one of their ‘guidelines for good red teaming’ which notes that nothing is more critical in fostering a culture of ‘challenge and criticism’. Two comments can be made about this particular guideline. Firstly, it is valid for all three forms of red teaming introduced above. Secondly, it also matches what most risk management professionals would look for in a healthy risk culture. Hence it is interesting to consider that wider use of redteaming might in itself provide a technique and spur for developing the risk culture within organisations that make it more effective. Moreover, in a risk intelligent organisation, it makes sense that all relevant, reliable and credible intelligence information received by those making strategic decisions is passed to the risk management makers to consider – including information they would rather not have to deal with. Accordingly, we might even advocate for healthy risk cultures manifesting as a mix of critical and control. Finally, it is interesting to consider that hiring individuals with high scepticism and strategic intelligence will be a defensive risk to red teaming, does seem to bring it with increased opportunity for using secretive red teams as ‘fronts’ for corporate espionage, or at least for competitive intelligence activity which pushes legal and ethical boundaries. Concerns are likely to be high if/when the individuals hired have previous histories of engaging in such activities.

Finally, it is interesting to consider that hiring individuals with high scepticism and strategic intelligence will be a defensive risk to red teaming, does seem to bring it with increased opportunity for using secretive red teams as ‘fronts’ for corporate espionage, or at least for competitive intelligence activity which pushes legal and ethical boundaries. Concerns are likely to be high if/when the individuals hired have previous histories of engaging in such activities.
CONCLUSION

Many are drawn to the risk profession because they are fascinated by ideas. They appreciate that it is one of the few professions where skill and innovation in theorising the things that need to be managed is everything. They discern that organisational risk management, while no longer in its infancy, remains far from exhausting all lines of theoretical inquiry and experimentation with new practices through which it might fulfil its potential.

The present discussion document has undertaken to reflect, inspire and to some extent direct this optimism and enthusiasm for a greater future for risk management. It has striven to provoke discussion through a recommendation for improving risk management as an intelligence-gathering practice. This theoretical possibility has been available as low-hanging fruit for risk management theorists for as long as the modern risk management profession has existed, and yet its various strands – including various writings on risk intelligence and related concepts which have proliferated in the last fifteen years – have not been drawn together into a simple proposal for the future of risk management until now. Perhaps if organisational risk management had become an important profession in the post war world of the mid 20th century, deliberately recruiting from demobbed ex-forces personnel with military intelligence experience, it might today seem obvious that this pattern of recruitment was necessary to set the risk profession on firm foundations. This didn’t happen, of course, and so we perceive the profession very differently.

Critics of this document’s main contention may ask whether scope really remains for the risk management profession to find and incorporate some new and transformative common sense. In the early 2000s the idea that ‘opportunity’ could be managed in the same way as ‘threat’ emerged within best practice guidance as what seemed like transformative common sense to many – and yet it didn’t quite fulfil all expectations. Critics may correctly remark that this idea met with mixed success and created an odd disconnect between best practice guidance advocating it and real world practice staunchly opposed to it, even in some very large organisations.

Taking stock, it seems highly unrealistic to advocate for untried and untested ideas. Instead it seems much more appropriate to seek opportunities for importing ideas and practices boasting prior history and pedigree in alternative management domains – particularly when these have clear relevance to the work of risk managers. Accordingly, this document has advocated a reshaping of risk management towards a fundamental concern with ‘risk intelligence’ under the influence of ideas and methods that are already well established. Comments from readers are welcome on their own experiences, or ideas, regarding the synergies we have outlined and tentatively advocated for.