6

Policy implications of convergence in the new security environment: An investigation into the symbiosis between risk management and intelligence

Katina Michael[1] and Mark Loves[2]

[1]Senior Lecturer, School of Information Systems and Technology, University of Wollongong, [2]Senior Lecturer, Program Manager, Centre for Transnational Crime Prevention, University of Wollongong

Abstract

For some time there has been a movement away from the traditional view of security as a purely functional activity which occurs within a single department of an agency or enterprise, to security being understood as a value added capability serving the overall mission of an organization. Enterprise risk management (ERM) is a process that is conducted by private companies for the purpose of due diligence informing key decision makers like chief information officers (CIOs). In the same light, the intelligence cycle is conducted by government organizations for the purpose of maintaining national security and informing policy makers like heads of state, ministers and other agencies tasked with security such as the military. The new security paradigm has spurred on the development of enabling business processes that have not only an enterprise-wide view of risk but an interdependent organization-to-organization view of risk. Entities interconnected in the intelligence community (IC) must consider sharing their information to ensure robustness in their decision-making capabilities. In changing the way things

have been done, entities in the new security environment are undergoing the trend of convergence on a number of levels including information, products and services, platforms (i.e. standards), and organizations. Of importance in this paper, is the convergence and integration occurring between the risk management and intelligence cycles which has born about the emerging concept of risk intelligence (RI).

Keywords: Security convergence, enterprise risk management, intelligence cycle, business intelligence, real-time business intelligence, risk intelligence, business process

1 Introduction

This paper argues that convergence is occurring within the security environment, notably in the disciplines of intelligence and risk management. Commentators are unanimous in their assessment that the security environment is undergoing a steep rate of change in the way the intelligence community functions, some stating that the change is so dramatic that it can even be considered revolutionary. The trend of convergence is prevalent at multiple levels, causing a cultural shift[1] away from a silo and stovepipe mentality towards transparent information sharing. The paper begins by defining convergence in the new security environment, and broadly outlines the different types of convergence that have been defined in the literature. A normative description of risk management and intelligence is then provided, showing the basic steps carried out for each by enterprise and government organizations. The contribution of this paper is in identifying how risk management and intelligence cycles can be integrated through business processes and the benefits ensuing from this integration. Beyond integration, it is predicted in this paper that the risk management and intelligence processes will soon be referred to interchangeably and universally in the literature. The emerging concept of "risk intelligence", explicitly merging together the domains of 'risk management' and 'intelligence' is then discussed prior to concluding remarks restating the importance of the trend of convergence in the new security environment.

2 Security convergence

The term "convergence" has its roots in mathematics and the natural sciences dating back to the late sixteenth century.[2] In its modern interpretation "convergence" has to do with the evolutionary trends in technological

[1] United States Government Accountability Office, 'Information Security Management' (U.S. Government, 1998) 28. '… it is likely a "cultural shift" will occur among the public safety agencies, organizations and personnel. This "cultural shift" is more a product of the process than an intended consequence. The SMEs in a recent panel stated: "As a consequence of the collaboration, information sharing, and coordinated activities inherent in adopting and executing a Risk Management Model, or some other analytical risk and vulnerability model, it is expected that there will be a "Cultural Shift" in the public safety community.'

[2] Edward P. Borodzicz, *Risk, Crisis and Security Management* (2005) 13.

development.[3] The term is therefore now linked to the idea of symbiosis occurring between products or between processes.[4] At an enterprise level, convergence can be observed as individual business units come together to enhance security for the purpose of creating competitive advantage.[5] At a state level, convergence can be understood within the context of national security, as agencies that start looking more and more alike come together to engage in collaborative efforts to meet performance criteria, and to ultimately reduce costs by removing duplication and redundancy. ASIS International defines "security convergence" as:

> 'the identification of security risks and interdependencies between business functions and processes within the enterprise and the development of managed business process solutions to address those risks and interdependencies.'[6]

A more recent definition of security convergence states its relevance to enterprise security risk management (ESRM)[7] and emphasizes the combined management of physical and logical security.

2.1 Types of security convergence

In discussing convergence, this paper engages the reader at four different levels (figure 1):

> Convergence of *security organizations* at the national and enterprise level.[8] This type of convergence includes companies that are coming together to offer solutions to the intelligence community, as well as convergence of government agencies that would work more effectively together than as stand-alone organizations;

[3] K. Michael et al, 'The hybridization of automatic identification techniques in mass market applications: towards a model of coexistence' (Paper presented at the Third International Conference on Management of Innovation and Technology, Singapore, 21st-23rd June 2006) 1046.

[4] Katina Michael, 'Trends in the selection of automatic identification technology in electronic commerce applications' in N. Cerpa and P. Bro (eds), *Building society through e-commerce: e-Government, e-Business and e-Learning* (2003) 135.

[5] Allen Booz, *Convergence of Enterprise Security Organizations* (8 November 2005) The Alliance for Enterprise Security Risk Management <www.asisonline.org/newsroom/alliance.pdf> at 1 May 2008 6.

[6] Ibid 4.

[7] Michael P. Johnson and Jeff M. Spivey, 'ERM and the Security Profession' (2008) 55(1) *Risk Management* 31. 'ESRM is a holistic risk management process that aligns organizational drivers affecting strategy, processes, people, technology and knowledge to protect key assets in accordance with governance, risk, and compliance (GRC) requirements. ESRM requires cross-functional collaboration within the back drop of ERM between multiple management disciplines including, but not limited to physical and logical security, safety, legal, risk management, crisis management and business continuity planning.'

[8] Jagdish Pathak, 'Risk management, internal controls and organizational vulnerabilities' (2005) 20(6) *Managerial Auditing Journal* 569.

Convergence of *security processes* (i.e. standards/ platforms). This involves the identification 'of security risks and interdependencies between business functions and processes within the enterprise and the development of managed business process solutions to address those risks and interdependencies';[9]

Convergence of *security products and services*, fundamentally involving 'different companies' people and IT systems working together to deliver a convergent product or service';[10] and

Convergence of *information*, ie sources and quality content that is used to inform business processes, including technical, human, open source intelligence etc.[11]

The model of convergence has been said to be 'ideal' for 'managing uncorrelated… risk through a systematic, coordinated process.'[12] However, the complexity of convergence in reality should not be understated.[13] Taking policies and processes that were once created in silos and trying to make some collective sense out of them to institute change, is multifaceted and complicated.[14] While at the enterprise level convergence is being driven by compliance,[15] government agencies and organizations have not come under similar scrutiny.

Figure 1. Convergence in the new security environment

[9] Michael Peterson, *Information Convergence, Transforming the Information-Centric Enterprise* (2006) SNIA Data Management Forum <www.sresearch.com/articles/SRC-DMF-Article_Information-Convergence_20060112.pdf > at 27 April 2008 3.

[10] Mark Layton, *Urgent Convergence: Fostering Risk Intelligence in the Technology, Media & Telecommunications Industries* (2008) Deloitte <www.deloittte.com/RiskIntelligence> at 27 April 2008 2.

[11] Peterson, above 9, 3.

[12] Todd L. Williams, 'Convergence' (1999) 46(8) *Risk Management* 14.

[13] Margaret T. Wrightson and Stephen L. Caldwell, 'Risk Management' (United States Government Accountability Office, 2005) 8. 'The task of managing this complexity centers on the Department of Homeland Security, which since its inception in March 2003 has been faced with the challenge of transforming 22 agencies into an organization that can plan, manage, and carry out operations effectively.'

[14] Matt Podowitz and Brian Tretick, *Compliance, Convergence and How IT Fits* (8 January 2008) CIO <http://www.cio.com/article/print/170000> at 27 April 2008 1.

[15] Ibid 1.

2.2 Security as a value add

The premise for the convergence phenomenon sweeping the global security industry has been a shift in mindset that sees security as a "value add" to the overall mission of businesses and government agencies alike.[16] It is the realization that security cannot be achieved alone, but requires a meshed network of stakeholders and entities to work together towards a common goal. More than any other event in recent U.S. history, September 11 (2001) showed the failure of intelligence agencies in sharing information regarding possible terrorist targets. For instance, an inquiry into the actions of the Federal Bureau of Investigation (FBI) concluded that the main problems were: severely inadequate information and communication technology (ICT) systems, an inability to bridge together human intelligence (HUMINT) and technical intelligence (TECHINT) to conduct all source analysis, and problems related to the recruitment and training of analysts.[17] Apart from asymmetric terrorist strikes that have caused significant loss of life post September 11, imperatives towards convergence in the security environment have come from enabling high technologies that have blurred traditional functional boundaries, new compliance and regulatory regimes, and the emphasis today on information-based assets (i.e. as opposed to physical items).[18] Security convergence has meant change in the context of:

people and their respective roles and responsibilities;
processes in terms of standards to follow and regulations; and
technology in terms of enabling tools and applications.

2.3 The end-to-end security lifecycle

The motivation behind convergence in the security environment is one that espouses a whole-of-life,[19] holistic,[20] highly collaborative exchange between organizations and agencies. It is a movement away from the silo functional organizational security view which treated the areas of prevention, detection, response and recovery separately, toward a view which espouses the entire end-to-end security lifecycle as a super-system. The challenge with such a system is getting organizations and agencies who have thought and acted a

[16] Booz, above 5, 4.

[17] Peter Gill, 'Intelligence and the Post 9/11 Shift' (2004) 19(3) *Intelligence and National Security* 467–489 475.

[18] Booz, above 5, 8.

[19] Russ Banham, 'The convergence of risk' (1995) 42(7) *Risk Management* 22. 'Companies that regard all their risks as a totality can better make decisions to protect themselves from risk.'

[20] Ibid 23. 'Academically the concept of holistic risk management seems to represent an effective risk management strategy.' See also, Podowitz and Tretick, above 14, 1, who call this a 'federated' approach.

particular way for decades, to change their ways and to begin working closer together in order to solve problems.[21]

The *new* security environment[22] is characterized by strategic changes, changes to processes, and changes to the roles and responsibilities of people in security organizations. The nine traditional operating levers can be adapted to help organizations perform better in the new converged security environment. The levers that can be applied with respect to internal and external drivers include: risk management, governance, budget processes, standards and guidelines, integration, business case, roles and responsibilities, leadership and knowledge of business.

3 The risk management process

3.1 Security = Risk Management[23]

Till now this paper has focused on the notion of convergence. In this section the risk management domain is explored within the context of the new security environment. To begin with risk[24] is defined, as a unified language is presently missing from the domain. This is vitally important as often different fields of study claim to be the 'owners' of risk management (eg information technology[25] and insurance) when quite oppositely, risk is enterprise-wide[26]. Where there are security issues of any type, then risk management practices should be instituted. Traditionally risk was only considered to be about physical assets- 'the potential

[21] Booz, above 5, 6.

[22] Borodzicz, above 2, 68. 'The security industry is beginning to change in function and application … The simplistic conception of security- controlling physical access to the organization and controlled movement of property- may have been adequate 20 years ago. Today this would include a much larger range of risks, such as fraud, terrorism and disaster contingency plans.'

[23] Mark Merkow and Jim Breithaupt, *Information Security Principles and Practice* (2006) 27. Merkow and Breithaupt state in their principle 7 that security equals risk management. See also, Borodzicz, above 2, 50 who states: 'security can be seen as risk management in practice'.

[24] Borodzicz, above 2, 52-55. Borodzicz writes that risk management can be studied using eight different approaches: historical, psychological, sociological, functionalist, management, normative, structural, and descriptive.

[25] Gurpreet Dhillon, *Information Systems Security: Text and Cases* (2007) 157. 'Security risk management is not a standalone activity. It should be integrated with the systems development process. Any typical systems development is accomplished through the following steps: initiation, requirements assessment, development or acquisition, implementation, operations/maintenance, and disposal. Failure to integrate risk management with systems development results in patchy security'.

[26] Jerry A. Miccolis, 'Towards a Universal Language of Risk' (1996) 43(7) *Risk Management* 46. ''…There should be a convergence of the treasurer's and risk manager's definition of risk… In order for senior managers to have a complete grasp of all-encompassing risk as it affects their businesses, they need to communicate the varieties of risk in a common language. Only then can they approach risk holistically, with an understanding of how the risks work independently and together, and how they could affect the bottom line when combined.'

that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm, to the organization.'[27] Today however the business of risk has changed.[28] Risk management[29] is now more about the organization's strategic-level initiatives[30] which encompass *both* physical and logical assets. For this reason, enterprise risk management (ERM) is about 'bringing business functions (eg finance, line management, R&D, human resources) closer together to build a common risk-based framework for better decision making…'[31]

3.2 Risk management standards and guidelines

No matter what risk analysis process is used the standard method remains the same.[32] Risk management is composed of three main parts: risk assessment, risk mitigation, and risk evaluation.[33] Will Ozier defines risk management as the process:

> 'of identifying risks, risk-mitigating measures, the budgetary effect of implementing decisions related to the acceptance, avoidance, or transfer of risk… [it also] includes the process of assigning priority to, budgeting, implementing, and maintaining appropriate risk-mitigating measures in a continuous or periodic cycle of … management.'[34]

[27] Enisa, *Glossary of Risk Management* (2008) Enisa: a European Union Agency <http://www.enisa.europa.eu/rmra/glossary.html> at 27 April 2008 4. See also, Thomas R. Peltier, *Information Security Risk Analysis* (2001) xi who states that risk is 'someone or something that creates or suggests a hazard.' Jae Shim et al, *Information Systems Management Handbook* (1999) 19. Traditionally, the common objectives of risk management included: 'avoiding, reducing or transferring risk; reducing the cost of managing risk; actively managing risk in a consistent manner throughout the organization; and providing senior management with reports on risk-management activities within the organization.'

[28] Todd L. Williams, 'An integrated approach to risk management' (1996) 43(7) *Risk Management* 22. See also, Miccolis, above 27, 48 who divides risks into two types: hazardous and non-hazardous. He categorizes risks into five different types including: physical (eg property and data), business (eg prices and reputation), legal (eg contractual and statutory), political (eg terrorism and regulation) and financial (eg securities and interest rates).

[29] Jill Slay and Andy Koronios, *Information Technology and Risk Management* (2006) 2: ''a continuous process designed to assess the likelihood that an adverse event will occur, implement measures to reduce the risk that such an event will occur, and ensure that the organization can respond in such a way as to minimize the consequences of the event.' For a detailed overview of risk management see also, Wrightson and Caldwell, above 13.

[30] Institute of Risk Management, *IRM: A Risk Management Standard* (2002) AIRMIC <www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf> at 27 April 2008 2.

[31] Miccolis, above 27, 48.

[32] Thomas R. Peltier, *Information Security Risk Analysis* (2001) 5.

[33] Dhillon, above 26, 155-170.

[34] Will Ozier, 'Risk Assessment and Management' in Thomas R. Peltier (ed), *Information Security Risk Analysis* (2001) 224.

While many versions of the risk management cycle are available from diverse sources- international bodies like the OECD (Organization for Economic Co-operation and Development)[35] and the ISO (International Standards Organization),[36] national standards bodies,[37] government agencies, industry-specific bodies[38] and even single organizations[39] - the cycles all encompass the same broad steps. One of the first contemporary renditions is depicted in Figure 2 (the GAO/AIMD-98-68 Information Security Management guidelines):

Assess risk and determine needs;

Implement appropriate policies and related controls;

Promote awareness; and

Monitor and evaluate policy and control effectiveness.[40]

It is worth mentioning also, that the Australian and New Zealand Standard on Risk Management AS/NZS 4360: 2004[41] is considered as leading edge[42] because it specifically addresses all forms of risk management and can be applied independent of industry type.[43] This standard, applied correctly,

[35] Slay and Koronios, above 30, 82. The OECD Guidelines for the Security of Information Systems and Networks are subtitled 'Towards a culture of security.' One of the nine basic principles on which a culture of IS security can be founded is risk assessment.

[36] Institute of Risk Management, above 31, 5. 'Risk Assessment is defined by the ISO/IEC Guide 73 as the overall process of risk analysis and risk evaluation.' See also, ISO, *ISO/IEC Guide 73:2002: Risk management -- Vocabulary -- Guidelines for use in standards* (2008) International Standards Organization <http://www.iso.org/iso/catalogue_detail?csnumber=34998> at 27 April 2008 and Garry Roedler, *A Path to Convergence of Risk Management Standards* (July 2006) Lockheed Martin Corporation <www.incose.org/practice/techactivities/wg/risk/docs/7_Roedler_Slides_28JUN06.pdf> at 27 April 2008 3. The latter reference described ISO/IEC/IEEE 16085, as a good base for risk management principles.

[37] Slay and Koronios, above 30, 88. 'HB 231:2000 provides an exhaustive examination of the risk management process and in so doing establishes the 'strategic context', 'organizational context' and 'risk management context' within which an enterprise will carry out the risk management process.'

[38] See, eg, Dhillon, above 26, 172-178 for the I2S2 model.

[39] Peltier, above 33, 4. In many organizations risk management is synonymous with quality assurance.

[40] Peltier, above 33, 17-19. See also, Gary Stoneburner, Alice Goguen and Alexis Feringa, 'Risk Management Guide for Information Technology Systems' (National Institute of Standards and Technology, 2002) and John Walz, *Risk management in ISO standards* (2005) Sarbanes Oxley <http://www4.asq.org/blogs/sarbanes-oxley/2005/12/risk_management_in_iso_standards> at 27 April 2008.

[41] SAI Global, *Risk Management* (2008) Standards Australia <http://www.riskmanagement.com.au/> at 28 April 2008 1. See also, Slay and Koronios, above 30, 83 who state that the precursor to this standard was AS/NZS ISO/IEC 17799:2001 Code of Practice for Information Security Management.

[42] Kevin Knight, *New approach to risk management* (August 2003) SAI Global <http://www.sai-global.com/newsroom/tgs/2003-08/risk/risk.htm> at 27 April 2008.

[43] Tom Godfrey, *New risk management standard to help businesses meet ASX requirements* (14 September 2004) Standards Australia <http://www.standards.org.au/cat.asp?catid=41&contentid=197&News=1> at 27 April 2008.

promotes strategic advantages.[44]

Figure 2: The steps in the risk management cycle[45]

3.2.1 Steps explained

The heart of any risk management process is a risk assessment (figure 3). Typically a risk assessment begins with identifying risks. Risks are usually categorized into different types to make assessment more meaningful. A method is then formulated to prioritize risks which typically include both quantitative and qualitative data, and may take the form of a risk score and/ or mapping exercise. A critical risk analysis is then conducted to evaluate risk-loss/risk-return values modeled against performance indicators. The risk model is then implemented and strategies are recommended to mitigate losses. [46] It is important to emphasize that risk is everybody's business. A risk assessment is considered robust if it covers a range of issues- technological, human factors, policies, third party, etc…[47]

[44] Godfrey, above 45.

[45] United States Government Accountability Office, above 1.

[46] Foley & Lardner LLP, *Enterprise Risk Management - Risk Intelligence and Anti-Fraud Controls* (2007) National Director's Institute at 27 April 2008 2.

[47] Dhillon, above 26, 235. Dhillon claims rightly that 'since most systems are interconnected and interdependent, any risk assessment should also consider threats that might originate elsewhere.'

Figure 3: The risk management process[48]

3.3 What does risk management have to do with national security?

It has already been established that risk management and enterprise security go hand-in-hand. But a question that can be legitimately posed is whether or not risk management has any relevancy to national security? Figure 4 represents a contribution to knowledge as it attempts to unravel the links between terminology, processes, stakeholders, and the broader intelligence community. For the rest of the paper, these links will be explored in more detail. While it is typical to think of risk management in areas like insurance and finance, it is atypical to relate risk management to domestic terrorism. And yet, the risk management process has been embraced by the U.S. Congress and the President, post September 11, in order to strengthen against future terrorist strikes.[49] In the context of national security then, risk management can be defined as a 'strategy for helping policymakers make decisions about assessing risks, allocating resources, and taking actions under conditions of uncertainty'.[50] In the following section we investigate first the intelligence cycle, and then the likeness of the intelligence cycle to the risk management process. We pose the following hypothesis- that the intelligence cycle and risk management are converging domains and that before too long, the processes will be used interchangeably.

[48] Institute of Risk Management, above 31, 4.

[49] Wrightson and Caldwell, above 13, 8.

[50] Ibid 8. Cf chapters two and three in Jae Shim et al, *Information Systems Management Handbook* (1999) with the Wrightson and Caldwell definition- one prior to September 11 and the other after the attacks.

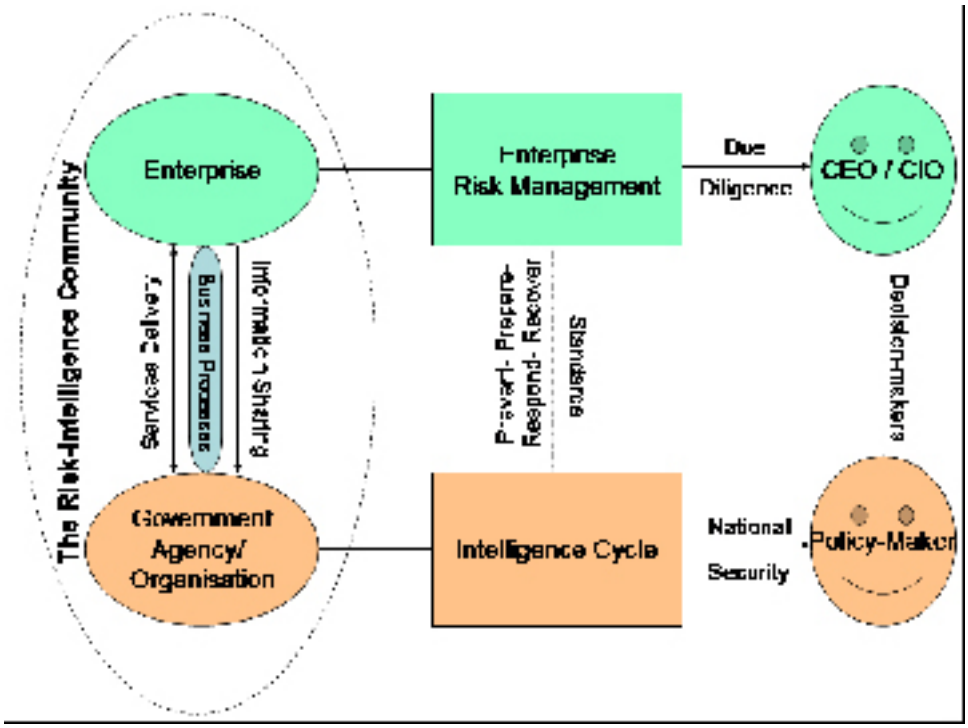

Figure 4: Making sense of the risk management and intelligence processes

4 Intelligence cycle

The common misconception is made, that the intelligence cycle is strictly something conducted by tactical military analysts. However, it is well-known that practitioners in industry widely practice intelligence-related activities for a variety of reasons, including for the purpose of competitive business intelligence (BI). Unlike the risk management process which has undergone a great deal of standardization due to compliance and other globalization factors, the intelligence cycle has remained a fairly generic framework that organizations can choose to follow completely or partially. On the national security and defense side, however, intelligence as a process is continually being improved upon, especially to combat future asymmetric attacks.

4.1 Defining the intelligence cycle

The intelligence cycle[51] can be defined as:

[51] Loch K. Johnson, 'Making the "Intelligence" Cycle Work' (1986) 1(4) *International Journal of Intelligence and Counter-Intelligence* 1 for the definitive article on describing the intelligence cycle and how it works. See also, New Zealand Qualifications Authority, *Intelligence Analysis: Demonstrate knowledge of the intelligence analysis process* (2003) New Zealand Government <www.nzqa.govt.nz/nqfdocs/units/doc/18503.doc> The NZQA define intelligence as the collective 'functions, activities, and/or organizations which are involved in the process of planning, gathering and analyzing information of potential value to decision makers, and to the production of intelligence.' See especially, Henry H. Willis, *Using Risk Analysis to Inform Intelligence Analysis* (2007) RAND Corporation <http://www.rand.org/pubs/working_papers/2007/RAND_WR464.pdf> at 7 February 2008 3 who states that the goal of intelligence is to 'produce guidance based on available information

> 'the process by which information and data is collected, evaluated, stored, analyzed, and then produced or placed in some form for dissemination to the intelligence consumer for use. The cycle consists of: consumer, collector, evaluation, analysis, production, dissemination, consumption, consumer.'[52]

Figures 5 shows the main phases carried out in a typical intelligence cycle; the distinct phases have remained relatively unchanged in modern times, save for the addition of the initial "requirements" phase, enabling policy makers to make a request for information (RFI).[53] This phase helps analysts to plan and better direct the intelligence effort. Data is then collected, processed, analyzed and disseminated to the appropriate stakeholders.[54] The U.S. military have developed a sophisticated "Intelligence Process Model" (IPM) that helps analysts to work through RFIs and also for decision-makers to track the status of their request(s).[55]

Figure 5: The intelligence cycle[56]

4.2 The phases of the intelligence cycle

The *request for information* is where information needs are identified by policy makers.[57] In the *planning and direction* phase resources are identified[58] and care is taken to balance the level of intrusiveness of the request with what is legally permissible.[59] The *collection* phase follows and is where the raw information is gathered. Information comes from varied sources- it may be public,

within a time frame that allows for purposeful action.'

[52] United States Government Accountability Office, above 1, 27.

[53] Compare the intelligence cycles of: Lisa Krizan, *Intelligence Essentials for Everyone* (1999) Joint Military Intelligence College <http://www.scip.org/2_getinteless.php> at 5 February 2007 and Directorate of Intelligence, *The Intelligence Cycle* Federal Bureau of Investigations <http://www.fbi.gov/intelligence/di_cycle.htm> at 27 April 2008 1.

[54] US Intelligence Board, *Planning and Direction* (2007) <http://www.intelligence.gov/2-business_cycle1.shtml> at 10 April 2008.

[55] J.O. Miller, *Modeling the U.S. Military Intelligence Process* (2008) Department of Defense <www.dodccrp.org/events/9th_ICCRTS/CD/papers/044.pdf> at 27 April 2008 5.

[56] Directorate of Intelligence, *The Intelligence Cycle* Federal Bureau of Investigations <http://www.fbi.gov/intelligence/di_cycle.htm> at 27 April 2008 1.

[57] Canadian Intelligence Security Service, *Backgrounder No. 3: CSIS and the Security Intelligence Cycle* (2004) <http://www.csis-scrs.gc.ca/en/newsroom/backgrounders/backgrounder03.asp> at 9 March 2008 2.

[58] Miller, above 56, 3.

[59] Canadian Intelligence Security Service, above 58, 2.

foreign or illegally intercepted[60] via satellite or other communication technology, even human intelligence (HUMINT).[61] These sources are combined with open source intelligence (OSINT) including newspapers, periodicals, foreign and domestic broadcasts (eg CNN, BBC, Aljazeera.net) and official documents (eg Commonwealth inquiries).[62] The collected data is then *processed* and made into a form that is usable by analysts. This is often where the most errors creep into the process, as different sources of data are brought together. Maintaining quality in the data sets being processed is of paramount importance. Some have referred to this processing melting pot as the 'fusion centre'. [63] It is how linkages are made between the structured and unstructured data that might be the difference between good and bad intelligence. In the *analysis*[64] *and production* phase, fused data is prepared to make intelligence products which are usually categorized by their primary use (eg indications and warning and counterintelligence).[65] Common analyses performed in these products include association, temporal and spatial charting; and link, financial, content and correlation analysis. [66] The *dissemination* phase can happen in two ways. Intelligence may be delivered to the consumer who requested it in a 'push' action or stored to be 'pulled' at a later date.[67]

[60] Ibid 3. 'In the competitive global economy of the 1990s, acquiring scientific and technological information from other countries has become increasingly important for many nations. Sometimes, this is done by covert or unlawful means.'

[61] Miller, above 56, 4. 'Organizations or agencies that operate collection assets such as satellites or surveillance equipment task those assets to gather information at specified times and places. The means and methods of collection are highly dependent on the source of the information and these sources are generally categorized into various intelligence disciplines.'

[62] Canadian Intelligence Security Service, above 58, 2.

[63] United States Government Accountability Office, above 1, 27.

[64] New Zealand Qualifications Authority, above 52, 2. 'Analysis refers to a process in the production step of the intelligence cycle in which intelligence information is subjected to systematic examination in order to identify significant facts and derive conclusions. The 'raw intelligence' collected, whether by human or technical means, is frequently fragmentary and at times contradictory. Through analysis a sorting, evaluating and interpreting of the various pieces of data occurs including an interpretation of meaning and associated significance.'

[65] Miller, above 56, 4.

[66] United States Government Accountability Office, 'Information Security Management' (U.S. Government, 1998) 27.

[67] Miller, above 56, 4.

5 Integrating risk analysis into the intelligence cycle

5.1 Is risk management and the intelligence cycle linear?

Now that a brief overview of the risk management process and the intelligence cycle have been presented, let us examine the premise that both processes are not linear but network-centric, meshed, and highly collaborative. This does not mean that the actual steps or phases are contested in each process- but the manner in which stakeholders interact with one another is brought into question.[68] The move is revolutionary[69] and towards a network-centric collaboration process using a target-centric approach to interlink stakeholders and information.[70] In the new security environment convergence is acting to bring stakeholders (eg collectors, processors, analysts, policy makers) together to communicate through a centralized means to make decentralized decisions.[71] This does not mean that hierarchy is abandoned altogether in the intelligence community but that stakeholders can make use of technologies which allow for a more agile working environment. The National Infrastructure Protection Plan (NIPP)[72] in the United States presents a context for information sharing amongst the primary stakeholders. It does not mean that the new environment contains members belonging to 'one large happy family', as each organization still differs in their mission and goals.[73]

5.2 Risk management based intelligence (RMBI)

If real-time collaboration is a result of the new security environment, and private and public members of the intelligence community are sharing data (ie contributing and retrieving data), then it follows that processes too can be integrated. In a seminal paper on terrorism, Willis demonstrates how this

[68] R.M. Clark, 'The Intelligence Process' in *Intelligence Analysis: A Target-centric approach* (2004) 12 15. '…The intelligence cycle has become somewhat of a theological concept: No one questions its validity. Yet when pressed many intelligence officers admit that the intelligence process *really doesn't work like that*.'

[69] Deborah G. Barger, *Toward a Revolution in Intelligence Affairs* (2005) <http://www.rand.org/pubs/technical_reports/2005/RAND_TR242.pdf> at 2 February 2008 20.

[70] Clark, above 69, 17-18.

[71] Ibid 17.

[72] Homeland Security, *National Infrastructure Protection Plan Information Sharing* (n.d.) U.S. Homeland Security at 23 April 2008 2. 'The NIPP information-sharing approach constitutes a shift from a strictly hierarchical to a networked model, allowing distribution and access to information both vertically and horizontally, as well as the ability to enable decentralized decision making and actions.'

[73] William J. Lahneman, *The Future of Intelligence Analysis: Volume I, Final Report* (2006) Center for International and Security Studies at Maryland <http://www.cissm.umd.edu/papers/files/future_intel_analysis_final_report1.pdf> 2008 3.

integration is possible (figure 6). The diagram depicts the intelligence cycle on the top right, and then shows how information flows can be applied to enhance risk analysis. Arrows in the figure indicate how information can pass between stages of the intelligence cycle through to the risk management process and back. Willis states that risk analysis can be used to sharpen intelligence products and to prioritize resources for gathering intelligence.[74] He goes on to explain that 'risk analysis can be a tool that can help intelligence practitioners sharpen their conclusions by providing analytic support for identification of scenarios of greatest concern'.[75] It must be noted however, while risk analysis enhances intelligence, it still remains mere intelligence and far from foolproof- especially with regards to the prediction of asymmetric strikes.

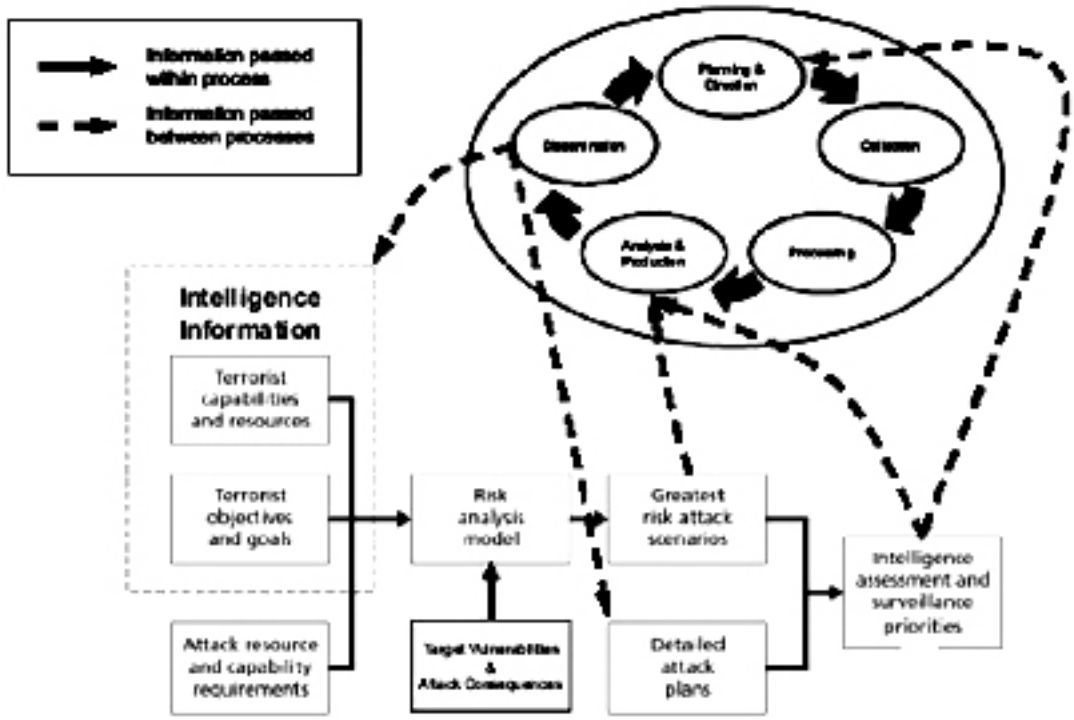

Figure 6: Connections between risk analysis and the intelligence cycle[76]

The integration of the risk management process and the intelligence cycle has been referred to as "risk management based intelligence" (RMBI). RMBI is defined as

> 'an approach to intelligence analysis that has as its object the calculation of the risk attributable to a threat source … a means of

[74] Willis, above 52, 3-4.

[75] Ibid 15.

[76] Willis, above 52.

providing strategic intelligence for planning and policy making especially regarding vulnerabilities and countermeasures designed to prevent criminal acts; a means of providing tactical or operational intelligence in support of operations against a specific threat source, capability or modality; can be quantitative if a proper data base exists to measure likelihood, impact and calculate risk; can be qualitative, subjective and still deliver a reasonably reliable ranking of risk for resource allocation and other decision making in strategic planning and for operations in tactical situations.'[77]

We can denote from the above that risk management is clearly integrated in the modern intelligence cycle; from this integration stems an even closer relationship which we can refer to here as symbiosis- ie, the trend of convergence at multiple levels including organizational,[78] process, product, and information. It is perhaps the latter convergence trend, that of information convergence, that has propelled the cultural shift in the intelligence community at large.[79] When analysts from different organizations (public or private) begin to rely on the same information sources, and are able themselves to contribute information to such causes as critical infrastructure protection (CIP), then opportunities for convergence in products, processes, and organizations emerge.[80]

5.3 Risk intelligence as a business process

If we restate Sherman Kent's classic definition of intelligence being a kind of "knowledge"[81] then we can continue to explore the notion of information

[77] United States Government Accountability Office, above 1, 28.

[78] Kent Anderson, 'Convergence: A holistic approach to risk management' (2007) *Network Security* 4 7.

[79] Peterson, above 9, 1. '… the world is converging around the value of information, not that information is converging around or into something else. Instead, information is the new central actor, defining the enterprise organization and its business. On one hand, information is power and a competitive weapon. In this sense, information is the chief asset of the business. Yet, on the other hand, information is also the chief risk. It is a legal and security liability and we're required to keep it exposed for what seems like forever. In the end, it is this paradox that is the catalyst for change; change which is transforming the Information-Centric Enterprise.' See also, Jill Robinson, *Risk Convergence: Future State* (2007) Ernst & Young Consulting <http://www.ey.com> at 27 April 2008 4 who describes the '… creation of a common data structure for risk and control processes and a common technology architecture supporting this effort. This common ground not only enables the Risk/Control functions to speak a single language, it also fosters communication, greater coordination, and increased understanding.'

[80] Alexandra Psica, *Destination ahead: establishing an effective risk management regime* (1 February 2007) <goliath.ecnext.com/coms2/gi_0199-6288561/Destination-ahead-establishing-an-effective.html> at 27 April 2008 2. 'Whether it's a matter of capturing information for a risk management regime, an audit, or to demonstrate regulatory compliance, the organization should aim to gather it once and use it many times. It's too costly and inefficient to ask the same question multiple times.'

[81] Andrew Rathmell, 'Towards Postmodern Intelligence' (2002) 17(3) *Intelligence and National Security* 88f.

convergence as enabling business processes between members of the intelligence community. In the corporate world, the recognition that 'knowledge' equated to power became prevalent in the 1990s. Organizations were quite aware that there was 'too much information, and too little knowledge'. It was at the turn of the millennium that ICT solutions also became available to solve the problem of 'islands of information' through electronic resource planning systems (ERP), many of which contained a business intelligence module to go beyond data warehousing.[82] It should be no surprise to us then, that today "risk intelligence" (RI) has emerged as a completely new business process.[83] Two consulting companies, Deloitte[84] and Ernst and Young, have already begun to market an RI framework. Figure 7 represents an authentic convergence of the risk management process and the intelligence cycle. Risk intelligence enterprises are those organizations that are characterized by their future vision, ability to bridge silos and speak a common language, conduct impact assessments, weigh up the vulnerabilities, allocate resources appropriately, act with a risk conscious spirit, and even pursue risk for the purposes of higher rewards.[85] The risk intelligent chief information officer (CIO)[86] is someone who practices risk intelligence. And just like any other framework or process, there are differing levels of sophistication that can be attained.[87]

[82] Gill, above 17, 476. 'But the construction of ever-larger databases, data warehousing and data-mining, though of great significance in intelligence, cannot 'solve' intelligence problems without a process of targeting, careful evaluation of information and human analytical skills.'

[83] B. Azvine et al, 'Operational risk management with real-time business intelligence' (2007) 25(1) *BT Technology Journal* 155. Risk intelligence should not be confused with real-time business intelligence (RTBI), despite the fact that the terms are closely allied. RTBI attempts to deliver 3 critical components: 'real-time information delivery, real-time business performance analysis, real-time action on the business processes.'

[84] Robinson, above 80, 4. 'Many organizations are now looking at convergence models to integrate risk and control processes and create a common framework for assessing and monitoring the organization's risks.'

[85] Layton, above 10, 2.

[86] Lee Dittmar and Bill Kobel, 'The Risk Intelligent CIO' (2008) 55(3) *Risk Management* 42.

[87] Nathan Houser and Sean Conlin, *Creating Risk Intelligence: A High Level "How To" Guide for Program Managers* (2006) Deloitte <management.energy.gov/06W_RMconHou.ppt> at 27 April 2008 6.

Figure 7: The risk intelligence framework[88]

5.4 Problems associated with the risk intelligence process

A number of problems plague the intelligence community in the new security environment. It does not mean that risk intelligence will not work, but governments need to understand that these challenges are not trivial, and attempt to combat them with longer-term initiatives. Even if we take the naïve view that implementing convergence is 'easy', we still require competent analysts who understand the data and can deal with the increasing complexity of technical products.[89] For many, the answer lies in professionalizing the security-risk industry. Training programs for analysts by a single accreditation organization is widely recommended. Providing intelligence in a timely manner is another issue, alongside the capability to simplify the information being gathered so it is meaningful and can be applied into action by decision makers.[90] In

[88] Layton, above 10, 5.

[89] Lahneman, above 74, 3. 'The report concluded that, if current practices continue, the intelligence community (IC) of 2020 will experience an imbalance between the demand for effective overall intelligence analysis and the outputs of the individually-oriented elements and outlooks of its various analytic communities.'

[90] Azvine, above 83, 155.

addition, what kind of data will reside in the intelligence system for the conduct of all-source analysis by organizations should not be forgotten as a key challenge- after all garbage in/garbage out (GIGO).[91] Perhaps the biggest challenge at hand however, is governance- how do you bring the intelligence community together within an integrated culture,[92] break down the barrier of secrecy, and still maintain limits to information accessibility based on RFIs. Trust in people and systems, along with enforceable policies and procedures will be paramount in this emerging environment.

6 Conclusion

The overarching benefit of convergence in maintaining national security is strategic, ie keeping one step ahead of the enemy to prevent terrorist attacks in order to minimize the element of surprise. Convergence has the ability to make a reduction in overhead and duplication and to streamline once separate security groups and organizations. [93] Today convergence is about remaining successful;[94] and more than that it is about giving life to new opportunities and emergent benefits that cannot be achieved individually.[95] At the moment the trend towards a unified security program[96] seems to be about reducing risks and increasing control through quality intelligence. However, one could also be critical of the security industry at large and point out, that the trend towards a 'super' converged system is destined to failure because monolithic systems are subject to singularities, and could create more complications than answers. Some may even say the effort towards convergence is a waste of money, time and energy because anti-terrorism capabilities are a fallacy. [97] Is the

[91] Ibid 160. 'Good data often leads to visionary and profitable decision making. Poor data quality is often the cause of bad strategic decisions and inaccurate financial and management reporting.'

[92] Lahneman, above 89, 10. 'The U.S. intelligence community is the "Community that Isn't." It is a series of nearly autonomous organizations, each with its own way of doing business. The analytic portion of the IC reflects the fragmentation of the overall intelligence enterprise. Such a fragmented approach is at odds with the need for greater knowledge sharing to enable effective analysis of dispersed threats and other issues.'

[93] Anderson, above 79, 6.

[94] David Silverstein, *It's All About Convergence* (2007) Inc.com <http://www.inc.com/resources/office/articles/20070601/silverstein.html> at 27 April 2008.

[95] Anderson, above 80, 6.

[96] Ibid.

[97] Gill, above 17, 478. 'Given what is known about the modus operandi of those carrying out the attacks, it is extremely unlikely that such a piece of information exists. Nor was it just a case of the system failing 'to join the dots' between pieces of data so that warning could have been provided though this starts to get closer to the real failure of US intelligence: the failure of processing and analysis.'

technology[98] available today propelling us all toward a future environment that may create even more problems for us as a society? Time will tell.

[98] Pathak, above 8, 569. 'This shift is being driven by the "convergence" of IT security methods with those of the more traditional physical security methods.'