Globalisation and Its Impact on Military Intelligence

by CPT (NS) Fu Wen Hao, Kelvin

Abstract:

Global intelligence communities are wrestling with the tidal changes that are happening around the world, coming to terms with the rapid pace of change that has come to characterise the 21st century. These changes have been exacerbated by globalisation, which has caused tremendous changes in the global, political, social, cultural and security landscape. The revolution in military affairs, which was built on information technology and communication revolution, heralded a dramatic shift in the way militaries conduct warfare, paving the way for the integration of complex command and control systems and the fusion of various types of firepower into highly coordinated military operations. The following essay will argue how globalisation has led to greater intensification of the interactions among people, ideas, economies, governments and nations which greatly redefine the way militaries must realign their strategy.

Keywords: Globalisation, Unconventional Threats, Intelligence Communities, Information Collection, Impacts

INTRODUCTION

Intelligence communities globally are wrestling with the tidal changes that are happening in the world and are coming to terms with the rapid pace of change that has come to characterise the world in the 21st century. These changes have been exacerbated by the phenomenon that we commonly term as globalisation which has caused tremendous changes in the global, political, economic, social, cultural and security environments.

The revolution in military affairs heralded a dramatic shift in the way militaries will conduct warfare where they not only have to contend with the land, sea, air, space dimensions of warfare but also the dimension of information warfare. According to Andrew Marshall, Director of the Office of Net Assessments in the Office of the Secretary of Defence:

> *A revolution in military affairs is a major change in the nature of warfare brought about by the innovative application of new technologies which, combined with dramatic changes in military doctrine as well as operational and organisational concepts, fundamentally alters the character and conduct of military operations.*[1]

The revolution in military affairs was built on the information technology and communication revolution which paved the way for the integration of complex command and control systems together with the fusion of various types of firepower into highly coordinated military operations. Yet, the revolution in military affairs seems to have bypassed the intelligence communities as it appears to be falling behind the technological marvels of 21st century warfare.

Advances in technology and the interconnectedness of the world have meant that the information environment has exhibited phenomenal growth. The advances in the intelligence gathering capabilities which capture data (often) indiscriminately have also meant that there are risks of information overload. The lack of information specificity, in the case of 9/11, had prevented the intelligence community from developing a clear and comprehensive threat picture prior to the attacks.[2] Indeed, the information revolution may be accelerating faster than the intelligence community's ability to keep pace.[3]

Globalisation, defined as the growing interconnectedness and growing interdependence of communities around the world, is multifaceted as it encompasses security, political, social and cultural ramifications for the relations between states and non-states entities. The expanding web of interdependence should not lead one into thinking that the occurrence of war has been reduced. The potential for wars or conflicts remain fundamentally unchanged as there are many unresolved disputes ranging from sovereign, territorial, political and social disputes. As the political, economic and social relations among the major powers shift and as these shifts are further exacerbated by globalisation, the likelihood for tensions persists.[4] Moreover, globalisation contributes to political alienation, radical ideologies, religion fused with ethnic conflict and the proliferation of non-state and sub-state actors on the global stage. It also facilitates transnational networks of terrorists by giving them access to technology and weapons that threaten national security. The result for military intelligence is a complex array of threats, potential threats and a formidable set of challenges that it will have to overcome to remain relevant in today's globalised security environment.

The expanding web of interdependence should not lead one into thinking that the occurrence of war has been reduced. The potential for wars or conflicts remain fundamentally unchanged as there are many unresolved disputes ranging from sovereign, territorial, political and social disputes.

Producing useful military intelligence—information needed or sought-after by the military in pursuance of mission objectives—poses significant challenges. It requires a complex integration of many of the intelligence community's sophisticated technological capabilities to collect data, process and analyse the data to produce useful analysis for the decision makers in a timely and accurate fashion. Military intelligence is not limited to a tactical level of intelligence as the new security environment entails a multidisciplinary approach which, *inter alia*, encompasses political, economic, military and tactical considerations. It requires the intelligence community to incorporate interpretations of intents of the adversary as well as its physical capabilities and actions. Military intelligence is also about understanding intentions. It is about knowing and understanding as much as possible about actual and potential adversaries and competitors. It is about self-awareness, about understanding one's own capabilities, strengths and vulnerabilities so that effective counter exploitation measures can be developed and adopted. In short, military intelligence is about knowing the information environment from all angles and achieving superiority over the information space.[5]

In this paper, I will argue that globalisation has led to greater intensification of the interactions among people, ideas, economies, governments and nations which greatly redefine the way militaries must realign their strategy. Military intelligence, as the basis for all military operations, must therefore realign their collection and analytical functions. Although the technological aspects of globalisation has revolutionised the way military intelligence is conducted, technology does not provide all the answers. Useful military intelligence cannot be reduced to the mundane scientific competence of information collection and analysis. The element of strategic surprises cannot be eliminated and there are persistent risks of misperception and miscalculations. In order to make sense of the globalised world and to stay relevant, military intelligence must rely on both scientific competency through technical intelligence and human competency through human intelligence.

This paper is organised into three main sections. First, I will discuss the impacts of globalisation on the security environment, the type of warfare fought and the changes in military affairs. This will lead on to the second section which will discuss the changing role of military intelligence. Third, I will address the challenges of producing useful military intelligence and propose an alternative way of restructuring military intelligence with greater emphasis on human intelligence. Throughout this paper, I will be using selective examples of military intelligence failures to support my argument and show how globalisation has intensified and increased the level of uncertainties in intelligence estimates. A thorough understanding of the impacts of globalisation on military intelligence will be an important step in preparing for the new globalised security environment that is emerging.

GLOBALISATION AND THE NEW SECURITY ENVIRONMENT

Carl von Clausewitz said that the first principle of strategic thinking is to understand the nature of the war that one is embarking on and today, we have a very different security environment. Globalisation is not a new phenomenon but the pace and depth of the changes currently being ushered in by this process has major implications for the conduct of warfare and military intelligence. The type of warfare conducted will directly affect the type of military intelligence to be gathered, the way it is analysed, disseminated and acted upon. Hence, in order to understand the impacts of globalisation on military intelligence, we must first understand the impacts of globalisation on the type of warfare conducted in the new security environment.

In the post-Cold War period, the world is shifting towards an emerging multilateral world which is seeing a surge of states and non-states entities competing for influence in global affairs. Traditionally, security threats have been defined in geo-political terms encompassing aspects such as deterrence, power balancing and military strategy. These aspects are by no means irrelevant given the continued salience of the state. Traditional hard security issues will continue to be a major underpinning in inter-state relations but one cannot purely focus on hard security issues. The threat of inter-state war does not constitute the sole cause of insecurity. The new threats include outbreaks of ethnic conflicts, problems of identity in many developing parts of the world, the contagious impact of economic crises in an increasingly integrated global economy and related issues of governance and institutional development. The impact of this broad range of security threats has been magnified by globalisation, which has become increasingly evident since the early 1990s.

The paradoxes of this globalised age are two fold: first, modern technology is both the great separator and the great equaliser in military; second, greater interdependence and greater interaction between communities have not necessarily reduced the level of conflicts in the world. The processes driving globalisation are not new phenomena but have intensified due to the dramatic developments in telecommunications, information technology and transport, which has eroded traditional economic boundaries and transnationalised the impact of local issues and problems. As governments open up their countries in an attempt to reap some of the financial benefits of participation in the global information economy, they leave themselves open to social and political effects of change. Moreover, information age technologies of the internet and computers have provided new channels for international crime and terrorism.[6]

With the increasing interdependence brought about by globalisation, people and cultures are being brought together wittingly or unwittingly. This creates interaction between people and communities that may or may not necessarily understand or accept one another. The anti-globalisation movement has more often than not been a movement of anti-Westernisation, where people rally and protest again the perceived notions of cultural imperialism by the West. The clash of civilisation thesis as coined by Samuel Huntington, explored the notion that conflicts in the future would be fought along the lines of cultures and peoples who share different and unique cultural practices and belief systems.[7] While some scholars have dismissed the clash of civilisation thesis as overly exaggerated, Huntington's thesis is an important one to consider in the light of the rapid pace of globalisation which could lead to the aggravation of differences and foster greater misunderstandings. Other academic scholars have also built upon his thesis to take into account the clash of ideas and ideologies to help explain the rise of religious extremism, radicalism and terrorism.

Unconventional threats such as terrorism, counterinsurgency operations cannot be defeated with conventional forces. In the case of counterinsurgency warfare, there is a fundamental paradox that too much aggression can be counterproductive and that a 'softer' approach can actually produce better results. The rising threats of asymmetric tactics employed by weaker state and non-state entities against stronger adversaries are a manifestation of the leveraging of the duality and utility of the forces of globalisation in order to exert disproportionate power. In the globalised age, Clausewitz's notion of war as a 'clash of two living forces' would prove to be salient where globalisation can be seen as either a great equaliser or separator, depending on the nature of the actor and its ability to harness the forces of globalisation. Max Boot, Senior Fellow for National Security Studies at the Council on Foreign Relations asserted that:

> *[Future revolutions] are likely to take warfare in strange and unexpected directions, many of which will empower small states and sub-state groups at the expense of large nation-states…Yet, the focus on cutting-edge technology is in no way meant to suggest that political or organizational developments will not be important in the future; the nature of war will always be determined by the interaction between warriors and their tools, not by the tools alone.*[8]

The changes in military power brought by the information revolution are still in their early stages and they still have serious limitations. Even the best surveillance systems can be stymied by simple countermeasures like camouflage, smoke and decoys, by bad weather, or by terrain like the deep sea, mountains or jungles. Sensors have limited ability to penetrate solid objects, so that they cannot tell what is happening in underground bunkers such as those that North Korea and Iran are likely to use to hide their nuclear weapons programmes. Urban areas present a particularly difficult challenge: there are far more things to track (individuals) and far more obstructions (buildings, vehicles, trees, signs) than at sea or in the sky. Figuring out whether a person is a civilian or an insurgent is a lot harder than figuring out whether an unidentified aircraft is a civilian airliner or an enemy fighter. It is harder still to figure out how many enemy soldiers will resist or what stratagems they will employ. No machine has yet been invented that can penetrate human thought processes. Even with the best equipment in the world, militaries around the world frequently have been surprised by their adversaries. Some strategists expect that advances in information technology will greatly diminish if not altogether obliterate some of these difficulties.

Yet no matter how far information technology advances, it is doubtful that militaries will ever succeed, as some utopians dream, in 'lifting the fog of war.' The fallibility of soldiers and the cunningness of their enemies will surely continue to frustrate the best-laid plans. Moreover, societies that are increasingly reliant on high-tech systems create new vulnerabilities of their own: Future enemies have strong incentives to attack computer and communication nodes. Strikes on military information networks could blind or paralyse the armed forces, while strikes on civilian infrastructure, such as banking or air control systems, could cause chaos on the domestic front. Adversaries will almost certainly figure out ways to blunt the informational advantage. For example, whether fighting in the mountains of eastern Afghanistan or in the alleys of Ramadi and Fallujah, U.S. soldiers have been ambushed by insurgents who managed to elude their sensor networks through such simple expedients as communicating via messengers, not cell phones.

This is, however, not to suggest that globalisation has entirely reduced the likelihood of inter-state war and focused militaries exclusively on waging 'small wars.' There is still a need to be able to fight large, conventional conflicts against potential state adversaries, if only to prevent them from happening in the first place. The point is that regular armed forces must gain greater competency in unconventional warfare such as counterinsurgency and related disciplines in order to account for the new security environment that they are operating in.

IMPACTS OF GLOBALISATION ON MILITARY INTELLIGENCE

Military intelligence is concerned with the gathering and analysis of information related to the distribution of capabilities and the perceptions of threat of the adversary. Indeed, Sun Tzu emphasised the crucial role of intelligence as a battle of wits, mind and strategy prior to the actual physical conduct of war. It must first be acknowledged that military intelligence agencies in the world, depending on the country's political system and structure, are diverse in the roles and functions. Some countries restrict the role of military intelligence to strictly that of supporting tactical operations on the battlefield; whereas others take up additional roles in supporting the higher level intelligence demands such as strategic intelligence. In this paper, I will be discussing military intelligence in a general sense as one that plays a supporting role for military operations and functions as crucial inputs for higher level intelligence analysis such as strategic intelligence.

The need for intelligence and for a capability to collect, produce and disseminate it, remains critical. The end of the Cold War has not ushered in an age of peace and security. Nor is the need for intelligence eliminated by new sources of open information. There are still important but hard to learn facts about targets including the intentions and capabilities of rogue states and terrorists, the proliferation of unconventional weapons and the disposition of potentially hostile military forces that can only be identified, monitored and measured through dedicated intelligence assets.[9]

In the post-Cold War world, the intelligence community will need to adjust to the reality that the world is a less structured one, one in which power in all its forms: economic, political and military is more diffuse. It will also have to contend with a world that not only is more open and transparent than ever, but also one that contains large and important areas that remain virtually closed to those dependent on normal means of transportation and communication.

In the post-Cold War world, the intelligence community will need to adjust to the reality that the world is a less structured one, one in which power in all its forms: economic, political and military is more diffuse.

The information and technological revolutions have posed formidable sets of challenges for the intelligence community. Information is the root of all intelligence production and it has become the principle commodity in today's world.[10] The technology revolution has fuelled the rise of greater global interdependence and interconnectedness. The digitisation of information and ease of access to communication technology present both challenges and opportunities for the intelligence community. The strategic deployment of signals and electronic intelligence can effectively intercept electronic communications. This is a form of passive intelligence collection where there is no discrimination of any information that passes through the networks. This wealth of information is fed into the intelligence cycle, data-mined and prepared for analysis and dissemination. Technology driven globalisation and increased technological capabilities have fostered positive growth and evolution in collection, processing and analytic capabilities. Yet, it has also stimulated the capabilities of the targets which can make use of the same technology to disrupt and counter intelligence collection efforts against them. In short, technology and information revolution is a double-edged sword.

The commercialisation of technology and the proliferation of highly sophisticated technologies available off the shelves have also meant that technology capabilities that were once the monopoly of highly secretive intelligence agencies are now available to anyone who is willing to pay for it. In some cases, governments have imposed restrictions on the export of sensitive technology but this would hardly stop a determined group from going around these restrictions. Encryption mechanisms available to the market are capable of reaching military grade levels which will in turn challenge the code breaking abilities of intelligence agencies. Terrorists have also been known to employ sophisticated cryptology techniques such as steganography—the art or science of embedding hidden messages into a medium for the intended party—and encryption to thwart intelligence collection efforts.

The new security environment, information and technological revolution means that intelligence communities have to adapt and keep up with the changes, invest in bolstering information collection and analysis capabilities, manage effectively the intelligence cycle and stay relevant. Military intelligence is not simply about harnessing technology to collect and analyse information about the target. The core of military intelligence is to assess the capabilities, intentions and activities of the targets. This will not be accomplished simply by employing methodological processes that mine the wealth of data in search of patterns and trends that can provide insights into the target. Technology and technical competence can help but, in the new security environment marked by nuances, subtle political gesturing and signalling activities combined with the ability of the target to employ counter measures to circumvent the best efforts of the intelligence communities, there is no replacement for an experienced, well-trained analyst that can harness all available resources to produce informed assessments.

Technology provides the enabling capabilities necessary to understand and exploit the growing global information network through the development and deployment of sensor-based automated collection systems.[11] However, information such as hostile intentions harboured secretly by unfriendly governments and the disposition of hostile military forces are rarely available on the information superhighway or through commercial satellite imagery; it is certainly not available with enough detail and timeliness to serve policymakers and combatants. To the contrary, there are a number of threats to a state's interests and well-being that can only be identified, monitored, and measured adequately by using dedicated intelligence assets. Knowing the target's order of battle says little about its goals and willingness to use the resources at its disposal. To this end, the revolution in information and technological revolution must be tackled by a revolution in intelligence affairs with greater emphasis on human intelligence.

HUMAN INTELLIGENCE: THE BEDROCK OF INTELLIGENCE

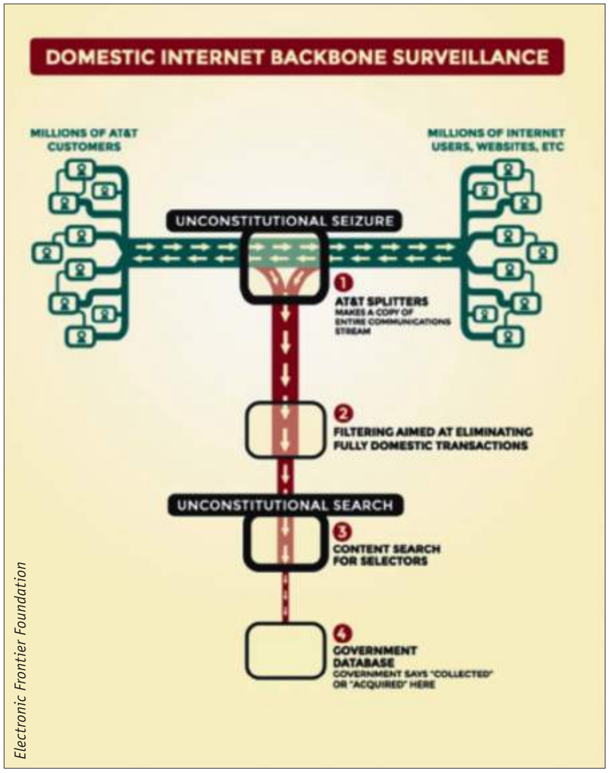
The most advanced weapons systems and most sophisticated information technology is hardly a perfect shield against other kinds of destructive power. Likewise, the most advanced technical intelligence gathering systems will not be sufficient to combat the new threats posed by the new security environment. To this end, human intelligence is required to complement the technical intelligence assets. Human intelligence is the collection of information from human sources which includes the employment of espionage, reconnaissance elements and intelligence officials under official or non-official 'cover' to procure information. Sun Tzu recognised the importance of human intelligence in gaining strategic insights about the target:

What is called foreknowledge cannot be elicited from sprits, nor from gods, or by analogy with past events nor from calculations. It must be obtained from men who know the enemy situation.[12]

Technology and technical competence can help but, in the new security environment marked by nuances, subtle political gesturing and signalling activities combined with the ability of the target to employ counter measures to circumvent the best efforts of the intelligence communities, there is no replacement for an experienced, well-trained analyst that can harness all available resources to produce informed assessments.

Human intelligence is one of the myriad of intelligence assets employed by intelligence communities to collect information. It differs from the other technical sources of intelligence which are heavily reliant on the technical competency and deployment of technology to collect information. Signal intelligence derives intelligence from intercepted electromagnetic waves and communications. Imagery intelligence involves photography to collect intelligence.[13] In recent years, the sheer technological prowess in creating sophisticated collection devices has been unparalleled. This is further exacerbated by the willingness of certain Western governments to suspend privacy and legality concerns in the name of national security in order to extend snooping programmes on its citizens. The exposure of the clandestine National Security Agency wiretapping programme on U.S. citizens demonstrated the extent to which technical intelligence can be deployed silently and effectively against societies that are underpinned and reliant on information and communication technologies.[14] Moreover, the co-option of private enterprises to aid the intelligence collection efforts signal the wide-ranging reach of intelligence assets that are not limited to government deployed intelligence assets. AT&T, one of the largest telecommunications enterprises in the U.S. was found to be complicit in aiding the secret wiretapping programme for the U.S. government.[15]

In a world of increasing interconnectedness and reliance on communication networks and computers, technical intelligence competency can easily lead to an overestimation of what technical intelligence can accomplish and a concomitant depreciation of human intelligence.[17] Imagery intelligence can clearly show the military build-up at an exposed location such as in the case of Iraq's army massing on the Kuwaiti border in July 1990. However, it could not illuminate Saddam Hussein's intention or reasons for the build-up. In other words, understanding the target's intentions, strategy, perceptions of the situation is also crucial for assessment into useful military intelligence. In this view, a human intelligence source would prove to be invaluable as it could provide the essential first


DOMESTIC INTERNET BACKBONE SURVEILLANCE
MILLIONS OF AT&T CUSTOMERS
MILLIONS OF INTERNET USERS, WEBSITES, ETC
UNCONSTITUTIONAL SEIZURE
1 AT&T SPLITTERS
MAKES A COPY OF ENTIRE COMMUNICATIONS STREAM
2 FILTERING AIMED AT ELIMINATING FULLY DOMESTIC TRANSACTIONS
UNCONSTITUTIONAL SEARCH
3 CONTENT SEARCH FOR SELECTORS
4 GOVERNMENT DATABASE
GOVERNMENT SAYS "COLLECTED" OR "ACQUIRED" HERE
Electronic Frontier Foundation

The framework of AT&T's domestic internet surveillance[16] indication that something of interest is occurring or would occur at a given location through its infiltration of the target's circle of trust and domain.[18]

The meaningful collection of information through technical intelligence is based on the assumption that there is sufficient information to be collected from the target that can be analysed through scientific competency. In addition, it assumes that the information gathered will be susceptible to a methodological and rational process of analysis in order to yield useful intelligence. The biggest stumbling block for technical intelligence is that it is unable to provide insights into the intangibles of perceptions and misperceptions. Robert Jervis views on how misperception is common throughout international relations are not hopeful for students of intelligence analysis.[19]

Correctly identifying the technical intelligence collection system for the procurement of sensitive information may be a virtually insoluble task. This is especially so when the target employs sophisticated countermeasures to circumvent the technical collection system. Alternatively, one can exploit the assumptions of the technical collection by reverting to primitive technology for communications or to minimise the use of fixed facilities or communications. In this case, human intelligence will be necessary to infiltrate the group and collect intelligence.

Satellite Image from a commercial satellite, Soyuz Karta showing vehicles massed around Kuwaiti oil fields – September 11th 1990.[20]

That said, the role of technical intelligence and human intelligence can serve complementary roles as they provide distinct kinds of information. There are systems that are more suitable for certain situations and some are more reliable in others. In order to have useful intelligence, it would be crucial to rely on as many sources of intelligence as possible to fill in information gaps and to assess the intentions, capabilities and actions of the target. To this end, a mere reliance on scientific competency of information collection and analysis would be inadequate to fulfil the needs of the new security environment.

STRATEGIC INTELLIGENCE ANALYSIS AND ASSESSMENT

The attacks of 11th September, 2001 on the World Trade Centre underscored the growing challenges to intelligence in the new security environment where small groups of individuals can inflict destruction that was once the monopoly of nation-states. The threat of non-state actors that wield disproportionate power relative to the resources is a manifestation of the increasingly globalised world. The general conclusion of the various inquiries into what went wrong that allowed 9/11 to happen with respect to intelligence analysis, was that there had been a failure of imagination or a failure to 'connect the dots.' There had been warning signs of attacks on the U.S. but analysts had failed to integrate the various information together to form a holistic picture. The analysis tended to *"be risk averse and more concerned with avoiding mistakes than with imagining surprises."*[21] Indeed, mental roadblocks to more imaginative analysis are persistent challenges. The essence of analysis is information plus insight, derived from subject matter knowledge. Intelligence analysis informs decisions and acts in ways that make a positive difference. Timely intelligence warns of looming crises, identifies threats, monitors fast-breaking situations, illuminate issues and detect threats. In sum, timely and well informed analysis underpinned by reliable information, is crucial for useful intelligence.

The role of intelligence assessment is to provide actionable knowledge or anticipatory warning to decision makers. This actionable knowledge should anticipate risk through foresight into complex situations.[22] At the heart of intelligence assessment lays the issue of predictability and risk management. Leaders of all sorts want control over the organisation they lead and the environment in which they operate.[23] The predictive ability, however, has never reached a level of capability where strategic surprise has been removed as a function of international relations.[24] In other words, there can be no assurance that strategic surprise will not happen again.

There is no room in intelligence analysis for partisan advocacy or opposition when providing actionable intelligence and identifying options. Analysts must check their personal political views at the door. The policy making customers that analysts seek to inform need to get clear, politically neutral, objective and intellectually honest analysis in order for it to be useful. The overwhelming flow of information poses increasing demands and expectations on the intelligence analysts as the range of possibilities is infinite, while the amounts of mental energy and man hours of analysts are finite. Moreover, there will be great deal of uncertainty that analysts have to grope through to come up with the finished product.[25]

The fact that developments worldwide are reported in real time contributes to an atmosphere of perpetual crisis, of needing to respond instantly to anything and everything—an atmosphere in which current intelligence carries the day. This overemphasis on current intelligence works to the detriment of in-depth analysis and reduces the utility to strategic intelligence. However, the fact remains that decision makers want and need both strategic (long term) and current (immediate) analysis. The key is the ability to integrate both types of analysis and to produce actionable intelligence for policy makers. This leads to the question of resource scarcity and allocation. Clearly, the way forward would then be to invest more heavily in improving the efficiency of the intelligence officers and to also provide them with more competent resources such as adding more manpower.

One can only hope to reduce the severity—to be only partly surprised, to issue clearer warnings, to gain a few days for better preparations and to be more adequately prepared to minimise the damage once a surprise attack occurs.[26] Indeed, in some sense, leadership is precisely about an understanding of and ability to master intuition and practical wisdom about other's situations.[27] Understanding the psyche, the nuances of the human mind and dynamics of culture and relationship requires specialised and privileged information. It requires a depth of knowledge, humility about our ability to understand and predict and a holy fear of the power of contingency.[28]

> *Managing knowledge to sustain [the] information edge is less about infrastructure than leadership, engendering cultural change, encouraging entrepreneurial analysis and learning to accept risk, whether in operational, informational or acquisition processes. It requires focus and innovation at every level, with an active public debate about the strategic effectiveness and future direction of … intelligence.*[29]

To this end, the key to providing actionable intelligence is to have strong leadership, a willingness to accept cultural changes, the encouragement of entrepreneurial analysis and a more risk-tolerant culture.

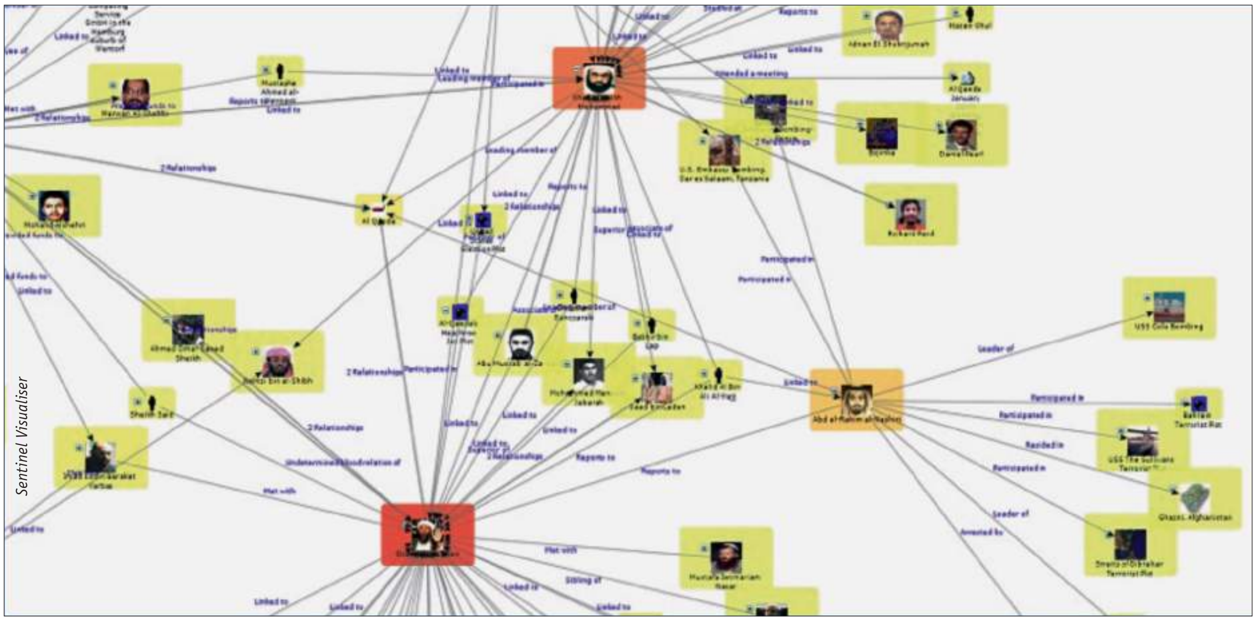
THE RELEVANCE OF SCIENTIFIC COMPETENCY

As the means of producing and transmitting information increases, so does the volume. The rapid increases in both technology and volume have created many more opportunities for distortion of that information.[30] Thomas Quiggin asserts that 1. the failure to share information (stove-piping); 2. the failure to adapt to the new information (mindsets); and 3. the imbalance of resources applied in the intelligence process are, to a large extent, responsible for the continuous failure of intelligence.[31] According to his analysis, intelligence agencies spend close to 99% of budget spending on technology, infrastructure and various systems and only the most minor portion of the budget on analysis. The increasing sophistication of technical intelligence and the preoccupation with building up capabilities has come at the expense of analytical capabilities. Robert David Steele, former case officer at the Central Intelligence Agency (CIA) and Chief Executive Officer of an open source intelligence provider summarised this imbalance of resources and the need to harness technology effectively as such:

> *Information technology has imposed on the policy maker financial, productivity, secrecy and opportunity costs. Billions of dollars are being wasted through a lack of coordination and standardisation…Information technology continues to offer extraordinary promise, but only if the policy maker begins to manage the technology rather than abdicate technology procurement decisions to technologists far removed from the core competencies of the policy environment.*[32]

The pursuit of technology at the expense of personnel may lead to a less capable analysis community in the future. Clearly, technology cannot provide all the solutions for the intelligence community. But, it can, if harnessed correctly, provide significant leverage, speed and efficiency in helping to manage the information flow. Bearing in the mind the limitations of human capacity, technology can then help to supplement and complement the capabilities. Technology and software algorithms provide the methodological and thorough processes by sifting through masses of information in a much faster time then the human mind can.

In a bid to help intelligence analysts connect the dots and make sense of the myriad of information available, software have been developed to address these needs. Tangram, funded by the CIA's own



An example of Network Metrics generated by Sentinel Visualiser. This feature makes it easy to visually acquire meaning in even the most complex inter-related data.[33]

venture capital arm In-Q-Tel, is envisioned as a fully automated, continuously operating and intelligence analysis support system.[34] Tangram aims to assist the analyst in gaining insights into behavioural patterns, relationships, intentions and methods through sophisticated software algorithms and logical patterns. Another software called Sentinel Visualiser is pitched as a tool that provides a powerful new generation of visualisation and analytical capabilities that allows the user to form new insight, patterns, and trends hidden in existing data leading to accurate and actionable intelligence.[35] The accuracy of this analytical software is still unknown and it may not be able to fully address the demanding needs of intelligence analysis in today's world yet. However, the deliberate attempts by the private sector and government sector to capitalise on technology to assist in the improvement of intelligence analysis cannot be discounted.

In the above sections, I have highlighted the importance of the human capacity and its ability to go beyond simple bean counting and technical analysis. I have also shown the risks of the imbalance of resources that are overly in favour of technology. I do, however, acknowledge the potential advantages that technology and scientific competency can provide if harnessed correctly. The software algorithms aim to help analysts connect the dots may not be mature enough for actual deployment in real situations but it adds to the tool kit of the intelligence analyst. The potential rewards for getting the right mix of technology and leveraging on it could mean a paradigmatic shift that the intelligence community has been looking for all these years.

TENSIONS BETWEEN THE INTELLIGENCE COMMUNITY AND DECISION MAKERS

The previous sections have highlighted the preliminary steps of the intelligence cycle and focused on how the information is collected, analysed and disseminated. Regardless of the intelligence product that is disseminated, the key determinant to whether the policy makers view this product as useful or not is highly subjective. Arthur Hulnick, a veteran in the intelligence services serving in the U.S. Air Force Intelligence and CIA, argues that the intelligence collection process is driven by the system to fill the intelligence gaps and not driven by policy makers.[36] The key is to ensure the independence of the intelligence analysts and to underscore the importance of political and policy detachment when it comes to producing relevant and effective finished intelligence.[37]

This does not mean that the intelligence managers and policy makers are to be kept separate. Policy makers do give some guidance and inputs to intelligence managers to come up with the product that is most relevant to the demands of the policy makers. Indeed, *"[t]he national interest is best served when the two camps work together to combine sound intelligence analysis with sound policy analysis."*[38] This is the ideal case where the two camps do work together. More often than not, there are tensions between the intelligence community and the decision makers (the policy makers) because of the difference in professional mission and goals:

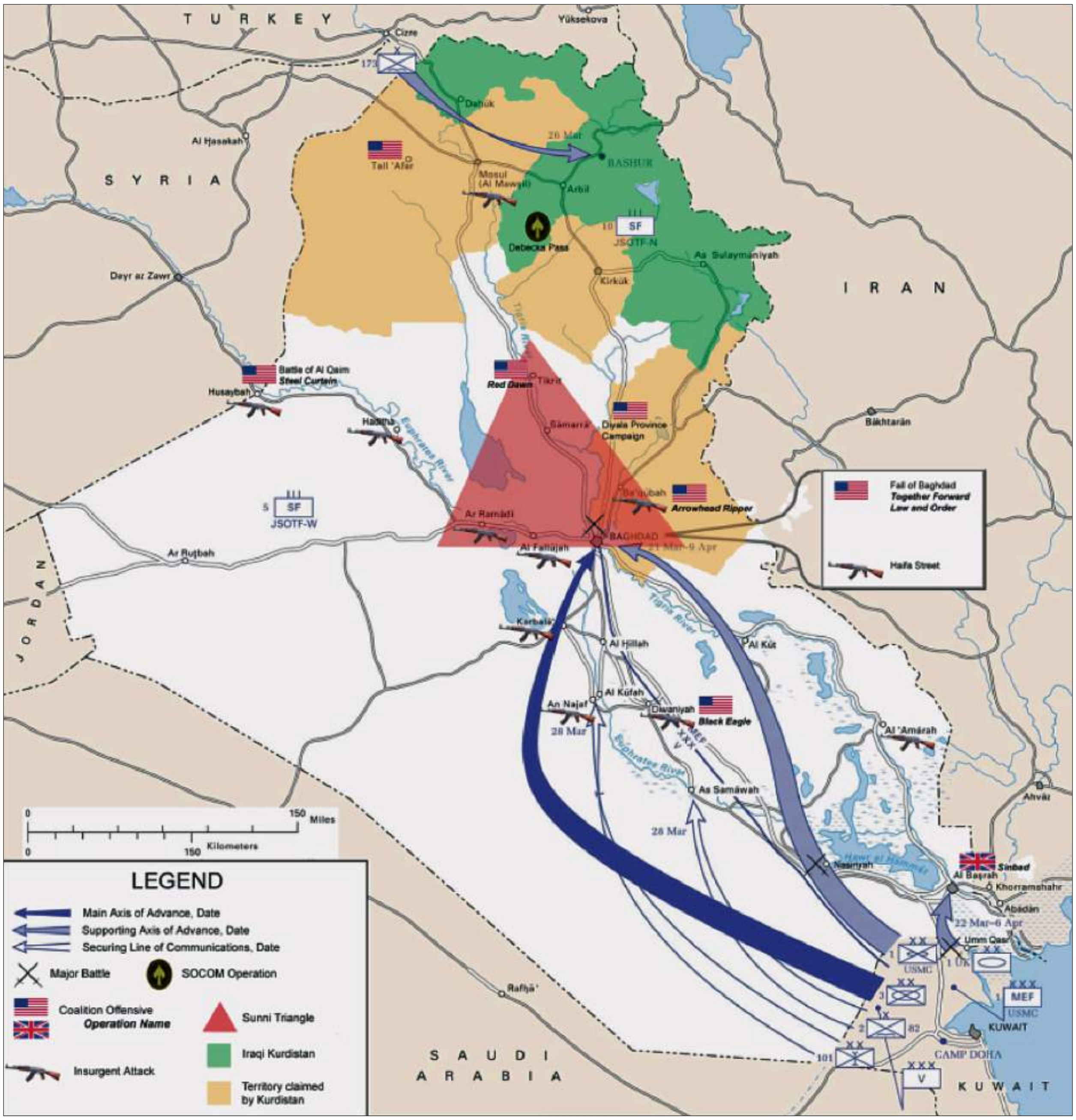
> *The analyst's professional commitment is to assess national security issues without bias for or against the outcomes sought by the incumbent presidential administration; the policy maker's professional commitment is to articulate, advocate, and advance the administration's national security agenda.*[39]

Apart from the different goals and missions of both parties, Robert M. Gates, former Director of Central Intelligence, argued against the need to keep both parties detached. He argued for closer working relations with policy makers in order to produce actionable intelligence that will be of immediate and direct use to policy makers.[40] In this view, analysts must be aware of the needs of policy makers and intelligence managers have an obligation to task analysts so that they can produce useful intelligence for their clientele.[41]

Intelligence communities have unrivalled access to sources of privileged information – information that is not privy to others that are often obtained through covert means—that may help to shed light on motivations, intentions and reduce the uncertainty that *"fogs complex world events."*[42] The production of useful military intelligence must then be guided by analytic professionalism that emphasises objectivity (defined as tough minded evaluation of evidence and other sound analytic practices) and utility (defined as distinctive data and insights policy officials find useful for managing threats to and opportunities for advancing national interests).[43] The challenge for analysts is to turn these tensions into professional advantage by maintaining rigorous, analytic tradecraft standards while enhancing the utility of their assessments to policy makers.[44]

Sherman Kent, a Yale professor who established the national estimates system in the CIA, argued that the best way to avoid politicisation of intelligence—where policy makers place overt or subtle pressure on intelligence analysts and managers to produce intelligence estimates that support current political preferences or policies—was to remain distant and aloof.[45] Kent's approach guards against politicisation because it creates real procedural and even physical barriers that prevent policy makers from influencing the questions addressed and answers presented in finished intelligence.[46] Yet, by distancing and setting up barriers between policy makers and intelligence analysts, it may result in a disjuncture between the demands of the consumers and the final product which would be of little utility.

On the other hand, Roger Hillsman, one of the intelligence chiefs at the State Department argued that intelligence had to be close to policy to remain relevant.[47] If one were to look at the case of the recent Iraq war, it would appear that Kent was right. The intelligence system was politicised to come up with estimates that met the needs of the George W. Bush administration which was looking to provide justifications for the already planned invasion of Iraq. The assessment that Saddam Hussein possessed weapons of mass destruction was based on faulty assumptions and unreliable sources. Yet, senior intelligence managers were only too keen to satisfy the



Map of major operations and battles of the Iraq War as of 2007

political needs of the White house.[48] In this case, the scientific competence of information collection and analysis had fallen victim to the political machinery that was highly selective in its use of intelligence.

The case of the Iraq war highlights another important factor in the production of intelligence and that is the consumers themselves. There must be good communication between the policy consumers and intelligence managers if intelligence is to be on target and meet the needs of decision makers. At the same time, intelligence managers must be able to stand up to efforts by policy officials that attempt to massage or skew intelligence products. Moreover, some policy consumers will not easily admit or welcome intelligence that runs counter to their own judgments.[49]

INTELLIGENCE FAILURE

The failure of intelligence and other systems can be attributed to a large extent on factors related to the human capacity and the fact that humans have cognitive bias or preconceived notions that can colour the perceptions and judgment. Some of the pitfalls include: 1. mirror imaging—the assumption that others would have the same values and though processes as you; 2. Groupthink—the tendency to have one's interpretation reinforced by others coming to the same conclusion; 3. failure to adapt to new information or changes—assessments made under one set of conditions frequently are not reassessed or challenged when new information becomes available; and 4. perceptions and misperceptions—one's own intentions influence the perceptions of enemy intentions. Misunderstanding the target's character will affect how accurate the analyst assesses the target.[50]

In other words, globalisation has not significantly reduced intelligence failure even though it supposedly fosters greater interdependence and intensifies the interactions between people, communities and states. Strategic surprises may remain the norm as intelligence analysts attempt to 'make some sense out of the apparent incoherence of the world scene' where there is imperfect information and pressures to produce timely intelligence products.

For all the above reasons, it can be stated that most of the problems above, derive directly from the problem areas of knowledge and assessment, not data and information. Greater emphasis on improving the collection systems or improving methodological processes of analysis alone would not result in significant improvement because of the dynamic nature of intelligence and the existence of too many unknowns. Intelligence failure, in this regard, can be seen as an inevitable occurrence; it would be impossible to achieve full predictability in intelligence assessment. In other words, globalisation has not significantly reduced intelligence failure even though it supposedly fosters greater interdependence and intensifies the interactions between people, communities and states. Strategic surprises may remain the norm as intelligence analysts attempt to 'make some sense out of the apparent incoherence of the world scene' where there is imperfect information and pressures to produce timely intelligence products.[51]

CONCLUSION

In this paper, I have shown how the processes of globalisation have impacted the security environment and the way militaries have had to adjust to the new conditions. Globalisation provides an environment where the infrastructure for information sharing is available and greater interdependence between communities could have the potential to reduce strategic surprises and intelligence failures. Yet, conflicts, wars and strategic surprises persist. Further, globalisation has increased the level of potential security threats and uncertainties that are in part the result of political alienation, spread of radical ideologies, extremism and terrorism. I have also shown the limitations of the human capacity and the intelligence failures that could result from the inherent cognitive bias and preconceived notions that colour analysts' perceptions and judgments. To this end, intelligence failures may be inevitable but there are ways that we can mitigate or identify these failures early in order to rectify them. This can be achieved through greater investment in shoring up the capabilities of the human capacity through robust training and deployment of more human intelligence assets that can infiltrate deeper into the target's domain.

The mere reliance on the scientific competence on information collection, namely the deployment of technologically sophisticated technical intelligence systems, cannot provide insights into the intangibles of intelligence such as intentions and motivations of the target. Without understanding the full picture on the ground, there is little utility in the final strategic intelligence assessment. The key, therefore, is to produce actionable intelligence—one that is objective, accurate and timely. Technology, aided by complex software algorithms capable of a methodological process to mine the myriad of data and information, form patterns and trends of impending threats and provide insights into intentions and perceptions and could be a way forward to supplement the human capacity. Intelligence analysts should leverage on these technologies and add them to their tool boxes to improve their analytical capabilities. In short, the scientific competence of information collection and analysis can be leveraged and improved upon in order to provide better and more useful strategic intelligence.

The usefulness of the intelligence product then depends on how relevant it is to the present context and the level of rigour and objectivity of the intelligence assessment. To this end, the tensions between the intelligence analysts and policy makers pose significant challenges as both sides have different professional goals and visions to uphold to. Clearly, full separation and independence of both parties will reduce the utility and relevancy of the intelligence product. On the other hand, excessively close relationships between both parties will run the risks of politicisation of intelligence. It is a fine balance that has to be constantly tweaked and refined. Nevertheless, there must be communication and interaction between both producers and consumers in order for the strategic intelligence product to be useful.

In conclusion, until the focus moves away from technology and towards the humanisation of the intelligence process, no substantive progress in the production of useful military intelligence is likely. It is not a case of zero sum game where we either use more or less of the scientific competency of intelligence collection and analysis systems. In a world where information is overwhelming and growing at an exponential rate, providing timely and accurate intelligence requires intelligence analysts to leverage on as many tools and skills as possible to derive the most objective product that he can up with. Intelligence analysts grounded in scientific competency, technology flexibility and adaptability have the potential to achieve high levels of competency that are necessary to digest information from various sources, integrate them into analysis and present them into a coherent and convincing fashion to intelligence consumers.

BIBLIOGRAPHY

Colby, Elbridge A. *Making Intelligence Smart: Some necessary reforms,* (Stanford: Hoover Institution, 2007.)

Flanagan, Stephen. (1985). "Managing the Intelligence Community", *International Security*, Vol. 10, No. 1. (Summer, 1985), 58-95.

George, Roger Z. "Meeting 21st Century Transnational Challenges: Building a Global Intelligence Paradigm". (*Washington: CIA, Center for the Study of Intelligence,* 2007,)

Goodman, Melvin A. "9/11: The Failure of Strategic Intelligence", *Intelligence & National Security*, Vol. 18, No.4 (Winter), 59-71, 2003.

Greenberg, Maurice R. & Haass, Richard N. *Making Intelligence Smarter: The Future of U.S. Intelligence,* (New York: Council on Foreign Relations Press, 1996).

Huntington, Samuel P. *The Clash of Civilizations and the Remaking of World Order,* (London: Simon & Schuster, 1996).

Ibrügger, Lothar. *The Revolution in Military Affairs: Special Report,* (NATO Parliamentary Assembly Committee Reports: Science and Technology Committee, 1998).

Johnson, Loch K. (ed.) *Strategic Intelligence I: Understanding the Hidden Side of Government.* Westport: Praeger Security International, 2007).

Johnson, Loch K. (ed.) *Strategic Intelligence II: The Intelligence Cycle: The Flow of Secret Information from Overseas to the Highest Councils of Government,* (Westport: Praeger Security International, 2007).

Johnson, Loch K. (ed.) *Strategic Intelligence III: Covert Action: Behind the Veils of Secret Foreign Policy.* Westport: Praeger Security International, 2007.

Quiggin, Thomas. *Seeing the Invisible: National Security Intelligence in an Uncertain Age,* (Singapore: World Scientific Publishing, 2007).

Shulsky, Abram N. & Schmitt, Gary J. *Silent Warfare: Understanding the World of Intelligence,* 3rd Edition, (Dulles: Potomac Books Inc., 2002).

Tomes, Robert R. & O'Connell, Kevin. *Keeping the Information Edge: Reforming intelligence for the age of terror,* (Stanford: Hoover Institution, 2004).

ENDNOTES

1. Lothar Ibrügger, "The Revolution in Military Affairs: Special Report," *NATO Parliamentary Assembly Committee* Reports: Science and Technology Committee, November 1998, http://www.nato-pa.int/archivedpub/comrep/1998/ar299stc-e.asp.

2. Daniel S. Gressang IV, *The Shortest Distance Between Two Points Lies in Rethinking the Question: Intelligence and the Information Age Technology Challenge, in Loch K. Johnson, eds., Strategic Intelligence I: Understanding the Hidden Side of Government* (Westport: Praeger Security International, 2007), 131.

3. Ibid., 132.

4. Ibid., 123.

5. Ibid., 129.

6. Andrew T.H. Tan and J.D. Kenneth Boutin, eds., *Non-Traditional Security Issues in Southeast Asia* (Singapore: Select Publishing Pte Ltd, 2001), 2.

7. Samuel P. Huntington, *The Clash of Civilizations and the Remaking of World Order* (London: Simon & Schuster, 1996).

8. Max Boot, *War Made New: America's Military Lead Can Be Lost* (New York: Gotham Books, 2006).

9. Maurice R. Greenberg and Richard N. Haass, *Making Intelligence Smarter: The Future of U.S. Intelligence* (New York: Council on Foreign Relations Press, Jan 1996), 4.

10. Daniel S. Gressang IV, *The Shortest Distance Between Two Points Lies in Rethinking the Question: Intelligence and the Information Age Technology Challenge, in Loch K. Johnson, eds., Strategic Intelligence I: Understanding the Hidden Side of Government* (Westport: Praeger Security International, 2007), 123.

11. Ibid., 128.

12. Thomas Quiggin, *Seeing the Invisible: National Security Intelligence in an Uncertain Age* (Singapore: World Scientific Publishing, 2007), 53.

13. Abram N. Shulsky and Gary J. Schmitt, *Silent Warfare: Understanding the World of Intelligence, 3rd Edition* (Dulles: Potomac Books Inc., 2002), 22-26.

14. "Bush defends NSA spying program," CNN.com, 1st Jan 2006, http://edition.cnn.com/2006/POLITICS/01/01/nsa.spying/.

15. Declan McCullagh, "AT&T sued over NSA spy program", Cnet, 31st Jan 2006, http://news.cnet.com/ATT-sued-over-NSA-spy-program/2100-1028_3-6033501.html

16. Electronic Frontier Foundation, *Domestic Internet Backbone Surveillance*, http://www.eff.org/nsa-spying.

17. Abram N. Shulsky and Gary J. Schmitt, *Silent Warfare: Understanding the World of Intelligence, 3rd Edition* (Dulles: Potomac Books Inc., 2002), 34.

18. Ibid., 36.

19. Canadian broadcasting Company, *History of Fundamentalism*, http://www.irmep.org/hf.htm, 54.

20. Ibid.,

21. John Hollister Hedley, "The Challenges of Intelligence Analysis", in Loch K. Johnson, eds., *Strategic Intelligence I: Understanding the Hidden Side of Government* (Westport: Praeger Security International, 2007), 124.

22. Thomas Quiggin, *Seeing the Invisible: National Security Intelligence in an Uncertain Age* (Singapore: World Scientific Publishing, 2007), 45.

23. Ibid., 53.

24. Ibid., 54.

25. Elbridge A. Colby, *Making Intelligence Smart: Some necessary reforms* (Stanford: Hoover Institution, 2007), 5.

26. Thomas Quiggin, *Seeing the Invisible: National Security Intelligence in an Uncertain Age* (Singapore: World Scientific Publishing, 2007), 55.

27. Elbridge A. Colby, *Making Intelligence Smart: Some necessary reforms,* (Stanford: Hoover Institution, 2007), 4.

28. Ibid.

29. Robert R. Tomes and Kevin O Connell, *Keeping the Information Edge: Reforming intelligence for the age of terror* (Stanford: Hoover Institution, 2003), 2.

30. Thomas Quiggin, *Seeing the Invisible: National Security Intelligence in an Uncertain Age* (Singapore: World Scientific Publishing, 2007), 47.

31. Ibid., 99.

32. Ibid., 101.

33. Sentinel Visualizer, *Analysis*, www.fmsasg.com/smsag/Products/SentinelVisualizer/analysis.asp

34. See ARDA & AFRL, *Tangram: Proposer's Information Packet (PIP)*.

35. "The Next Generation of Big Data Visualization," Sentinel Visualizer, http://www.fmsasg.com/Products/SentinelVisualizer/.

36. Arthur S. Hulnick, "What's Wrong with the Intelligence Cycle?", in Loch K. Johnson, eds., *Strategic Intelligence II: The Intelligence Cycle: The flow of Secret Information from Overseas to the Highest Councils of Government,* (Westport: Praeger Security International, 2007), 2.

37. James J. Wirtz, "The Intelligence-Policy Nexus", in Loch K. Johnson, eds., *Strategic Intelligence I: Understanding the Hidden Side of Government* (Westport: Praeger Security International, 2007), 140.

38. Jack Davis, "Intelligence Analysts and Policy Makers: Benefits and Dangers of Tensions in the Relationship", in Loch K. Johnson, eds., *Strategic Intelligence II: The Intelligence Cycle: The flow of Secret Information from Overseas to the Highest Councils of Government,* (Westport: Praeger Security International, 2007), 157.

39. Jack Davis, "Intelligence Analysts and Policy Makers: Benefits and Dangers of Tensions in the Relationship", in Loch K. Johnson, eds., *Strategic Intelligence II: The Intelligence Cycle: The flow of Secret Information from Overseas to the Highest Councils of Government,* (Westport: Praeger Security International, 2007), 144.

40. James J. Wirtz, "The Intelligence-Policy Nexus", in Loch K. Johnson, eds., *Strategic Intelligence I: Understanding the Hidden Side of Government* (Westport: Praeger Security International, 2007), 140.

41. Ibid., 142.

42. Jack Davis, "Intelligence Analysts and Policy Makers: Benefits and Dangers of Tensions in the Relationship", in Loch K. Johnson, eds., *Strategic Intelligence II: The Intelligence Cycle: The flow of Secret Information from Overseas to the Highest Councils of Government*, (Westport: Praeger Security International, 2007), 147.

43. Ibid., 150.

44. Ibid., 153.

45. James J. Wirtz, "The Intelligence-Policy Nexus", in Loch K. Johnson, eds., *Strategic Intelligence I: Understanding the Hidden Side of Government* (Westport: Praeger Security International, 2007), 139.

46. Ibid., 141.

47. Arthur S. Hulnick, "What's Wrong with the Intelligence Cycle?", in Loch K. Johnson, eds., *Strategic Intelligence II: The Intelligence Cycle: The flow of Secret Information from Overseas to the Highest Councils of Government,* (Westport: Praeger Security International, 2007), 9.

48. Ibid.

49. Ibid., 8.

50. John Hollister Hedley, "The Challenges of Intelligence Analysis", in Loch K. Johnson, eds., *Strategic Intelligence I: Understanding the Hidden Side of Government* (Westport: Praeger Security International, 2007), pp. 132-133 and Quiggin, Seeing the Invisible: National Security Intelligence in an Uncertain Age, 56-57.

51. Thomas Quiggin, *Seeing the Invisible: National Security Intelligence in an Uncertain Age* (Singapore: World Scientific Publishing, 2007), 58-59.

CPT (NS) Fu Wen Hao, Kelvin's previous appointments in the SAF included OC of Foxtrot Company in 11C4I Bn and Staff Officer at the Integrated System Development Group, Air Combat Command HQ.

CPT (NS) Fu is currently the Senior Executive at one of the largest private equity funds based in Shanghai providing growth capital to companies with solid track records across diversified industries. He is responsible for the deal sourcing, due diligence investment evaluation, structuring and portfolio management. He has worked on numerous deals spanning across consumer related sectors, energy and healthcare in different geographic regions such as North Asia, Southeast Asia and Europe.

CPT (NS) Fu has a Masters of Applied Finance from Macquarie University and studied Political Science at the National University of Singapore and Technopreneurship at Fudan University.