PRODUCING INTELLIGENCE IN AUSTRALIA: HOW A NATIONAL OPEN SOURCE FOUNDATION MIGHT SERVE NATIONAL SECURITY AS WELL AS NATIONAL COMPETITIVENESS.

by

Nicholas Chantler

Justice Studies (Faculty of Law),
Queensland University of Technology,
Brisbane, Australia.

The Third Open Source Solutions Symposium 7-10 November 1994, Alexandria, Virginia (Washington),

BACKGROUND

I have watched with interest, the Open Source Solution "Six-Year Revolution" of Robert Steele in the USA (Steele:1994a). It is true that, since the end of the Cold War, there have been many changes; political, social, cultural, technological, economic and financial; to mention but a few...

(Some people regard Australia as being remote from these reformations. However this is not the case, because Australia continues to have an increasing role to play within the South Pacific and associated regions. The continual developments in new trade agreements; changes in alliances; greater involvement with United Nations Peace-Keeping Operations, for example the recent deployment of Australian troops in Cambodia, Somalia and Rwanda; are some of the indicators which demonstrate the continued expansion of Australia's interests and responsibilities.)

I believe that, in Australia, we are already aware of changes taking place in information technology, albeit focussed on 'The Information Superhighway". Those of us who use information as a raw material are aware of even greater, and perhaps more subtle changes, which the rest of society is still coming to grips with.

In November last year, I was able to attend the 1993 OSS conference. Prior to my visit the Australian media gave some very favourable publicity to the concept of Open Source Solutions... particularly because it coincided with government murmurings (in the Press) of changes in handling information.

In March this year we were honoured with Robert Steele's presence; Australia held its own OSS Conference in the nation's capital, Canberra. Again, this attracted more interest. From watching various indicators, such as the growth of information technology and the changes appearing on Internet, I again proposed, at the Canberra conference, that Australia should have a National Strategic Information Policy (Chantler, 1993). ...I know that the message is 'getting-through' because I have had requests from the parliamentary library to furnish my papers, at the request of an unidentified Member of Parliament.

Nearly every week there are articles which appear in the national newspapers which discuss aspects dealing with Information Technology, particularly management and policy.

Realising that we need to continue, to take advantage of the developing embryo of Open Source Information (OSI), it seems to me that the next logical step is to propose a National Open Source Foundation. This agency will be able to serve national security and national competitiveness.

At the annual national AIPIO (Australian Institute of Professional Intelligence Officers) Conference - INTEL'94, I presented a paper to the delegates (Department Heads, Directors, Intelligence and Information Managers, and other specialists. This included representatives from the Australian "big five" intelligence agencies). The paper proposed that a National Information body (Foundation, Agency or Organisation) be established to capitalise on the growing amounts of information that are becoming easier to access. My proposal suggests that, as a trial, it should focus on Internet for "data mining".

I see a National Information Agency (NIA), as an information broker at national level, to be able to address the information requirements of both the Federal and State Governments; the corporate, industrial, academic sectors... and even the requests of individuals.

Before I discuss this, we need to consider what National Security consists of, applicable to this context; and also what National Competitiveness is, and how the two relate to each

other. We will then have a much better appreciation of where an NIA becomes the next logical step to provide the "missing-link" to be able to support both these areas.

NATIONAL SECURITY

National Security in Australia addresses a range of different levels: (I think that this is true for most countries and not just Australia.)

Global
- at a global level (i.e. externally) in relation to other nations, various alliances and politics to give security within a region.

I have already addressed aspects of this area in a previous paper to do with "Paps" and the components of the strength of a nation (Chantler: 1993).

National (formal)
(For want of a better expression I have split "national" into "formal" and "informal")

- at a national level in a formal sense; with most people thinking of the Australian Defence Force (ADF) and the "big five" (Hartley: 1994) intelligence organisations to form the conventional security of a nation.

ONA - Office of National Assessments. Primarily involved with assessments, the ONA answers directly to the Prime Minister through the Department of the Prime Minister and Cabinet and is concerned with national strategic analysis, involving strategic and economic assessments.

DSD - Defence Signals Directorate is essentially a collection agency involved in the collection of signals intelligence (SIGINT).

ASIS - Australian Secret Intelligence Service. The primary function is the collection of human intelligence (HUMINT).

DIO - Defence Intelligence Organisation. Its mission is to promote the security of Australia by providing quality intelligence for defence policy making and the support of ADF operations, ONA and Foreign Affairs.

ASIO is both a collection and an assessment agency and is concerned essentially with internal security issues, including politically motivated violence and terrorism. Internally, national security relates to a social, political economic and financial stability. Whilst the main intelligence organisation that deals with this area is ASIO, there are many other users of Intelligence information; eg. Federal and State Police Forces, along with other government departments.

National (informal)
- at a national level in an "informal" sense; with security in a government's political stability, financial stability (interest rates, gross national debt), policing, organised crime, social standards (wealth, standards of education, health and living etc.).

State
- at a state level; security of state government politics, society within the state, policing, criminal activity, welfare and emergency services etc.

(Perhaps could take it a step further to **Local Community** level.. ?)

NATIONAL COMPETITIVENESS

Being competitive is not just "one business competing against another". It is the raising of standards, through working 'smarter' so that higher efficiencies and greater effectiveness can be achieved. This idea does not just apply to businesses. It stretches from the individual up to the multi-national corporations and beyond to The Nation itself.

In order to be competitive in all areas of life we need information. To be able to get our hands on information, in this day and age, we need to take advantage of technology.

I think it is fair to say that there is an awakening, perhaps greater in some countries than others, of the need for 'Competitor Intelligence' - as it has been called within the corporate sector.

In a recent paper Gray (1994) states "Competitor Intelligence is a tool by which businesses can gain information about their competitors, with the aim of gaining a commercial competitive advantage in the marketplace". He further describes how this intelligence is based on open source information; and in one particular case how he found the answer for a company within their own files.

(Truly a case of "We don't know, what we 'know'! ...Here is a classic indicator of the need for smarter handling of information.)

Competitor Intelligence assists National Competitiveness which relates directly to the areas that I have mentioned in the 'holistic view' of National Security presented above.

National Competitiveness relates to a variety of areas:

- how our nation is perceived by others
- our Gross National Product
- our balance of payments
- trade agreements
- financial investments
- smarter management
- greater scope for business opportunities
- faster reaction to changes in external political trends
- technological advantages in military strength
- changes in external alliances
- addressing threats to society
- quality of life
- multicultural balances
- environment

etc...

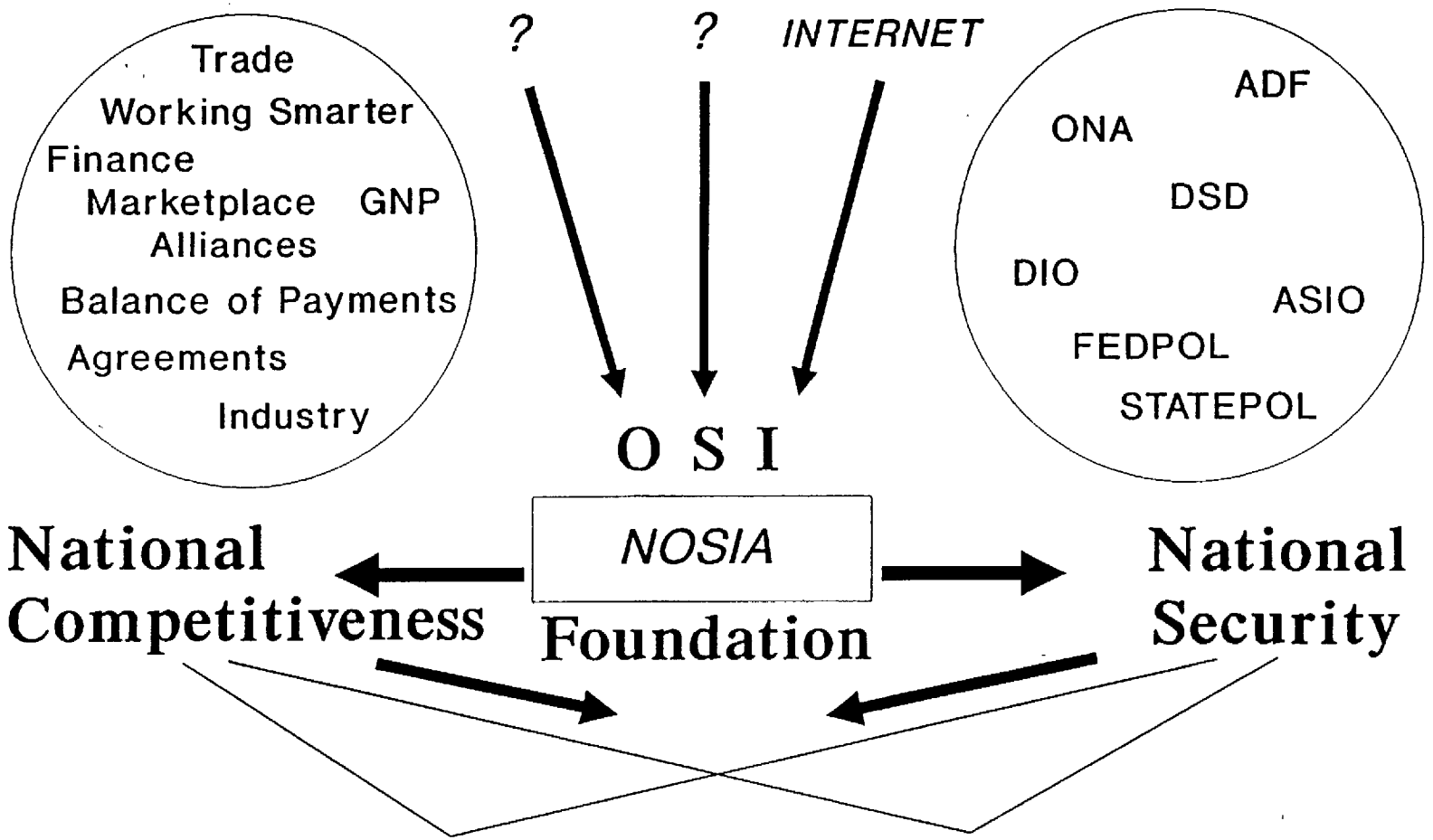

Figure 1. How a National Open Source Information Agency (NOSIA) Compliments National Security & National Competitiveness.

JUSTIFICATION

Having considered what National Security and National Competitiveness consist of, it can be seen how the two link together through areas which are common to both. Here is where we see the justification for the formation of an NOSIA (National Open Source Information Agency). The following points are further examples of the types of indicators which I believe are leading us to the development of an NOSIA.

For example, at the "**global level**" Hogan (1994) states: "Australian troops are becoming involved increasingly in multinational humanitarian and peacekeeping operations (PKO), usually under a United Nations (UN) banner, such as recent deployments to Cambodia, Somalia and Rwanda. A problem arises when intelligence support can not be provided to planning staffs and decision-makers in the field due to the practical limitations and political sensitivity of using classified intelligence in a UN environment. Intelligence which is releasable only to certain elements of a multinational force could cause embarrassment and mistrust. **One response to these changes could be the exclusive use of open, unclassified sources to produce intelligence in Peace Keeping Operations (PKO).**"

... at the "**national 'formal' level**"...the director of AUSTRAC (Australian Transaction Reports and Analysis Centre), Mr Bill Coad stated in a recent paper on "National Criminal Intelligence Requirements" that we "**Need to show value for money, need to invest in technology, be reactive to clients; you must define the strategic approach of your organisation...**".(Coad:1994)

...at the "**national 'informal'** level"...

- to address the substantial **changes in the structure of the economy** which have accompanied **increases in the volume of available information** and the extent of the information flows;

- to deal with the **significance of the growth of information, a major transforming factor with a unique capacity to change work, personal performance, leisure and the quality of life.;**

- to consider the use of intelligence/knowledge to **produce brain-based, high value-added goods and services;**

- to use the **centrality of information** as a central organising principle, a tool for understanding, and **a vital element in trade expansion;**

- to demonstrate the need to increase the community's use of information;

- to counteract the **threats to personal privacy and illegal access to information, and the risk of creating a new group of information poor;**

- to review the **hierarchical nature of government service delivery systems;**

- to question **the ownership and control of information by authorities and their reluctance to share it;**

- to rectify the lack of a **clearly defined community role in the information process, other than as a haphazard, passive and trusting end-users;** and

- to correct a **general ignorance on the relationship between data, information and knowledge.**

...at the "**state level**"...Mr Rupert Murdoch, the media magnate, on an ABC Radio interview (21st October 1994) was talking about the advances in technology. He suggested that the "Information Superhighway" would be of benefit to society in the: dissemination of truth, breakdown of totalitarianism and making people free to communicate with anyone else.

Information/Data Mining OSI (adapted from G. Hogan: 1994)

Any information acquisition strategy would exploit a variety of open sources. Potential sources are:

Print Media. The print media of both the target country and other nations of interest, provide a sound basis for background briefs and current reports.

Electronic Mail. Monitoring of electronic media, such as cable news services, offers instantaneous data on events and developments. CNN has become an indispensable tool to intelligence analysts and policy-makers alike.

Journals and Periodicals. Journals and periodicals lack the timeliness of news media, though they offer more in-depth analysis of local and world affairs. There is a wide range of foreign affairs, specialist and technical journals available.

Military Sources. Military sources range from specialist military journals to papers produced at staff and war colleges.

Academic Sources. Academic sources offer much detailed research and background material for exploitation. Academics can help in understanding a wide range of topics and specialised areas.

Technological Sources. Many technological sources, highly classified during the Cold War, are now available commercially. Remote sensing data will be useful for planning. Russia is reportedly selling imagery with a resolution of two meters.

Human Sources. Human sources will range from diplomats to attaches, travellers to expatriates. Intelligence derived from human sources is very important in low level operations.

Other Sources. Other sources exists which may be exploited by the open source analyst, from common reference works to UN reports, government publications to tourist brochures.

The global revolution in information technology makes open source intelligence possible. Whether open source intelligence is feasible, then, will depend on the advantages which may accrue from it.

ADVANTAGES

Cost. There will be no additional cost for using open source intelligence. Most open source information is currently in use. Manpower for staffing an analytical cell will be reallocated from existing resources.

Handling Procedures. Complex and convoluted handling procedures for the transmission, storage and destruction of classified information will be unnecessary. Special keying material for secure communications systems will not be required.

Sharing With Allies. Unclassified intelligence can be readily shared with multinational (for example Peace-Keeping Force allies, gaining their trust and enhancing the ADF's 'honest broker' reputation.

Appropriate For Low Level Operations. Open source intelligence is appropriate for low level operations. Cold War technological systems, designed for a sophisticated enemy with a huge equipment inventory, are largely ineffective in new conflict scenarios.

No Risk of Compromise. There is no risk of compromising sensitive sources if an unclassified approach is used.

Self-Reliance. Reducing a reliance on allied intelligence support is consistent with a policy of defence reliance. Intelligence products will also be free from restrictions imposed by other nations. Experience with open source intelligence will be useful if allied intelligence support is reduced or discontinued.

Consistent With UN Culture. With our increasing involvement in UN, open source intelligence will suit that organisation's innate cultural bias against conducting secretive operations or 'spying.' The UN prefers the euphemistic term 'information and research' to 'intelligence,' considering the former less inflammatory.

Promotes Cultural Change. The use of open sources will promote cultural change within the intelligence community, causing it to rethink its missions and reconsider the way it does business.

Consistent With Intelligence Principles. Open source intelligence is consistent with the basic intelligence principles of timeliness, accuracy, accessibility and usefulness. Unclassified intelligence will be, arguably, more timely, accessible and useful than intelligence with caveats on its distribution.

Major advantages will follow on from using an open source approach to strategic intelligence. Some disadvantages should also be anticipated.

DISADVANTAGES

Security Consciousness. There is a possibility that frequent use of open source intelligence will erode the security of those working with it, causing lax procedures when dealing with classified sources.

Reduced Expertise in Classified Intelligence. A preference for open sources will, over time, reduce expertise and degrade experience in the skills required to fully exploit classified and technology-based intelligence.

Exclusion of Certain Content. National security and policy considerations will dictate that certain sensitive content be excluded from open source products. This may limit the usefulness of the intelligence.

In summary of these points, the advantages of using open source intelligence (OSCINT) from open source information (OSI) far outweigh the disadvantages of such an approach.

NOSIA (NATIONAL OPEN SOURCE INFORMATION AGENCY)

I propose that a trial site focussing on Internet be the first stage to form a foundation that would also link National Competitiveness and National Security.

Initially there would be no analytical work (possibly some filtering? but a form of 'initial analysis' may come later), only the collection of information as tasked by the customers.

Other factors arising from having a NOSIA:

- NOSIA will support all types of customers from individuals to governments and corporate giants.
- All customers would be protected because the NOSIA allows them to be anonymous
- Having one agency collect information prevents duplication of effort
- This leads to increased efficiency through a single retrieval of data which can then be distributed rather than everyone 'getting their own'.
- This allows centrality of data management but without placing any restrictions on the information.
- NOSIA will provide an immediate focal point for agencies
- NOSIA could provide measures i.e. 'indicators of information gathering' for cross-agency comparison purposes as a measure of productivity for the Inspector General of Agencies office.
- NOSIA can become a source of triangulation for validating data already held in existing agencies
- NOSIA can provide a career entry point for professionals who wish to develop a specialist career in Intelligence & Security
- It will also provide an experienced group of specialist operators for 'surfing' INTERNET and data mining.
- NOSIA could be a self-financing agency (essentially non-profit, but self-sustaining from the financial input of corporate customers ?) or government funded/supported...perhaps with representatives from each organisation which wants to capitalise on OSI.
- It could be a new 'stand-alone' organisation, or part of an existing intelligence organisation; a 'wing' of the National Library of Australia... perhaps allied to a university...? there are several possibilities.

SUMMARY

There are some very strong points which support the development of a NOSIA (National Open Source Information Agency). The current world trends, in the development of information technology and its importance in a Nation's Security and its Competitiveness, dictate that we need to keep ahead in everything we do. Information is the raw material which keeps us competitive in political, financial, security and many other matters.
If we (Australia) wait and watch, we may well find that we have 'left our run' too late. If that is the case we will sink further behind in the world stakes and exist in a position of

false security - merely because our information which reflects our security (in the widest possible sense) is not current.

BIBLIOGRAPHY

Chantler, A.N. (1993) To demonstrate the need for Australia to develop a strategic policy on OSI (Open Source Information) which capitalises on emerging trends, *Proceedings of the Second International Symposium: National Security and National Competitiveness: Open Source Solutions*, Vol 2. 2-4 November 1993, Omni Shoreham Hotel, Washington DC.

Coad, B. (1994) Needs & Strategies to Meet National Criminal Intelligence Requirements, *Proceedings of AIPIO Conference*, Brisbane, Australia, 13-14 October 1994

Hartley J. MAJ GEN (1994) Managing an Intelligence Organisation, *Proceedings of AIPIO Conference*, Brisbane, Australia, 13-14 October 1994

Hogan, G. (1994) Open Secrets: Rethinking ADF Strategic Intelligence,*The Bridges Review* - Journal of The Australian Intelligence Corps. December 1994

Steele, R. (1994a) *OSS Notices (Open Source Solutions)*, Volume 2, Issue 7., 30 September 1994, OSS Inc, 11005 Langton Arms Ct, Oakton Virginia 22124-1807

REFERENCES

Chantler, A.N. (1994) Intelligence & Security - Indicators of Change: Australian Open Source Information (OSI), *Proceedings of AIPIO Conference*, Brisbane, Australia, 13-14 October 1994

Chantler, A.N. (1994) Intelligence, Information Technology & Open Source Information, *Proceedings of the OSS (Open Source Solutions) Conference*, 17 March 1994, Canberra, ACT.

Steele, R. (1994) *National Information Strategy Act 1994*, OSS Inc,11005 Langton Arms Ct, Oakton Virginia 22124-1807

Steele, R. (1993a) *Proceedings of the Second International Symposium: National Security and National Competitiveness: Open Source Solutions*, Vol 1. 2-4 November 1993, Omni Shoreham Hotel, Washington DC.

Steele, R. (1993a)*Proceedings of the Second International Symposium: National Security and National Competitiveness: Open Source Solutions*, Vol 2. 2-4 November 1993, Omni Shoreham Hotel, Washington DC.

(Note: AIPIO is the Australian Institute for Professional Intelligence Officers, Canberra.)

Nicholas Chantler - Brief Curriculum Vitae - October 1994

Nicholas Chantler lectures in Intelligence and Security at the Faculty of Law, Justice Studies Department, QUT (Queensland University of Technology).

His background is multi-disciplinary; covering agriculture, education, electronics, computing and the military. An officer in the Australian Regular Army's Australian Intelligence Corps with thirteen years experience, he was the first Head of Computer Security. He now continues his military career in the Army Reserve, posted to the School of Military Intelligence, Canungra, Queensland.

Nicholas Chantler is currently completing a Ph.D. (Information Systems) through Curtin University, WA. This study considers: "Risk: The Profile of The Computer Hacker". He is also a Research Associate at RMIT (Royal Melbourne Institute of Technology) with ACARB (Australian Computer Abuse and Research Bureau).

This year he was appointed to the Queensland VETEC Committee for the examination, accreditation and maintenance of standards, of formal courses within the security industry. He is also a member of the International Federation for Information Processing (IFIP) dealing with Law Enforcement and Information Crime.

Nicholas Chantler has many publications to his credit in the Information Security arena. He presents papers at an international level and continues to be featured in the press, radio and television interviews. He is considered an authority on computer hackers; computer security, information and intelligence; and, open source information.)

THIRD INTERNATIONAL SYMPOSIUM on NATIONAL SECURITY & NATIONAL COMPETITIVENESS: OPEN SOURCE SOLUTIONS Proceedings, 1994 Volume II - Link Page

Previous	Harsh Realities: S&T Acquisition Costs, Obstacles, and Results, by Ms. Bonnie Carroll, President and CEO, Information international Associates, Inc.
Next	Overview of the Global information Industry, by Mr. Harry Collier, Managing Director and CEO, Infonortics (UK)Sponsor, Association for Global Strategic Information (AGSI)

Return to Electronic Index Page