SO11 Open Source Unit Presentation

Steve Edwards (Detective Constable) New Scotland Yard.

History

Since 1993 the Metropolitan Police in London (www.met.police.com) has been undertaking a complete rejuvenation of it's intelligence practices. During that process the concept of open source intelligence gathering became a very real issue. It was anticipated, however, that there would be some resilience to the suggestion that our intelligence community did not have, nor could it get, all of the answers that it needed from it's existing sources and pools of information.

Surprisingly this was not the case. Operational intelligence officers and grass roots police officers quickly warmed to the speed, efficiency and availability of open source information. The project also gave us the opportunity to show those who hold the purse strings how an investment in open source intelligence gathering was a value-for-money concept and that time, effort and exposure could be minimised by the employment of such strategies.

Definition

Let me first begin by establishing what we mean by the term "open sources". We consider open sources to be any *form* or *source* of information available to us either as a paying customer or for free. In reality we use on-line sources as the first string to our bow, but we frequently dip into our list of *real people* – experts in their particular field whenever we reach a dead-end or we want that little bit more. Magazines, periodicals and other publications also provide a valuable source of material, which we are able to exploit. As an example, each issue of the International Police Review produces about 30 open source items, which we evaluate and then forward to those who would make the best capital from them. We do not use any police-based data or informant or technical product and most of the sources we access are available to any *bona fide* person who has a legitimate reason and the right connections.

Strategic versus Tactical

Our open source response falls into two main categories, *Strategic and Tactical*. That is to say information which is needed right away and information which can be collected through long term research as part of an on-going project.

Most of the *Tactical* requests come from officers who are trying to track down fugitives or to establish links between criminal suspects and their *associates*, or information about their *businesses* and *financial dealings*. Much of this is surprisingly easy using some very simple tools and some officers are astonished when they come to us with nothing but a name and we return address lists, family names and addresses, companies and directorships, financial details and associates. (www.gb.co.uk http://cameo.bvdep.com/MainFrame.asp)

Officers finding themselves sent to strange parts of the world to conduct extradition and hostage negotiations do not always have the time to wait for sophisticated analyses and risk assessments from Special Branch or the FCO. More and more often we receive open source requests for such packages which we normally turn around inside an hour or two. (http://www.travelhealth.com/safety.htm http://www.stolaf.edu/network/travel-advisories.html http://travel.state.gov./travel_warnings.html http://www.webstrand.org/tony/crises.htm www.crg.com)

Strategic research can be a lot more challenging but generally speaking we have limited this purely to crime related matters. That may sound obvious but you might be surprised at just how many side-projects about DNA, Forensics, Psychological Profiling, etc. can quickly clog up an already overworked system. That's not to say that we don't try to accommodate specific requests for such information or that we discard anything interesting which we come across on our travels but we do have to prioritise our resources which was a lesson that we learned the hard way.

Generally speaking, our strategic research follows such lines as,
organised crime (http://www.afpc.org/issues/crime.htm),
money laundering (http://dharma.fad.phare.org/ml/topics.htm),
fraud (http://mailer.fsu.edu/~btf1553/ccrr/welcome.htm),
drugs (http://marijuananews.com/),
firearms (http://www.cops.aust.com/firearms/),
race/hate crime (http://www.officer.com/hate.htm),
terrorism (http://www.ict.org.il/default.htm),
protection of the Royal Family (http://www.geocities.com/CapitolHill/Lobby/1793/Index.html) and other serious crime issues. Most of our research in this area is done using the Internet, and I'll say more about that later. We have found that, given the correct amount of circumspection that the Internet provides a significant amount of information and access to news, academic articles and research which we couldn't possibly access – or afford, in any other way.

Security

Another lesson that we learned was security. All of our on-line transactions are done covertly and we use under-cover pseudonyms and covert companies in the same way that we do with any other covert operation. This helps to prevent anyone seeing that the police have been looking into their company records or personal details and also helps with security and similar issues on the Internet. The Provisional IRA and other extremist groups obviously expect the police and security services to be looking into their web sites but why should we give them any more information than we need to. The time and date of your access could have important relevance to some upcoming operation or arrest or activity on their part. There is also an issue surrounding the leaving of cookies and other telltale traces of access. Anyone who has ever taken the time to de-cipher the endless stream of gibberish at the end of their email will quickly see the sort of information which can be gleaned by the unscrupulous. It is rumoured that the MSN web sites takes 47 pieces of information about you and your machine every time you visit the site.

We are also conscious of physical security and our open source network is a small one, which has a complete air-gap between it and any other police systems.

Product

One of the beauties of open source research is the speed of it's turnaround. Robert Steele (www.oss.net) from Open Source Solutions Inc. calls it, 'Just enough, just in time'. We pride ourselves that our open source bulletins take one officer just one day to produce. This includes collection, collation and dissemination. They are not fancy or glossy and a supermarket would probably package them in a plain wrapper and call them 'economy' but they seem to be well received and get to the user's desk the next day. I have some copies if any of you would like to see them. An important point to make here though is that we do not profess to be experts in any particular field or criminal discipline. What we provide is done on a for-what-it's-worth basis. If the reader already knows 30% of the bulletin and doesn't need to know another 30% of it that still leaves 40% of valuable information. How many publications can we say are that useful? Bearing in mind that a bulletin takes just one day to produce, if only one article is useful then it was worthwhile.

All of this is not to say that we have not had our fair share of setbacks. The initial impetus for open source availability took a number of shifts to the back burner as other demands for project time took priority. Changes in personnel and management meant that open sources were *different flavours* to different bosses and we all know how frustrating that can be but eventually, with tenacity and dogmatic perseverance we won through. Other challenges came, and continue to come from the Data Protection Registrar. Above all we must comply

with the law but it seems that time after time we face an uphill struggle in the use of legitimate data collection which is so valuable in the fight against sophisticated and well organised criminals and those of a generally evil disposition. Even as we speak there is contention and confusion amongst a number of on-line service providers, Equifax and Experian to name but two, over exactly how DP Legislation is to be interpreted.

Co-ordination and Direction

But from all of our challenges came experience and learning and I would not like to miss an opportunity to give thanks and credit to all those who sought to assist us with their own experiences and learning. The thing about the open source community is that it is generally populated by those who make a living out of the exploitation of other people's hard work. The result of that lifestyle is that we seem to find some sort of assuaging of our guilt by putting something back every once in a while. Just as *we* received help and advice from organisations such as Europol, MoD, DERA, Comax, Lexis-Nexis, GCHQ and many others, we also have sought to help others establish open source initiatives and strategies.

This is a good community and well worth while becoming part of. We, *you*, all of us make use of open sources every day. Each time you pick up a phone and dial a colleague or friend for information. Every time you call directory enquiries or pick up an encyclopaedia. The concept is far from new and in law enforcement we have made use of such resources for many years. Telephone subscriber information, GIS data, newspapers, magazines, electoral roll - they all form part of the disparate nature of open sources already enjoyed by law enforcement.

Where we lack strength is in the co-ordination and collation of the resources and skills that go to make up such an environment. It's one thing for an NCIS detective in Yorkshire to call Equifax for a check on one of her or his suspects and another thing for an analyst at the National Crime Squad in London to pull an article about hydroponic drug cultivation off of the Internet. A Special Branch officer in Liverpool could make frequent and valuable use of a contact at the Control Risks Group and her colleague in London might have a similar contact at Kroll but none of this takes us very far forward collectively. What is required is a large-scale assessment of the number and types of open sources that would be valuable to law enforcement.

Specialisation

I would venture to suggest that each force in the country has had an open source capability, it's just that they don't know it. It might be called something else or nothing at all. There will be officers in most forces doing what we have already described – but they are only doing it for themselves or their own unit, squad or branch. And, again, that is not to say that there is not a

place for such use of open sources. The devolution of low-level open source facilities to grass-roots level will free up analysts and researchers for more important work but there is, in my opinion, a very real and important role for the open source specialist. Such specialists will know where to look and how to get there, the best searching techniques and above all the right source for the job in hand. These people will also enjoy the fellowship of the open source community and the facility that comes from the associations and contacts which they make.

Emerging Trends and Strengths

Let me turn now to the type of information that is so useful to us from open sources. As I indicated earlier it is always dangerous to suggest to an intelligence officer that there is something that he or she does not know about their given specialist field. One exception to this, however, is when new areas of interest become apparent, areas where there is no established knowledge base. Russian organised crime was a good example of that type of field and it is one where open source intelligence gathering proved fruitful. (http://members.tripod.com/~orgcrime/ruscali.htm). Names and pictures of criminals, organisational structures, tattoo markings and many other valuable pieces of information were quickly assimilated. Hydroponic drug cultivation has long been a problem in the United States and, like most US trends, eventually made it's way across the Atlantic. By that time there was a plethora of information already waiting to be harvested in academic and journalistic articles, not to mention commercial ventures who were growing rich from sales of hydroponic (http://home.earthlink.net/~daytrippn/growe.html) equipment and various growers pages on the Internet.

Our anti-terrorist branch is always on the look out for different trends in extremist violence and collects volumes of data on terrorist incidents around the world for close and strategic analysis. An abortion clinic bombing in Berlin today could be a problem in Sheffield tomorrow. The high school kids playing with pipe bombs in Minneapolis could quickly be mimicked by youths in Orpington, Kent who have downloaded the instructions from the Web. Before the Open Source Unit was formed the Bomb Data Centre carried out all of their information collection by using press clippings and faxes from the Security Services. This meant that they were restricted to articles printed in the available press and reproducing them by re-keying them into their own databases. Now we can provide large dumps of a far greater number and type through news-profiles and trawling exercises.

http://www.terrorism.com/terrorism/links.html
http://web.nps.navy.mil/~library/tgp/tgp2.htm
http://web.nps.navy.mil/~library/tgp/tgpndx.htm#1997
http://eob.org/terror/index.html
http://eob.org/terror/html/cyber_terror.html
www.acsp.uic.edu/OICJ/CONFS/terror02.htm
www.conservativebookstore.com/laden/messages/38.html

Current Projects

The Open Source Unit is currently engaged in strategic research projects on behalf of the following departments: Anti-terrorism, Royalty Protection, Race Hate Crimes, Money Laundering, Drugs, Organised Crime and Russian Organised Crime, Cyber Crime, Triads, Extradition, Hostage Negotiation and Fraud.

In addition the Metropolitan Police has recently reaped the rewards of two Internet campaigns to track down suspects wanted for murder. As a result the Open Source Unit has been tasked with developing the strategy for a more formal programme of intelligence gathering through the New Scotland Yard web-site. (www.met.police.com)

Useful Tools

Probably the most useful tools to our open source research are the bookmark file on the web browser or the contacts list in Microsoft Outlook. People are often accused of failing to learn from our mistakes but an open source analyst soon learns the importance of learning from his or her successes.

Having spent the afternoon looking for the definitive guide to Money laundering (http://www.ustreas.gov/fincen) or tracking down the best reverse phone checker on the web (http://www.555-1212.com) it would be a crime to have to start that whole process over again the next time one wanted to execute a search. Our bookmarks contain a valuable source of sources, which are constantly updated and added to. Also, by careful use of managed subscriptions we can examine those sites for changes which give us timely information relating to many of the groups and subjects which we monitor. Circumspection obviously prevents me from declaring those in open session but I'm sure your imaginations can fill in the gaps.

So what do we guard so jealously in our treasure chests of useful sources? OK, let's focus entirely on the Internet, as we have already owned up to making such capital from it. The most valuable commodities are the people that know. Whilst we can take our own levels of expertise for granted it's nice to know, also, that when the task or question arises that we don't have a clue about, there is always someone who we can turn to for guidance. And that is a reciprocal arrangement, a two-way street in the gift-economy of open sources. It is extremely gratifying to get help or advice from a person only to have that same person ask for your advice a few days later and you are able to help out. As mentioned before, the open source community is a close and helpful one.

Speaking of other useful resources on the Internet we make a lot of use of what we call, 'People Finders', sites where we can employ directories, public records, telephone records, lists, email finders, homepage finders etc.

Some of the more useful ones are as follows.

www.qb.co.uk
http://cameo.bvdep.com/MainFrame.asp
http://www.800go.com/homewiz/homewiz.html
http://mesa.rrzn.uni-hannover.de/
http://www.startingpage.com/html/lookup.html
www.qas.com
http://www.online.ru/esearch/
http://www.theultimates.com/
http://www.555-1212.com/
http://people.yahoo.com/

We also make good use of news sites and have a number of news profiles set-up to enable the continuous monitoring of subjects of interest. Sites such as excite (www.excite.com) are typical of the type of services which are available free. Also, many ISP's (Internet Service Providers) provide free email services which send the news directly to your email address. From my desktop I have access to newspapers from virtually anywhere in the world, nearly always in English and at the touch of a button I can get news and archive news from places such as China, Russia, India, South America or any number of exotic places. Imagine the difficulty of finding those publications, especially their archives, without the use of the Internet.

http://www.webwombat.com.au/intercom/newsprs/index.htm
http://www.clarinet.com/
http://www.utexas.edu/computer/is/e-newspaper.html
http://www.webwombat.com.au/intercom/newsprs/england.htm
http://www.thisislondon.com/dynamic/index.html
http://www.moscownews.ru/
http://www.lib.utexas.edu/Libs/PCL/News.html
http://gallery.uunet.be/internetpress/russia.htm
http://www.sinanet.com/index_gif.html
http://www.dso.com/cgi-bin/webc/home.html
http://www.esrin.esa.it/esairs/databases/UK_Newspapers.html

One source which I will definitely place amongst my list of valuable sources probably comes into several categories. Frans-Jan Mulslegal at Europol is a mentor, expert, resource and a source of excellent police-relevant material. I hope I have not caused him too much anxiety by advertising the service which he provides for many of us with a wide range of articles on many subjects.

Another useful area for Internet exploitation is in mapping and images. Maps of countries, towns and cities from almost anywhere in the world are now easily available and free to use.

Some of the more useful sites are listed below. Our police service provides many international functions and as a result we send officers all over the world. Maps and images of the places they are interested in can be found in abundance.

http://www.streetmap.co.uk
http://www.lib.utexas.edu/Libs/PCL/Map_collection/map_sites/cities_sites.html
http://www.mapquest.com
http://personal.msy.bellsouth.net/msy/s/h/sher07/bll-link.html
http://www.lib.utexas.edu/Libs/PCL/Map_collection/world_cities.html

If any of you would like to see how valuable one Internet site could be for providing information or links to search engines and other sites then the following might be of interest:

http://personal.msy.bellsouth.net/msy/s/h/sher07/bll-link.html (A collection of web sites relating to Russia)
http://www.officer.com (A police officers useful site list)
http://mprofaca.cro.net/firstone-ie.html (Mario Profaca – a Croatian Journalist and probably one of the best sites for Organised crime etc.)
http://rvl4.ecn.purdue.edu/~cromwell/lt/terror.html On of amny sites listing terrorist groups around the world and liks to or information about them.
http://home.rmi.net/~jflax/jmf_fun.htm (Typical of some of the lists that people compile for the fun and benefit of others)

There are hundreds of other sites that are a mine of information in themselves.

Results

So after all of this, what do we actually produce? Well most of our day-to-day work is taken up with what we have termed tactical requests. That is, requests from investigators, which are needed there and then. "Where does this person live and who are his associates?" www.experian.co.uk "I have a woman's first name and I know she lives in Manchester..." www.gb.co.uk " What can you tell me about the head of the Russian Organised Crime Task Force?" www.securities.co.uk "When is the next anarchist march on Parliament?" http://www.ainfos.ca "I need a picture of Fujian in China" http://china-window.com. "What can you find out about smart card fraud?" http://www.occ.treas.gov/launder/orig1.htm There is a constant stream of such requests, which arrive in the Open Source Unit.

In addition we conduct a monitoring service for a number of police clients. The Royalty Protection Unit uses us extensively to carry out research prior to royal visits or sensitive meetings. Although I am not free to give any details I can tell you that certain checks made through the Open Source Unit last year were critical and succeeded in providing an extra

level of protection for the royal family. The particular case I am talking about was able to use the connection of open sources and the transatlantic network of open source experts. It was an ideal case of knowing the right person with the right tools. www.lexis.nexis.com

One of our more recent projects is concerned with piracy, (http://www.vantage-security.com) not the type of piracy of intellectual copyright but the murder and robbery of people and companies on the high seas. Fortunately we were able to collect plenty of open source material from the Internet to allow a number of senior officers to attend conferences in some very exotic parts of the world. (sic) Seriously, though, we are having to deal with more and more cases of British citizens who are victims of such crimes and there is an international effort to deal with the problem as it continues to escalate. The Internet provides a rich source of cases, which span the past five to ten years, and it was very easy to see that escalation in real and human terms as the numbers and degree of violence and sophistication has risen. (http://www.usnews.com/usnews/issue/970623/23pira.htm)

In addition to tactical requests and ongoing research we have also begun to produce open source bulletins on a limited number of subjects. Focussing on Russian Mafiya, Organised Crime, Drugs, Terrorism and Money Laundering we have established a small but grateful clientele to whom we supply academic articles, expert observation, news and emerging developments in those fields. We concentrate on getting the bulletin produced quickly and onto the desktops of those who will really benefit, as well as those who just like to get a copy of everything! We have found that it is important to keep the size of the documents manageable but with the right balance of information type included. As each publication goes out we learn a little more about the skills of publication but pride ourselves that the speed and ease of production combined with the accurate targeting of the right customer far outweighs some of the niceties which some other glossy publications enjoy. Our first set of bulletins were researched, collected, collated, printed and distributed by one person, me, in one day. It was a bit rough but it certainly generated some interesting and interested telephone calls. The distribution list also doubled almost overnight. So far they have been very well received and there are hopes to increase the frequency and content as and when personnel changes in the unit make that feasible.

That concludes my presentation. I hope that this has been a useful insight into the workings of the Metropolitan Police Open Source Unit and it's everyday business. I shall welcome any questions and be happy to talk to any of you later either to give or receive advice.

Thank you.

EuroIntel '99 PROCEEDINGS E1-European Intelligence Forum "Creating a Virtual Intelligence Community in the European Region: Open - Link Page

Previous	Exhibitor: DataExpert (NL)
Next	THE INTERPOL EXPERIENCE

Return to Electronic Index Page