Statewatch Analysis

Spying in a see through world: the "Open Source" intelligence industry

Ben Hayes

The Open Source Intelligence industry has grown rapidly over the past decade. Private companies free from the privacy statutes that constrain state agencies are collecting data on a vast scale and the practice has been widely embraced by EU institutions and Member States

> *"In the past few years, Open Source Intelligence has become the target of what could almost be described as infatuation in both the EU institutions and many of its member states"* - Compagnie Européenne d'Intelligence Stratégique (2008).

Introduction: what is OSINT?

The US military defines 'Open Source Intelligence' (OSINT) as "relevant information derived from the systematic collection, processing and analysis of publicly available information in response to intelligence requirements".[1] "Open source" is "any person or group that provides the information without the expectation of privacy", while "publicly available information" includes that which is "available on request to a member of the general public; lawfully seen or heard by any observer; or made available at a meeting open to the general public". 'Open source' intelligence is thus defined by virtue of what it is not: "confidential", "private" or otherwise "intended for or restricted to a particular person, group or organization". But this distinction is undermined in practice by the categorisation of 'weblogs', internet 'chat-rooms' and social-networking sites as "public speaking forums".

Prior to the IT revolution, OSINT gatherers were primarily concerned with the left wing press and the situation in foreign countries. Intelligence was obtained by reading the papers, debriefing businessmen and tourists, and collaborating with academics and scholars. Indeed, OSINT specialists have

bemoaned the substantial decline in the number of foreign correspondents working for major newspapers (a consequence of declining print media revenues). This loss has been off-set, however, by the wealth of information now available on the world-wide-web, which has seen OSINT transformed into a desk-based activity requiring nothing more than an internet connection, a web browser and a telephone. As the RAND Corporation has observed: "the proliferation of [online] media and research outlets mean that much of a state's intelligence requirements can today be satisfied by comprehensive monitoring of open sources".[2] The CIA has even been quoted as saying that "80% of its intelligence comes from Google".[3]

From a security perspective there is nothing inherently problematic about the use of OSINT. On the contrary, the security services would be negligent if they didn't utilise information in the public domain to inform their work; everyone else engaged in public policy matters does the same thing. However, from a civil liberties perspective, the process of appropriating personal information for the purpose of security classification *is* inherently problematic, since it is often based on wholly flawed assumptions about who or what poses a 'threat'. The mere act of recording that someone spoke out publicly against the War, attended a demonstration, or is friends with a known 'security risk', brings with it a significant possibility that this information will be used prejudicially against them at some point in the future. This in turn calls into question the democratic legitimacy of surveillance and intelligence gathering, a legitimacy that rests on questions of who is doing the watching, how, and why?

OSINT and the police

In an address to the *Eurointel '99* conference, a spokesman for New Scotland Yard's (NSY) OSINT described open sources as "any form or source of information available to us either as a paying customer or for free".[4] Such information may be used for tactical or strategic purposes. "Tactical" information is that which is needed urgently, whereas "strategic" information "can be collected through long-term research as part of an ongoing project", around topics such as organised crime, money laundering, terrorism and drugs. Tactical requests to NSY's OSINT unit are said to include enquiries like "where does this person live and who are his associates?", "I have a woman's first name and I know she lives in Manchester", or "when is the next anarchist march on parliament"? According to NSY:

> *Much of this is surprisingly easily using some very simple tools and officers are astonished when they come to us with nothing more than a name and we return address lists, family names and addresses, companies and directorships, financial details and associates.*

The police OSINT specialists also use 'people finder' sites that "can employ directories, public records, telephone records, lists, email finders, homepage finders etc".

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 want that little bit more.

Tellingly, all of Scotland Yard's "online transactions are done covertly" using "undercover companies, pseudonyms and covert companies in the same way [as] with any other covert operation". "This helps to prevent anyone seeing that the police have been looking", they explain. It also raises fundamental questions of accountability [unlike the intelligence services, the police are supposed to be accountable for their investigative techniques], regulation [to what extent do police intelligence gatherers respect the laws and principles of privacy and data protection] and democratic control [what oversight mechanisms exist?]. The Yard's spokesman was candid about viewing data protection as an unreasonable 'barrier' to his work:

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 [credit rating and financial intelligence companies], to name but two, over exactly how DP legislation is to be interpreted.

Privatising OSINT

In 2002, Dr. Andrew Rathmell of *RAND Europe* called for the "privatisation of intelligence", arguing that there was "little reason to think that [OSINT collection] can better be done by in-house experts than by established private sector research institutes and companies".[5] As in other areas of security and defence, it was argued that outsourcing could "relieve budgetary pressures". "In order to benefit from the ongoing information and intelligence revolutions", suggested *RAND*, "all European states could benefit from closer European collaboration, both between governments and with the private sector". Dr. Rathmell also observed that:

Not only are open sources now more widely available, but the information revolution is now blurring the boundaries between open and covert sources in regard to the formerly sacrosanct technical collection means.

The OSINT industry has grown rapidly over the past decade as a trend that began in the USA has quickly taken hold in Europe. *Equifax* and *Experian* (referred to above), are 'data aggregators', organisations that are able to create an increasingly high-resolution picture of an individuals' activities by drawing together data from a variety of sources. As the *American Civil Liberties Union* (ACLU) has explained: "These companies, which include *Acxiom*, *Choicepoint*, *Lexis-Nexis* and many others, are largely invisible to the average person, but make up an enormous, multi-billion-dollar industry".[6] Whereas privacy statutes constrain governments' ability to collect information on citizens who are not the targets of actual police

investigations, "law enforcement agencies are increasingly circumventing that requirement by simply purchasing information that has been collected by data aggregators", say ACLU.

European data aggregators include *World-Check*, a commercial organisation that offers "risk intelligence" to reduce "customer exposure to potential threats posed by the organisations and people they do business with".[7] *World-Check* is the sort of place you go to check if an individual or entity appears on any of the 'terrorism lists' drawn-up by the UK, EU, USA or UN (among many others). The organisation claims to have a client base of "over 4,500 organisations", with a "renewal rate in excess of 97%". According to *World-Check's* website, its research department "methodically profiles individuals and entities deemed worthy of enhanced scrutiny"; its "highly structured database" is "derived from thousands of reliable public sources". Another service offered by *World-Check* is an online "Passport-Check" that "verifies the authenticity of 'machine readable' (MRZ) passports from more than 180 countries" as proof of due diligence". An annual subscription allows for "unlimited access, look-ups, printouts and suspicious name reporting".

In Britain in the 1980s, the *Economic League* drew up its own 'blacklists' and acted as a rightwing employment vetting agency. The League, which was acknowledged to have close links with the security services, had accumulated files on at least 30,000 people, files it shared with more than 2,000 company subscribers, in return for annual revenues of over £1 million. The files it held contained details of political and trade union activists, Labour Party MPs and individuals who, for instance, had written to their local papers protesting at government policy. The League always maintained that 'innocent' people had nothing to fear as they only kept files on "known members of extreme organisations". Critical investigative reporting coupled with a campaign against the organisation saw it disband in 1993 (though its Directors reportedly set-up a new company offering the same service on the basis of the same files the following year).[8] An enterprise considered illegitimate in the early 1990s has now been supplanted by an entire industry.

Infosphere AB, based in Sweden, is a "Commercial Intelligence and Knowledge Strategy consultancy".[9] "No other company or organization in the world has our experience in the use and development of [OSINT] methods and Business Knowledge strategy", it claims, "many nations and corporations both follow our recommendations and use our continuous support". *Infosphere's* "Profiling services" offer "fact based background checks, media analysis and relationship mapping of people, companies and organizations" in "any corner of the world":

> *With a range of proven methodologies, direct investments and ownership of state-of-the-art intelligence services, combined with an access to electronic and human sources throughout the world, we have the proven experience and knowledge to address even your most difficult product and development challenges.*

Sandstone AB ("Because You Need To Know"), based in Luxembourg, offers a similar range of services using "Actionable intelligence on demand".[10] *Infosphere* and *Sandstone* have teamed up to create *Naked Intelligence* ("Gathering Knowledge in a See Through World"), an OSINT conference "where knowers and doers from fields such as competitive intelligence, business intelligence, signals Intelligence and HUMINT gathers openly together under one roof".[11] *Naked Intelligence 2009* was held in Luxembourg, the 2010 event will take place in Washington in October.[12]

OSINT theory and practice

With information and communications technology offering up so much potential 'open source intelligence', scientists and computer programmers have teamed up to automate the process of collecting and analysing this data. The University of Southern Denmark, for example, has established an institute for applied mathematics in counter terrorism, the "Counterterrorism Research Lab" (CTR Lab), which conducts research and development around:

> *advanced mathematical models, novel techniques and algorithms, and useful software tools to assist analysts in harvesting, filtering, storing, managing, analyzing, structuring, mining, interpreting, and visualizing terrorist information.[13]*

Its products include the *iMiner* ("terrorism knowledge base and analysis tools"), *CrimeFighter* (a "toolbox for counterterrorism") and *EWaS*, (an "early warning system" and "terrorism investigation portal"). The CTR Lab has also organised international conferences on themes like "Counterterrorism and OSINT", "Advances in Social Networks Analysis and Mining" and "OSINT and Web Mining". As the EU's Joint Research Centre observes:

> *The phenomenal growth in Blog publishing has given rise to a new research area called opinion mining. Blogs are particularly easy to monitor as most are available as RSS feeds. Blog aggregators like Technorati and Blogger allow users to search across multiple Blogs for postings. Active monitoring of Blogs applies information extraction techniques to tag postings by people mentioned, sentiment or tonality or similar…[14]*

Ostensibly, governments use this technology to help them understand public opinion, in much the same way as they use 'focus groups'. Of course, the very same technology can also be used to identify groups and individuals expressing 'radical' or 'extremist' views.

In the USA, the Mercyhurst College offers degrees in "Intelligence Analysis", promising its graduates jobs with the CIA and the US Army, amongst others.[15] In July 2010, Mercyhurst organised a "Global Intelligence Forum" in Dungarvan, Ireland, with panels on medicine, law, finance, technology, journalism, national security, law enforcement, and business intelligence.[16] Kings' College in London now offers an OSINT diploma, covering "both theoretical and practical aspects of OSINT, including OSINT collection and analysis methodologies".[17] It advises that

"Students taking this module should consider applying for the traineeship scheme with the EU Institute for the Protection and Security of the Citizen" (IPSC, part of the EU Joint Research Centre).

From the private sector, *Jane's Strategic Advisory Services* (the consultancy division of defence specialist *Jane's*), also offers an OSINT collection and analysis training service.[18] The course covers "overarching methods, best practices, considerations, challenges and tools available to open source intelligence analysts". Tutors include Nico Prucha, whose expertise includes "on-line jihadist movements and ideologies", "using blogs and social networking tools for intelligence collection", "navigating and assessing forums and the 'Deep Web'", "key word analysis", "sentiment analysis" and "on-line recruitment and radicalization patterns".

Crossing the boundaries

As noted above, the information revolution is, in the words of the RAND Corporation, "blurring the boundaries between open and covert sources in regard to the formerly sacrosanct technical collection means". On the one hand, OSINT tools can be used to 'mine' publicly available (and privately held) datasets to conduct *de facto* surveillance on named groups and individuals. On the other, the very same 'community' of scientists, programmers and hackers, has developed a whole range of so-called 'spy-ware' applications that enable to users to conduct covert and intrusive surveillance. Products include 'phishing' applications, used to acquire sensitive information such as usernames and passwords, and a variety of 'keystroke loggers', used to surreptitiously record computer users activities. Meanwhile, the illegal interception of GSM (mobile) telecommunications is "cheap, easy, and getting easier" and, as Google demonstrated recently, the hacking of unsecured wireless networks is straightforward.[19] Although the EU has criminalised the unauthorised use of spy-ware, hacking and interception techniques, this has done nothing to stem their development. Moreover, some EU law enforcement are in clearly using them, having repeatedly demanded so-called 'lawful access' powers, allowing them to legally access suspects' computer hard drives through the internet, and without the knowledge of those affected. The crux of the matter is that both the police and the private investigator are steadily accumulating *the capacity* (if not the lawful powers) to conduct the kind of covert and intrusive surveillance that was once the preserve of GCHQ and the secret intelligence services.

OSINT and the European Union

The EUROSINT Forum is a Belgian not-for-profit association "dedicated to European cooperation and use of [OSINT] that prevent risks and threats to peace and security".[20] It was launched in 2006 with the support of the European Commission's "Justice, Liberty and Security" (JLS) Directorate.

EUROSINT's mission is to "create a European 'intelligence ecology' that is dedicated to provoking thought on [OSINT] and its use in the intelligence and security spheres by public and private sector organisations". Other goals include giving "voice" to "private sector actors dealing with security and intelligence issues" and "building a positive image for OSINT in the EU", and "the creation of partnerships between private companies and/or public organisms, to create European consortiums that can bring forward new projects". Members of the EUROSINT Forum include EU institutions, national defence, security and intelligence agencies, private sector providers of intelligence, technology developers, universities, think-tanks and research institutes. Among the companies paying the €5,000 EUROSINT annual membership fee are Jane's, Lexis Nexis, Factiva (UK), Oxford Analytica (UK), CEIS-Europe (Compagnie Européenne d'Intelligence Stratégique, France's largest Strategic Intelligence Company) and Columba Global Systems (Ireland).

EUROSINT believes that "OSINT provides EU institutions with the perfect platform to, quite legitimately, initiate intelligence cooperation".[21] These convictions are shared by SITCEN (the EU's "Joint Situation Centre" and forerunner to any future EU intelligence service), which also saw OSINT as the logical starting point for its activities.[22] SITCEN, FRONTEX and the EU JRC are all EUROSINT members, along with three Commission DGs. In 2008, Axel Dyèvre, Director of the European Company for Strategic Intelligence (CEIS, a founder member of EUROSINT), went as far as to claim: "In the past few years, [OSINT] has become the target of what could almost be described as infatuation in both the EU institutions and many of its member states".[23]

EUROSINT and its member organisations have received backing for their activities from the EU. In 2008, DG JLS funded a *EUROSINT* project on "Open Source Intelligence in the fight against Organised Crime" under its multiannual ISEC (organised crime) programme. *EUROSINT* is also part of the 18 member VIRTUOSO consortium, which has just been awarded €8 million from the EU Security Research Programme (ESRP). The consortium promises a "pan-European platform for the collection, analysis and disemination of OSINT" providing EU actors "with real-time OSINT aggregation as well as text-mining, early warning and decision support tools". Members of the VIRTUOSO consortium include *CIES* and *Colomba*, European Defence giants *EADS* and *Thales*, and the Dutch military research agency *TNO*. The European Defence Agency (EDA) has also funded EUROSINT to produce studies on "OSINT search engines" and the devlopment of "Universal Intelligence Analyst's Tools", and to provide OSINT training in conjunction with the EDA, including a 30 week course in 2009.[24] The EU *Joint Research Centre* (JRC) has even developed its own OSINT suite featuring a "web mining and information extraction tool, which is now in trial usage at several national law enforcement agencies".[25] The software "extracts and downloads all the textual content from monitored sites and applies information extraction techniques. These tools help analysts process large amounts of documents to derive structured data".

Many OSINT providers have homed in on the potential of this kind of software to identify *potentially* dangerous people by analysing information on the web, techniques that are coming to be known as 'counter-radicalisation'. SAFIRE is another ESRP-funded project, to which the EC is contributing €3 million. It promises a "Scientific Approach to Fighting Radical Extremism" and has the goal of "improv[ing] fundamental understanding of radicalization processes and us[ing] this knowledge to develop principles to improve (the implementation) of interventions designed to prevent, halt and reverse radicalization". The SAFIRE consortium is led by the Dutch military research institute *TNO* and includes the *RAND Corporation*, Israel's *International Counter-Terrorism Academy* and *CEIS*. "Radicalization on the Internet" and "observable indicators of the radicalization process" are among the topics that SAFIRE will address.[26] The European Union has already adopted a far-reaching 'radicalisation and recruitment' Action Plan as part of its counter-terrorism programme and, according to documents just revealed by *Statewatch*, the EU has now tacitly extended this programme to include political activists from across the political spectrum, which it labels as "Extreme right/left, Islamist, nationalist or anti-globalisation".[27]

Conclusion

Writing recently in the Guardian, Professor John Naughton observed:

> *[T]he internet is the nearest thing to a perfect surveillance machine the world has ever seen. Everything you do on the net is logged – every email you send, every website you visit, every file you download, every search you conduct is recorded and filed somewhere, either on the servers of your internet service provider or of the cloud services that you access. As a tool for a totalitarian government interested in the behaviour, social activities and thought-process of its subjects, the internet is just about perfect.[28]*

The present threat to civil liberties, however, comes neither from the internet nor totalitarian governments, but from a neo-McCarthyite witch-hunt for "terrorists" and "radicals", and a private security industry bent on developing the "perfect surveillance" tools to find them. For all the concern about *Facebook's* privacy policy,[29] that company is no more responsible for its users' wishes to 'broadcast themselves' than travel agents are for tourism. Of course *Facebook* should offer maximum privacy protection for its users, but those of us concerned with freedom and democracy need to see the bigger picture in terms of who is doing the watching, how, and why. We must then develop the tools and communities needed to bring them under democratic control.

Footnotes

1 "Open Source Intelligence", US military handbook, 5.12.2006 http://www.fas.org/irp/doddir/army/fmi2-22-9.pdf.

2 "The Privatisation of Intelligence: A Way Forward for European Intelligence Cooperation – "Towards a European Intelligence policy", A. Rathmell, RAND Europe, in "NATO Open Source Intelligence Reader", February 2002:
http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf.

3 "Open Source Intelligence", Clive Best, EU Joint Research Centre, 2008: http://media.eurekalert.org/aaasnewsroom/2008/FIL_000000000010/071119_MMDSS-chapter_CB.pdf.

4 "SO11 Open Source Unit Presentation", Steve Edwards (Detective Constable), New Scotland Yard, Eurointel '99:
http://www.oss.net/dynamaster/file_archive/040319/c7f74b0455dda7c58e7dd31d909c9d31/OSS1999-E1-05.pdf .

5 See: "The Privatisation of Intelligence...", note 2, above.

6 "The Surveillance-Industrial Complex: How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveillance Society", American Civil Liberties Union, 2004:
http://www.aclu.org/surveillance.

7 World Check website: http://www.world-check.com/.

8 "Economic League disbanded", Statewatch Bulletin, July 1993. See also "Economic League relaunched", Statewatch Bulletin, June 1994.

9 Infosphere website: http://www.infosphere.se/.

10 Sandstone website: http://www.sandstone.lu/.

11 "A unique Open Source Intelligence event in the heart of Europe", press release, 5.7.2009: http://www.prlog.org/10274607-unique-open-source-intelligence-event-in-the-heart-of-europe.html

12 Naked Intelligence website:
http://www.nakedintelligence.org/extra/pod/

13 CTR Lab website: www.ctrlab.dk/

14 See "Open Source Intelligence", note 3, above.

15 Mercyhurst College website: http://www.mercyhurst.edu/

16 Global Intelligence Forum, Dungarvan Conference 2010, 11-13.7.10: http://www.regonline.com/builder/site/Default.aspx?eventid=826351

17 Kings' College website:
http://www.kcl.ac.uk/schools/sspp/ws/grad/programmes/options/opensource.

18 Janes' website: http://www.janes.com/consulting/OSINT.html

19 "Intercepting Mobile Phone/GSM Traffic", David Hulton, Black Hat Briefings, 2008: http://www.blackhat.com/presentations/bh-europe-08/Steve-DHulton/Presentation/bh-eu-08-steve-dhulton.pdf

20 EUROSINT website: http://www.eurosint.eu/publications

21 EUROSINT (powerpoint presentation):
http://www.eurosint.eu/files/Eurosint%20Presentation.pdf

22 "Secret Truth: The EU Joint Situation Centre", Jelle van Buren, Eurowatch, 2009:
http://www.statewatch.org/news/2009/aug/SitCen2009.pdf

23 "Intelligence cooperation: The OSINT option", Axel Dyèvre, Europolitics.info, 28.10.2008: http://www.europolitics.info/dossiers/defence-security/intelligence-cooperation-the-osint-option-art151325-52.html

24 http://www.eda.europa.eu/genericitem.aspx?area=organisation&id=308

25 See "Open Source Intelligence", note 3, above.

26 "TNO, RAND and Israeli Counter-terrorism academy awarded €3 million EC "radicalisation and recruitment" contract", NeoConOpticon blog, June 2010: http://neoconopticon.wordpress.com/2010/06/16/tno-rand-and-israeli-counter-terrorism-academy-awarded-e3-million-ec-radicalisation-and-recruitment-contract/

27 See "Intensive surveillance of "violent radicalisation" extended to embrace suspected "radicals" from across the political spectrum", Tony Bunyan, Statewatch, June 2010: http://www.statewatch.org/analyses/no-98-eu-surveillance-of-radicals.pdf

28 "The internet: Everything you ever need to know", Observer, 20.6.2010: http://www.guardian.co.uk/technology/2010/jun/20/internet-everything-need-to-know

29 "Privacy Groups to Facebook: There's More to Do", American Civil Liberties Union, 16.6.2010: http://www.aclunc.org/issues/technology/blog/privacy_groups_to_facebook_theres_more_to_do.shtml

This Analyses was first published in *Statewatch Journal*, vol 20 no 1