Chapter 4
OSINT as Part of the Strategic National Security Landscape

Laurence Marzell

Abstract This chapter looks at the context, application and benefits of OSINT for use in decision making, as an integrated part of the wider intelligence mix and, as an essential component within the overall Intelligence Cycle. OSINT is a growing and increasingly critical aspect in decision making by LEAs—and has been even before the burgeoning use of social media brought open source to the fore. But, its full integration into the wider intelligence mix, as well as into an overarching information governance framework, is essential to ensure efficient and effective contribution to usable intelligence able to support better informed decision making. Fundamentally, unless the system in which OSINT is used as interoperable as the system is in which decision-making is taking place, the application and value of OSINT will be far less effective, efficient and meaningful. This chapter addresses OSINT in the context of the Intelligence Process and the need to resolve the challenges and issues surrounding the integration and use of OSINT into the Intelligence Cycle. It further discusses how an overarching information governance framework may support OSINT for decision making within the wider Intelligence Mix.

4.1 Introduction

This chapter looks at the context, application and benefits of OSINT (Open Source Intelligence) for use in decision making, as an integrated part of the wider intelligence mix and, as an essential component within the overall Intelligence Cycle. Both of which are described in detail in the section on understanding the Intelligence Cycle in which OSINT must exist and the wider intelligence mix in which it must integrate. Then as part of this wider intelligence mix and cycle, how LEAs (Law Enforcement Agencies) need to enable their use of such an integrated OSINT, through a unified framework of information governance: able to bring both

L. Marzell (✉)
SERCO, Hook, UK
e-mail: Laurence.Marzell@serco.com

B. Akhgar et al. (eds.), *Open Source Intelligence Investigation*,
Advanced Sciences and Technologies for Security Applications,
DOI 10.1007/978-3-319-47671-1_4

open and closed source intelligence together in a meaningful and unified way to support better informed decision making.

So like all other data, OSINT must be understood, integrated and used in a unified way and as part of the mix with the myriad other data sources available to decision makers, to create the trusted intelligence they need to support their tasks. It is important to note that, in their use of OSINT for decision making—and indeed, not just OSINT but the entire mix of data across the spectrum of the intelligence cycle—both LEAs and the military face similar, shared challenges and issues.

In setting OSINT into context, this chapter uses the decision making needed in major crisis, humanitarian and emergency situations, and some areas of serious organised crime and counter terrorism as its basis. Here, while civil jurisdiction presides, LEA decision making often relies closely on the capability and expertise that underpins that of the military, in use of the wider intelligence mix and cycle, where data sources, information processing and analysis are heterogeneous and shared. It is here also that military capability and expertise can also often be used to support LEAs in an operational capacity.

4.2 Understanding the Strategic Landscape into Which OSINT Must Be Applied

Decision makers, in both the civilian and military domains, operating at Grand Strategic,[1] Strategic and Tactical levels, face a continuous need for faster, more trusted and better informed decision making. Analysts interpreting the data, turning it into meaningful intelligence, face a constant struggle to cope with the ever increasing Volume, Velocity, Variety and Validation of data (4Vs) (Akhgar et al. 2015), the plethora of formal and informal (OSINT) data sources and, the ambiguities surrounding the trustworthiness of that data.

Better informed decision making manifests itself in many ways. At the grand strategic level it can be seen in situations such as, for example, questioning whether sufficient and reliable intelligence is available on terrorist activity in Nigeria to warrant external intervention. Alternatively it can be at a lower but no less critical level, as might be found in peacekeeping, humanitarian relief and disaster response operations such as that in the Mediterranean supporting refugees. Or, in the Nepalese earthquake of April 25, 2015 where a massive 7.8 magnitude quake struck Nepal, just northwest of the capital of Kathmandu—the worst quake to strike the region in more than 80 years. Moreover, decision making in this context may arise when used by LEAs against serious organised crime or terrorism. In all of these

[1]Grand Strategic: An overarching concept that guides how nations employ all of the instruments of national power to shape world events and achieve specific national security objectives. Grand strategy is also called high strategy and comprises the "purposeful employment of all instruments of power available to a security community" (Military historian B. H. Liddell Hart).

examples a number of critical factors combine and compound themselves. This makes achieving the increasing 4V's of data being created, and therefore potentially that must be considered, for both short and long term analysis, a significant, increasing, and ever present challenge (see Chaps. 2 and 3).

For the military, this need for better informed decision making has seen the development and deployment of an integrated ability to collect and disseminate information through the use of extremely powerful sensors (Visual-optical and infra-red, Radar-active and Electronic Warfare—passive) fitted to a variety of high value air, land and naval platforms. This ability, known as C4ISTAR, addresses a spectrum of capabilities that covers Command, Control, Communications, Computers, Information/Intelligence, Surveillance, Targeting Acquisition and Reconnaissance.

This ability was supplemented in the early 2000s with constellations of geo-stationary and earth orbiting satellites that further enabled this and added time and positioning capability. The need for accurate and timely data for decision making is no less in the civilian world. While the technology and access to budgets might be somewhat different to those of the military, with the now relatively inexpensive access not only to open source space-based imagery and time and positioning or voice and data communications, the increase in technological advancement across a swathe of data generating sensors (both space-based and other) means that the same challenges of speed, volume, ambiguity and trustworthiness faced by the military (i.e., the 4Vs) in support of better informed decision making, affects civilian LEA end users too.

The Battlespace[2] is the term used to describe the domain in which the military now conduct their operations in time of hostility. In peacetime, where the military are operating in support of LEAs the term might best be described as the Security space; where all of the assets, people, information, networks and technology function together and are considered as a system of systems, when looked at and considered as a whole.

Of increasing significance for civilian authorities and LEAs—regardless of their geographic or territorial jurisdiction—is our increasingly complex and interconnected world in which decision making must now take place amidst greater complexity, ambiguity and interdependency; and, in which the supporting intelligence cycle must keep pace technologically as well as through all aspects of the human dimension.

[2]Battlespace: The effective combination, or integration, of all elements of a Joint force to form a coherent whole, clearly focused on the Joint Task Force Commander (JTFC)'s intent, is critical to successful Joint operations. Integration of individual Force Elements (FEs) enables their activities and capabilities to be coordinated and synchronised, in accordance with clear priorities, under unified command. On multinational and multi-agency operations, the contributions of other participating nations and non-military actors should also be harmonised wherever feasible. UK doctrine is, as far as practicable and sensible, consistent with that of NATO. The development of national doctrine addresses those areas not covered adequately by NATO; it also influences the evolution of NATO doctrine in accordance with national thinking and experience. Source: UK MoD Joint Doctrine Publication 3-70 (JDP 3-70), dated June 2008.

This can be seen in society's relationship with Critical Infrastructure (CI) upon which citizens, communities and society as a whole, depend for its health, well-being and very survival. Here society, and the many varied and different communities in which citizens live, has become wholly dependent upon the many sectors of CI and essential services such as transport, energy, health, finance, food and communications with which their health and well-being is intrinsically linked. CI and the network of interconnected and interdependent systems that support and underpin it, like the Security Space of decision making mentioned above, can also be described as a system of systems.

Critical infrastructure is often described as a 'system of systems', which functions with the support of large, complex, widely distributed and mutually supportive supply chains and networks. Such systems are intimately linked with the economic and social wellbeing and security of the communities they serve. They include not just infrastructure but also networks and supply chain that support the delivery of an essential product or service (Pitt 2008).

And sitting within, alongside or straddling these CI System of Systems, are the many varied and inextricably intertwined different communities, often referred to as ecosystems in how they evolve are structured and function. It is against this backdrop that the decision making must occur in relation to the planning, preparation, response and recovery to significant man-made, malicious or natural events.

This dependence of communities and society is exponentially increased to risks, hazards, threats and vulnerabilities by the very nature of how these System of Systems interoperate in order to function; with many unseen and indeed unknown, interdependencies and dependencies across and between them. When shocks to the system occur, whether man-made, malicious or natural, they can have unknown consequences or cascade effects, disproportionate to the event that may have caused them (see Chap. 1).

It is here where multiple decision makers from the many different civilian organisations and LEAs (both at local and regional levels within individual nations or in cross-border border cooperation) must come together and collaborate efficiently and effectively to achieve a set of common and shared outcomes. These outcomes manifest themselves in the planning and preparation for, response to and recovery from such shocks, as well as in the planning, preparation, conduct and often review or inquest, of such law enforcement activities as might be seen with serious organised crime or terrorism.

It is in these instances, where complexity is inherent in the system itself. Where with the intrinsic difficulty of multiple different organisations needing to work together efficiently and effectively to achieve a combined effect from their collective effort that the unseen consequences or cascade effects arising from the interdependencies of the system itself will mean that poorly informed decision making can be counted in lives lost as well as in terms of economic cost, physical damage or societal well-being. OSINT is a growing and increasingly critical aspect in decision making by LEAs in these situations—and has been even before the burgeoning use of social media has brought open source to the fore. The advent of social media as a source of open source intelligence has, for the most part, brought the extent and

range of OSINT sources that are now available to a greater range of audiences, users and applications. Fundamentally, unless the system within which it sits and is used, in this case the Intelligence Cycle, is as interoperable as the system is in which decision making is taking place, then the application and value of OSINT will be far less effective, efficient and meaningful (see Chaps. 9 and 16).

One example which provides a useful historic context to this development and use, is taken from a 2002 case study in Australia as documented in a 2004 NATO report on OSINT (NATO 2002; see also Chaps. 12 and 16).

Case Study: The Heads of the Criminal Intelligence Agencies (HCIA) conference in Australia September 1998 directed that a business case be prepared for the establishment of a centralised open source unit. This was announced by Paul Roger, Director of Intelligence of the Queensland Criminal Justice Commission, in his paper presented at 'Optimising Open Source Information'. The open source unit will meet Australian law enforcement requirements for collection and dissemination of open source material. The clients of the open source unit will initially be limited to the agencies that comprise the Criminal Intelligence Agencies. After the unit is established, additional agencies may be included as clients of the open source unit. The establishment of an open source unit provides the criminal intelligence community with an ideal opportunity to market an information brokerage service to other agencies. There is also potential for the unit to become part of a larger unit and networking between other open source units including the Royal Canadian Mounted Police (RCMP), Europol and the UK's Metropolitan Police Service. The unit will initially concentrate on providing open source information rather than intelligence. When the unit has found its niche it can then concentrate on four other functions: current awareness briefs; rapid response to reference questions; contacting outside experts for primary research; and coordinating strategic forecasting projects. It will draw upon the full range of external open sources, software and services.

4.3 Understanding the Intelligence Cycle in Which OSINT Must Exist and the Wider Intelligence Mix in Which It Must Integrate

With the burgeoning use of and dependence on OSINT now firmly established, its full integration into the wider intelligence mix and with it, into an overarching information governance framework, is essential to ensure efficient and effective contribution to usable intelligence able to support better informed decision making. It is important at this stage to provide a context as to why information governance for the entirety of the intelligence mix, including that of OSINT, is so essential.

Different organisations view the world in which they exist and must operate very differently. These differing views are driven by many factors such as risk, history, culture, capability, economics and leadership. From these views flow how

organisations conduct their business: their governance and policies, training, budgets, processes, systems, and so on. An organisation's view of the world, relative to any other organisation(s) with which it collaborates, is neither right nor wrong; it is just different. But these differences, especially in terms of governance and policy, where resulting information and decisions need to flow across organisational, operational or jurisdictional boundaries (both internally within organisations or nations as well as externally of those organisations or nations), are significant areas of risk. This is where failures can and often do occur, especially in our interconnected world where dependencies and interdependencies can often, in the wake of a major incident, lead to consequences and cascade effects way beyond the original cause.

Where different organisations need to come together in mission critical situations, to achieve a set of shared aims, objectives and outcomes, without a unified and common understanding and approach to how information is processed, analysed, understood and acted upon, as would be provided by good information governance, the likelihood of failure or less effective results in achieving those aims, objectives or outcomes is extremely high. This is based upon the risk of the different organisations and agencies involved, making conflicting or ineffective decisions, resulting from their different interpretations of the intelligence or their different responses to the intelligence, as influenced by their different organisational approaches and views of the world in which they exist and operate.

In simple terms, both strategic and tactical decision making, in military or civil domains, or in those of the shared space that occurs in significant crisis, emergency or serious organised crime or terrorism events or operations, requires the collection of data from all available, relevant sources—technical and human—and from both open source (e.g. social media, internet and commercially available) and closed (military or other specific). It then requires the critical processing where the analysis takes place to turn the disparate, ambiguous and multiple source information into usable, meaningful, trusted, accurate and timely intelligence. Then for onward dissemination out to appropriate end users. A feedback mechanism is required to verify and validate the accuracy along with a metric, if necessary or appropriate, to decide which is 'best'. All of which needs to sit within a unified and common information governance framework to ensure that regardless of each organisation's differing view of the world, everyone is viewing the resultant intelligence and decision making needs from the one unified and shared view. Better informed decisions can then result.

It is here, that it is important to describe the Intelligence Cycle or Process, how it supports decision making, and, the issues and challenges that OSINT, as an integrated part of that mix and cycle, faces. Owing to the inherent nature and sensitivity of much of that which surrounds intelligence gathering, analysis and use, with much of the topic area subject to security classification, this chapter uses freely available open source material as its basis. This material is of sufficient detail and accuracy to offer sound explanation—a fitting testament to the breadth and depth of previously classified information which is now freely available. Six phases make up the Intelligence Cycle: (1) Direction; (2) Collection; (3) Processing; (4) Analysis; (5) Dissemination and (6) Feedback. Figure 4.1 provides an overview of the Intelligence Process.

Fig. 4.1 The intelligence process/cycle (Source: "Joint Publication 2-0, Joint Intelligence". Defense Technical Information Center (DTIC). Department of Defense. February, 2013)

1. **Direction**: Using an example at the Grand Strategic or Strategic level, in the first instance, intelligence requirements and needs are determined by a decision maker to meet the objectives they seek to achieve. In NATO, a commander uses requirements (sometimes called 'Essential Elements of Intelligence (EEIs)) to initiate the intelligence cycle, whereas in the United States requirements can be issued from the White House or Congress. This is termed Direction.
2. **Collection**: In response to requirements, intelligence staff develop an intelligence collection plan applying available sources and methods and seeking intelligence from other agencies. Collection includes inputs from several intelligence gathering disciplines, such as HUMINT (human intelligence), IMINT (imagery intelligence), ELINT (electronic intelligence), SIGINT (Signals Intelligence), OSINT (open source, or publicly available intelligence), etc. This is termed Collection.
3. **Processing**: Once the collection plan is executed and information arrives, it is processed for exploitation. This involves the translation of raw intelligence materials, quite often from a foreign language, evaluation of relevance and

reliability, and collation of the raw intelligence in preparation for exploitation. This is termed Processing.

4. **Analysis**: Analysis establishes the significance and implications of processed intelligence, integrates it by combining disparate pieces of information to identify collateral information and patterns, then interprets the significance of any newly developed knowledge. This is termed Analysis.
5. **Dissemination**: Finished intelligence products take many forms depending on the needs of the decision maker and reporting requirements. The level of urgency of various types of intelligence is typically established by an intelligence organization or community. An indications and warning (I&W) bulletin would require higher precedence than an annual report, for example. This is termed Dissemination.
6. **Feedback**: The intelligence cycle is not a closed loop. Feedback is received from the decision maker and other sources and revised requirements issued. During the cold war, 90 % of the data used for intelligence based decision making came from military or other agencies and 10 % from open sources. Now, the figure is 90 % from open sources with the 10 % from military or other agencies. Defence assets are normally tasked to be on station, whereas civil Low earth orbit (LEO) may only come around every 6 days. Optimizing both however is critical as useful civil data harvesting has a high potential to advance warn, or, retrospectively, work out how something was arrived at as opposed to real time streaming of an area of interest. This is termed Feedback.

So in the context of the above, if we imagine the current state of the art for the collection, processing, analysis and dissemination of this data—the intelligence cycle—as an increasingly narrowing funnel, with the exponential increase in the sources and demand for OSINT as an essential part of the mix, then the critical processing and analysis, where information is turned into usable intelligence, has become a considerable bottleneck (see Chaps. 1 and 2).

This critical bottleneck can be seen marked in red in Fig. 4.2. This process has not kept pace with the ability to collect data in today's digital world; especially, where 90 % of all data now comes from open sources. Nor has the current state of the art for the integration together of this multisource data kept pace in any meaningful way.

The increased use and exploitation of OSINT into the wider intelligence mix, will also include that which is space-based. Here, along with the challenges presented by the 4Vs of data, the issues associated with spaced based technology (especially that of imagery) from long communication times and either poor slave rates, or invariant (fixed) views of the terrain, will add to the issues that befall all other data in the current state of the art. Therefore in processing and analysis—the essential functions where the data becomes usable intelligence—the critical bottleneck is exacerbated when spaced based OSINT, an aspect that is increasingly common-place, is included into the mix.

There are issues too in the crucial human needs and behavioural understanding of the end user decision makers for how OSINT, as part of an integrated and wider

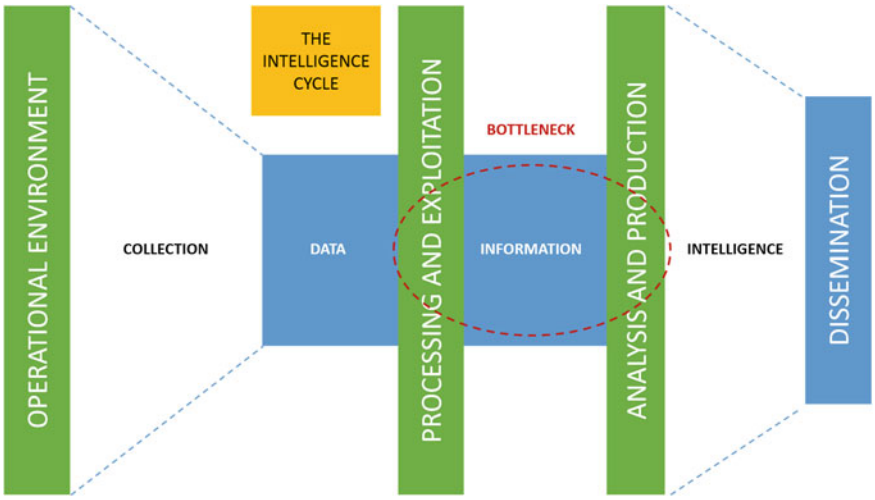

Fig. 4.2 Information bottleneck (Source: "Joint Publication 2-0, Joint Intelligence". Defense Technical Information Center (DTIC). Department of Defense. February, 2013)

intelligence mix, must be provided to them, in what manner it must be provided and through what means, in order to support better informed decision making. These can be summarised as the following:

- With the exponential increase in the availability and use of OSINT, the ability to collect data far exceeds techniques to analyse it and the 4V's of data requiring analysis is increasing logarithmically—thus the problem is only getting bigger. Thus more efficient (process) or faster (technology) approaches are required in Data Analytics—for those professional and expert individuals and analysts sifting through data, looking for themes and creating summaries.
- The pervasiveness of 24 h news and social media is leading to politicians needing an increasing confidence that intelligence has the highest probability of being correct and remaining time-stamped (i.e. valid) to enable an appropriate response. This is regardless of either civil or military context.
- The technology used by extremist groups/individuals equals, and may in some instances exceed, that available to either the military or civilian authorities and LEAs and often, their agility in how they apply such technologies, far surpasses that of the authorities.
- The application of Big Data and the benefits of Big Data analytics to the use of OSINT are much discussed and promoted but are little understood, let alone properly integrated into either the civilian or military decision making contexts (see Chap. 3).
- For the use of OSINT, the generation of data from space technology, generally in the form of imagery, Exocentric (god like) views of the earth, must now be recognised as a constant throughout the Intelligence Cycle and for this, there is

no exception to any other form of data. The 'views' need to make sense and their spatial orientation needs to be understood by the end user, trusted to be integrated into all the other data sources (ground based and aerial, human and technical, open source and specific) and when acted upon, some form of feedback needs to be provided to the end user that their actions are appropriate.

Taking all of the above into consideration, the need to resolve the challenges and issues surrounding the integration and use of OSINT into the Intelligence Cycle and wider mix is paramount, in order to enable decision makers to fully exploit its value and benefit. Such benefits as:

- The ability to ratify military intelligence, especially that from OSINT space-based imagery, which otherwise cannot be ratified
- A greater application and exploitation of OSINT as part of the wider mix for LEAs and emergency uses would have operational efficiency, effectiveness and economic benefits along-side those of better informed decision making
- The ability to speed up, make more accurate and increase the trustworthiness of OSINT that supports better decision making, would impact upon the quality of decisions made by politicians at the grand strategic level; as well as by strategic and tactical commanders operationally in times of stress, danger and need

One such example of this integration of OSINT into the wider intelligence mix and cycle is seen in the US model in moves by the Unites States intelligence community toward institutionalizing OSINT as seen in Fig. 4.3. It is taken from Open Source Intelligence: A Strategic Enabler of National Security produced by the Centre for Security Studies in Zurich, Switzerland in 2008.[3]

4.3.1 Understanding the Application of OSINT in Operational Decision Making

Gathering the data, processing and analysing it, then disseminating it as usable intelligence, is an international activity; as much as it is a local one. All dependent upon the task, need and outcomes sought. In many instances, local need translates and flows through into a national or international one. For the purposes of this chapter, UK decision making has been used as context and whilst structures and methods of working may differ from nation to nation, the principles and synergies to enable such international collaboration, especially where significant cross-sector cross border events are concerned, apply equally to one nation or LEA as they do to another.

At the highest level, the UK's National Security Council (NSC) and its supporting structures enable greater clarity of strategic direction, consolidated

[3]Pallaris, C. (2008). CSS Analysis in Security Policy. Available at: www.isn.ethz.ch.

Institutionalising OSINT: The US Model
Assistant Deputy Director of National Intelligence for Open Source • Establishes open source strategy, policy and program guidance • Makes sure that a single open source architecture is developed • Advises agencies and departments outside the National Intelligence Program regarding the acquisition of OSINT
National Open Source Committee • Provides guidance to the national open source enterprise • Members are senior executives from the Open Source Center, Office of the Under Secretary of Defense for Intelligence, department of Homeland Security, CIA, National Security Agency, National Geospatial-Intelligence Agency, Department of State's Bureau of and Research, Defense Intelligence Agency, Federal Bureau of Investigation, Office of the intelligence community's CIO
Open Source Center • Created in 2005 by the Director of National Intelligence, with the CIA as its executive agent • Several hundred full time personnel • Advances the intelligence community's exploitation of open source material; helps to develop mini open source centers within the respective agencies • Nutures acquisition, procurement, analysis, dissemination, and sharing of open source information, products, and services throughout the government • Makes reports, translations, and analytical products available online in a secure website available to government officials (www.opensource.gov)

Fig. 4.3 Institutionalising OSINT: The US model (Source: Best and Cumming 2007)

consideration of all national security risks and threats, and coordinated decision-making and responses to the threats faced. By way of providing context, the following, taken from the UK Government's National Intelligence Machinery, provides a useful overview to how all intelligence, whether OSINT or other, needs to be considered as a whole.[4]

4.3.2 UK Government Intelligence: Its Nature, Collection, Assessment and Use

Secret intelligence is information acquired against the wishes and (generally) without the knowledge of the originators or possessors. Sources are kept secret from readers, as are the many different techniques used. Intelligence provides privileged insights not usually available openly. Intelligence, when collected, may by its nature be fragmentary or incomplete. It needs to be analysed in order to identify significant facts, and then evaluated in respect of the reliability of the source and the

[4]National Intelligence Machinery: UK Government November 2010.

credibility of the information in order to allow a judgement to be made about the weight to be given to it before circulation either as single source reports or collated and integrated with other material as assessments.

SIS and GCHQ evaluate and circulate mainly single source intelligence. The Security Service also circulates single source intelligence although its primary product is assessed intelligence. Defence Intelligence produces mainly assessed reports on an all-source basis. The Joint Terrorism Analysis Centre produces assessments both on short-term terrorist threats and on longer term trends relating to terrorism. Assessment should put intelligence into a sensible real-world context and identify elements that can inform policy-making. Evaluation, analysis and assessment thus transform the raw material of intelligence so that it can be assimilated in the same way as other information provided to decision-makers at all levels of Government.

Joint Intelligence Committee (JIC) assessments, the collective product of the UK intelligence community, are primarily intelligence-based but also include relevant information from other sources. They are not policy documents. JIC products are circulated to No. 10, Ministers and senior policy makers. There are limitations, some inherent and some practical, on the scope of intelligence, which have to be recognised by its ultimate recipients if it is to be used wisely. The most important limitation is incompleteness. Much ingenuity and effort is spent on making secret information difficult to acquire and hard to analyse. Although the intelligence process may overcome such barriers, intelligence seldom acquires the full story. Even after analysis it may still be, at best, inferential.

Readers of intelligence need to bear these points in mind. They also need to recognise their own part in providing context. A picture that is drawn solely from secret intelligence will almost certainly be a more uncertain picture than one that incorporates other sources of information. Those undertaking assessments whether formally in a written piece or within their own minds when reading individual reports, need to put the intelligence in the context of wider knowledge available. That is why JIC assessments are “all source” assessments, drawing on both secret and overt sources of information. Those undertaking assessments also need to review past judgements and historic evidence. They need to try to understand, drawing on all the sources at their disposal, the motivations and thinking of the intelligence targets.

Where information is sparse or of questionable reliability, readers or those undertaking assessments, need to avoid falling into the trap of placing undue weight on that information and the need to be aware of the potential risk of being misled by deception or by sources intending to influence more than to inform. In addition readers and those undertaking assessments need to be careful not to give undue weight automatically to intelligence that reinforces earlier judgements or that conforms to others’ expectations. If the intelligence machinery is to be optimally productive, readers should feedback their own comments on intelligence reports to the producers. In the case of human intelligence in particular, this is a crucial part of the evaluation process to which all sources continually need to be and are subjected.

The quality of the information underlying the decisions taken by the National Security Council is crucial. Piecemeal consideration of issues by too many different bodies risks leading to incoherent decision-making and a lack of overall prioritisation. An "all hazards" approach to national security ensures cohesion and includes:

- The creation of a new National Security Risk Assessment to be updated every other year
- Constant assessment of all sources of information concerning those priority risks, feeding directly into the National Security Council
- A coordinated early warning mechanism to identify and monitor emerging risks
- A cross-Government horizon-scanning system to look at risks and threats which might emerge in the longer term

Figure 4.4 illustrates the UK's National Security structures.

Sitting below the NSC is the Cabinet Office Briefing Room (COBR) or sometimes referred to as COBRA and refers to the location for a type of crisis response committee set up to coordinate the actions of bodies within the UK government in response to instances of national or regional crisis, or during events abroad with major implications for the UK. The constitution of a COBR meeting depends on the nature of the incident but it is usually chaired by the Prime Minister or another senior minister, with other key ministers as appropriate, and representatives of relevant external organizations. The following diagram illustrates the relationship between COBR and the local level Strategic Coordinating Groups which are set up across the UK and meet regularly for planning, training and exercising, as well as in times of actual need to respond to a major incident. Figure 4.5 shows the construct of a COBR meeting.

With all major incidents, whether from man-made, malicious or natural causes, as a general principle, the collective planning, response and recovery effort will have one or more strategic level commanders who ultimately, are in charge of the situation; take the decisions; and, are responsible for the consequences of their actions. These strategic commanders may operate at different levels: from strategic command of the collective effort on the ground, up to grand strategic command at a

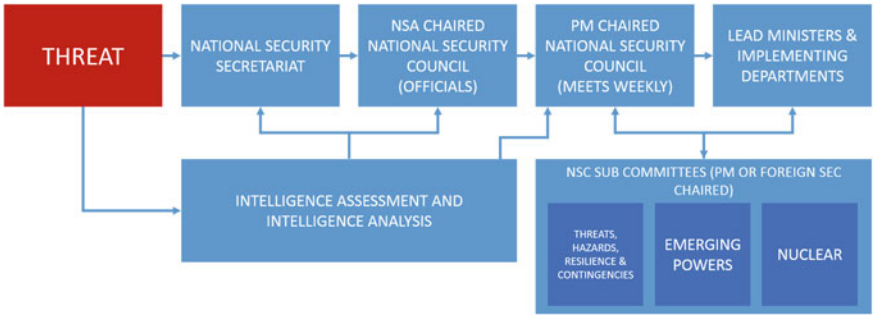

Fig. 4.4 UK National Security Council structure (Source: HM Government)

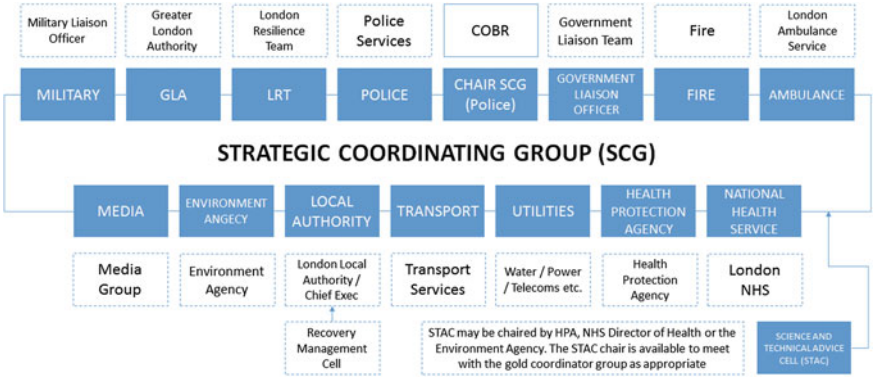

Fig. 4.5 Construct of a COBR meeting and Strategic Coordinating Group (Source: London Resilience, Strategic Coordination Protocol)

policy and/or political level. This is also the case for the strategic command of the individual multi-agency organisations involved in the event.

Their common, shared and defining criteria, is that they all need to clearly understand and have a full and shared situational awareness of the wide, strategic picture for the entirety of their remit, in which they need to make decisions. In the UK civilian context, these will be known as Gold Commanders. Whilst the command layers and decision making will differ in military only operations, where the military and civilian needs do converge, as is the case with MACA (Military Aid to the Civil Authority) operations, normally, the military will fall under this strategic command structure of the civilian authorities unless determined otherwise. Their existing very 'joined-up', interoperable and well-rehearsed decision making and command functions and structures, needing to work with and integrate with those of the civilian authorities. In instances of a serious and sustained terrorist attack for example, and against a political decision, this may well be reversed through the legislative ability to temporarily hand over command of an operation to the military.[5]

Sitting below the strategic commanders shown above, there generally sits two further levels of commanders that operate more closely to the front line. These are known in the UK context as Silver and Bronze. The Silver operating as the tactical command of the collective effort on the ground, focussing on achieving a less broad effect and outcomes from the Gold, with their effort directed into the incident itself and the immediate environs.

It should be noted that the terms Operational and Tactical are used in reverse between military and civilian organizations in the UK, including LEAs. Within the EU the military levels of command may be used in other countries. Bronze commanders will be responsible for the direct effort and effect of their organisations into the incident itself. Like the Golds, there may be multiple Silver and Bronze

[5]Military aid to the Civil Power (MACP).

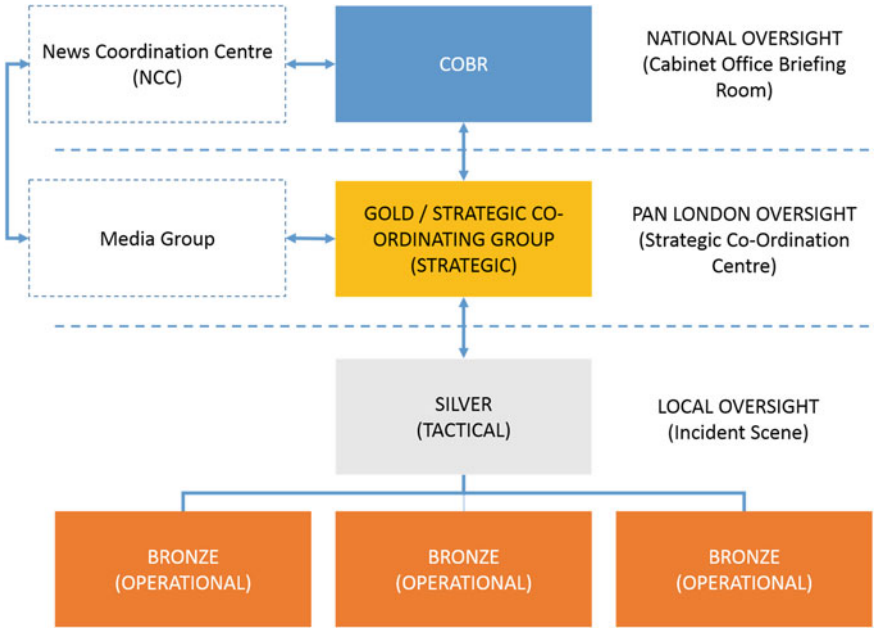

Fig. 4.6 Operational and tactical oversights (Source: HM Government)

commanders due to the multiple organisations and stakeholders involved. Aside from the establishment of clear lines of responsibility between all of the respective Gold, Silver and Bronze commanders, better informed decision making at all of the different levels from the application and exploitation of space-based imagery as part of the Integrated Intelligence mix, would be a much sought after outcome to benefit team and shared situational awareness. A recurring theme identified in many previous major incident inquests both in the UK as well as internationally. These structures can be seen in Fig. 4.6.

In support of the above structures and decision makers are the analysts and technicians working within the bottleneck of the data processing and analysis function of the Intelligence Cycle. This population, whether processing the data in order to create usable and meaningful intelligence for civil, military or converged operations, need to know and understand the end user needs and requirements emanating from the structures seen above; how decisions are informed by the intelligence and how, any greater exploited use of OSINT as part of the wider intelligence mix can be optimised for onward dissemination.

It is clear, that whether analysts are producing intelligence for politicians and diplomats to inform their decisions at a grand strategic or strategic level or, for operational commanders on the ground to use tactically, an understanding by those analysts of how the intelligence they provide needs to be received and used can only serve to help support better informed decision making. The following example

taken from the Royal United Services Institute report in 2010 on interoperability in a crisis underlines the importance of this approach:

> Several recommendations made in RUSI 2010 report Interoperability in a Crisis 2: Human Factors and Organisational processes16 refer specifically to the need to improve mechanisms for building and disseminating situational awareness, in particular, Recommendation 23, which calls for the strengthening of joint training that increases organisations' understandings of one another; and Recommendation 24, which calls for stronger frameworks for sharing information and lessons identified from actual events and from exercises, so that planners and responders can learn from previous experience …Technology solutions need to suck in data, but there need to be trained and experienced analysts who look at all the information coming in and turn it into a 'so what?' that enables command decisions. Information and intelligence needs to be handled and disseminated so that it makes sense to the people who receive it … GIS is essential … a common risk information picture in particular is needed at Silver and Gold (Cole and Johnson 2010).

It is clear from the above that the ability to collect information, to amalgamate information from different sources, to process and analyse this information and to use it to produce a Commonly Recognised Information Picture that can inform the command decisions of Gold, Silver and Bronze commanders is far from mature. The growth in sources and demand of OSINT can only compound things. Creating situational awareness on the scale needed in many of the incidents faced in the 21st century and enabling the means for better informed decision making that must result, is beyond the Governance mechanisms that currently exist as well as beyond the experience and training of most incident commanders, at all levels of the command and decision making chain.

4.4 How Might an Overarching Information Governance Architecture Support OSINT for Decision Making Within the Wider Intelligence Mix and Cycle?

Previously mentioned is the complexity of the System of Systems and how this complexity compounds and effects the use of OSINT for decision making. Across these complex systems and their array of supporting networks, there is both a supply and demand side for the data and its disseminated usable intelligence. The complexity of this supply and demand side of data, the systems and networks in which it exists and the multiple different stakeholders across and throughout the Intelligence Cycle, can all be captured. Through the use of an Enterprise Architecture,[6] approach, such as that used by NATO in developing a model of a current or future state of an enterprise. An enterprise being an organisation, a system (including the human factors) or a project. The purpose of enterprise

[6]NATO Architecture Framework: http://nafdocs.org/introduction/.

architecture is to capture the complex dependencies that exist in large-scale systems of systems so as to aid with decision support. In using such an approach, an overarching Information Governance Architecture (IGA) can be created, as can a set of supporting business process flows that map the stages and progress of each and every component—supplier, demander and stakeholder. Such an IGA would provide all decision makers across the entire spectrum of the Intelligence Cycle and decision making process, with an enabling means and set of tools, by which to understand and manage the complexity of the systems in which they operate and in which they are asked to make often critical decisions to protect us (see Chap. 1).

The IGA could represent an integrated model of the System of Systems in which the supply and demand of information and intelligence exists. This would be from the operational and business aspects, to the technologies and systems that provide capability. By covering both the operational and technical aspects across such a system, the architecture enables all communities of interest to gain the essential common understanding needed to deliver benefits that are required from the application of OSINT as an integrated component of the wider intelligence mix. Such an IGA would enable a unified, end to end view of where changes and transformation to any stage of the Intelligence Cycle can take place, whether human or technical, process or procedure, Governance or application, to improve the efficiency and effectiveness of the intelligence Cycle and therefore support better informed decision making whether at a strategic or tactical level.

In doing so, one of the main focuses of the IGA would be to present a clear vision of the system in all of its dimensions and complexity in terms of its existing state, or Current Operating Model (COM) and its desired, future state(s) or Target Operating Model (TOM). The result of this would be to support all aspects of the requirement for the use of a fully integrated OSINT including: Governance and policy; Strategic planning; Tactical planning and operations (front line and logistics); Automation of processes; Capability/requirements capture. An IGA would manage and simplify the inherent complexity in a multi-stakeholder and dynamic environment, with its 'single source of truth' used to drive agile and iterative testing and governing rules and principals for the use of an integrated OSINT and wider intelligence mix whether strategic or tactical. It would enable the capture, interrogation and understanding of the following critical questions surrounding the use of OSINT:

1. **Capability Mapping**—capturing the human and technical capabilities and expertise, both civil and military, for OSINT, including that of space-based imagery, and where and how it must be applied and be useful as part of the wider intelligence mix within the Intelligence Cycle, allowing:
    - A mapping and analysis of OSINT capabilities, technology, expertise and best practice currently available to end users from both the civil and military sectors
    - A roadmap for where and how OSINT will provide the most utility and benefit to end users in the decision making tasks and where and how it integrates into the wider intelligence mix to support decision making needs

2. **Requirements Capture**—how will end users, both analysts and decision makers, need to request, be presented with, access and use OSINT as part of the wider intelligence mix within the Intelligence Cycle, allowing;

   - A comprehensive needs analysis across the spectrum of end user requirements throughout the collection, processing, analysis, disseminating and decision making Intelligence Cycle.

3. **Big Data Analytics**—data for intelligence use is already Big Data in that it is far in excess of end users ability to cope with it. Greater exploitation of OSINT, especially with the inclusion of space-based imagery, will add to that: how can Big data analytics be better applied to support better informed decision making given the limitations of the current state of the art in processing and analysis, allowing:

   - An audit, map and analysis of Big data applications and solutions that can ensure OSINT can be used efficiently and effectively as part of the wider mix across the Intelligence Cycle, including but not exclusive to
   - A review of how techniques such as natural language and image processing, geo-location extraction and other sophisticated querying techniques and/or map-based visualisations can be used to mine social media and other open sources and how Big data technologies such as Hadoop or NoSQL data-stores may be implemented for effective querying, perhaps in real-time
   - Integration of relevant findings into the Technology Blueprint, TOM and Concept of Operations.

4. **Social Media**—with 90 % of data for intelligence based decision making now coming from open sources, of which social media is a sizeable slice, what social media currently exists and what might exist in the future? How might it, as part of the wider intelligence mix, help validate other data sources and support better decisions;

   - Produce an audit, map and analysis of the Social Media applications and requirements that can contribute into, and complement the use of OSINT, for better informed decision making
   - A review and analysis for how these findings integrate with the tasks and outputs for the Big data activities seen above, social media having all the hallmarks of big data, i.e., large in size, changes quickly over time, comes from multiple data sources in multiple formats and, has a degree of uncertainty about the accuracy
   - Integration of relevant findings into the Technology Blueprint, TOM and Concept of Operations

5. **Human Factors and Behavioural Modelling**—how will end users need to understand, request and use OSINT within the context of the wider intelligence mix? What human cognitive and behavioural attributes need to be understood and designed for to support better informed decision making and how these might be measured:

- Incorporation of a model for the needs and behaviours of end users for shared and team situational awareness in the context of better informed decision making
- Use of a psychological model(s) of reasoning and decision making in crisis situations including effects of biases and heuristics; understanding the range of end user needs such as exocentric and FPV (First Person Views), the use of degraded imagery and mobile technologies in support of decision making where space-based OSINT is concerned
- Review of how control rooms and C3i centres need to deal with and display OSINT during times of uncertainty, with multiple inputs and where centres are remote and/or decision making is distributed
- Training needs analysis and development of curricula for civil, military and shared communication and situational awareness domains, including an analysis and scope for new immersive synthetic training that would develop new forensic approaches and skills for the end user analyst community
- Integration of relevant findings into the Technology Blueprint, TOM and Concept of Operations

6. **Technology Blueprint**—what technology is needed to 'glue' OSINT into the wider intelligence mix and within the Intelligence Cycle together and what technology will provide the interface(s) for how end users will want to use it? How will it need to work in both the separate civil and military domains as well as shared ones?

   - A review and analysis across the spectrum of technology requirements and needs for OSINT integration across the Intelligence Cycle of data, processing/analysis, dissemination and feedback, ensuring capture and focus of the technology priorities of the integration of OSINT
   - Scope and produce a technology blueprint to support a knowledge architecture, ensuring inclusion of the findings from the activity areas detailed above, focussing on the core technology outputs, namely the end user interface(s), supporting applications and the technology integration needs
   - The blueprint should include those aspects of data sources, communications and networks, e.g., the new 4th and 5th generation platforms, where relevant to OSINT outputs and especially, where being able to achieve and successfully share this level of intelligence will draw into the equation the critical Cyber and Crypto elements

7. **Target Operating Model (TOM)**—overall what does a fully integrated OSINT as part of the wider mix within the Intelligence Cycle look like at strategic and operational levels? Where and how do all of the moving parts, including end users and OSINT sit and fit together?

   - Building upon the Technology Blueprint and driven by the Human Factors and Behavioural Modelling outputs and design a TOM which takes the human and technical aspects and wraps around the required business and

service delivery models that would support and enable OSINT capability for better informed decision making to be used operationally
- Use an overarching Enterprise Architecture framework such as that described earlier as used by NATO that enables a unified view to be defined and understood for the entire end to end process, in order to show the compatibility of OSINT across all end users in Law Enforcement, Government and the 5 Eyes[7] community
- Include within the TOM the necessary hooks into both the existing policy and governance arrangements for operational use of OSINT in LEA operations

8. **Concept of Operations (CONOPS)**—how will OSINT, including that of publicly available imagery such as Google maps or other space-based imagery, as an integral and integrated part of the wider Intelligence mix, be operated across the entirety of end users, both civil and military, across the Intelligence Cycle in both day to day use as well as in a crisis.

- Working with end users across the entire spectrum of the Intelligence Cycle, scope and produce a detailed Concept of Operations for how OSINT will be needed and used in both a day to day role as well as in varying different crisis situations.
- Include within the CONOPS scope a review for the use of OSINT in an integrated mix across the Intelligence Cycle that addresses the interoperability and interdependencies of the following.

  – *Training*: Do existing training methods for analysts and decision makers need to adapt or be re-written to accommodate, integrate and benefit from the use of OSINT?
  – *Equipment*: Are current or planned equipment, systems and technology fit for purpose for OSINT as an integrated part of the intelligence mix?
  – *Personnel*: Are the right people, skills and expertise in place to maximise the use and value of OSINT?
  – *Information*: Are existing information management approaches and outputs structured in the right way to accommodate a greater integration of OSINT?
  – *Concepts and Doctrine*: Are current and future methods of planning and implementation at a conceptual and doctrinal level affected by OSINT and in what way?
  – *Organisation*: Is the current structure of an organisation(s), it's governance, leadership, reporting and decision making enabled and in the right shape to benefit from OSINT?

[7]5 Eyes community: Canada, Australia, New Zealand, the United Kingdom (UK) and the United States (US) are members of the Five Eyes intelligence community. https://www.opencanada.org/features/canada-and-the-five-eyes-intelligence-community/.

- *Infrastructure*: Is the existing infrastructure—the networks, systems and any physical infrastructure right for incorporating OSINT into the intelligence mix?
- *Logistics*: Are the supporting logistics that enable and support the use of OSINT formed up correctly to exert maximum benefit and leverage from the use of OSINT?

9. **Operational Implementation—Enabling Functions**—An integrated model and part of the CONOPS embracing the spectrum of Policy and Governance, People and Process and Technology and Systems detailing what will be the functions used and needed by end users to implement an integrated OSINT; what are the service and business models needed to support the use of OSINT?

- An integrated and integral outputs from the CONOPS but with inclusion of policy and governance frameworks and guidelines which determine the political, legislative and management frameworks within which OSINT must reside
- Produce an audit, analysis and map of the policy, legislative and governance arrangements which currently surround the Intelligence Cycle, captured with the IGA
- Articulate and align these with the TOM to analyse and understand the alignment of the COM with those of the TOM and whether a Delta exists and what Course of Action (COA) may be required to manage any misalignment prior to inclusion into the CONOPS
- Scope, design, test and evaluate what the service delivery, commercial and business models might be to support and enable OSINT into an integrated mix for LEA use ensuring inclusion of the policy, legislative and governance needs
- Scope, design, test and evaluate for inclusion into the CONOPS the people, processes and technology required for the service delivery and commercial/business models of OSINT where these are different from the COM

4.5 Summary

To summarise this chapter, it is useful to refer to the opening two paragraphs from the US Congressional Research Service report Open Source Intelligence (OSINT): Issues for Congress December 5, 2007 as follows.

Open source information (OSINT) is derived from newspapers, journals, radio and television, and the Internet. Intelligence analysts have long used such information to supplement classified data, but systematically collecting open source information has not been a priority of the U.S. Intelligence Community (IC). In recent years, given changes in the international environment, there have been calls,

from Congress and the 9/11 Commission among others, for a more intense and focused investment in open source collection and analysis. However, some still emphasize that the primary business of intelligence continues to be obtaining and analysing secrets.

A consensus now exists that OSINT must be systematically collected and should constitute an essential component of analytical products. This has been recognized by various commissions and in statutes. Responding to legislative direction, the Intelligence Community has established the position of Assistant Director of National Intelligence for Open Source and created the National Open Source Centre. The goal is to perform specialized OSINT acquisition and analysis functions and create a centre of excellence that will support and encourage all intelligence agencies.

This statement, produced in 2007 provides a valuable reference to the direction of travel for the use of OSINT by LEAs in all aspects of their day to day use. However now, in 2016, there is a glaring absence in this statement of the terms Social media, Satellite and Drones, all of which have had an exponential increase in development, reduction of cost and use. This increase has led to a situation where during the Cold War, OSINT accounted for just 10 % of the information provision for intelligence with 90 % originating from closed source. Whereas today, this is reversed, with 90 % of information and data for intelligence use coming from OSINT.

The exponential increase in availability of OSINT and its use by LEAs, makes the need to ensure that full integration of OSINT, as it exists at present and might develop in the future, with that of closed source intelligence is essential; all within an overarching Information Governance framework. In so doing, a more accurate, timely and appropriate use by LEAs in their day to day decision making can be achieved.

Critically, this would provide a greater level of assurance in the use of such intelligence, the two sources providing mutual support, in order to assure both LEAs and the citizens whom they serve, with the knowledge that the decisions made and acted upon, have been based upon the most reliable, accurate and trusted information available at the time, and that better informed decisions have been the result. In achieving such an outcome, the perceived damage to the UK's political and intelligence communities, as indicated by the UK's inquest into the Iraqi war (BBC 2016), might be lessened or indeed, might never have occurred.

References

Akhgar B, Saathoff GB, Arabnia HR, Hill R, Staniforth A, Bayerl PS (2015) Application of big data for national security: a practitioner's guide to emerging technologies. Butterworth-Heinemann

BBC (2016) Chilcot report: findings at-a-glance. Retrieved 31 July 2016 from http://www.bbc.co.uk/news/uk-politics-36721645

Best RA, Cumming A (2007) Open source intelligence (OSINT): foreign affairs, defense, and trade division

Cole J, Johnson A (2010) Interoperability in a crisis 2 human factors and organisational processes. Retrieved from https://rusi.org/sites/default/files/201007_op_interoperability_in_a_crisis_ii.pdf

NATO (2002) NATO open source intelligence reader. Retrieved from http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATOOSINTReaderFINAL11OCT02.pdf

Pitt M (2008) The Pitt review: lessons learned from the 2007 floods. Cabinet Office, London, p 505